

ОСНОВНЫЕ БИОМЕТРИЧЕСКИЕ СИСТЕМЫ

Михайлов Алексей Алексеевич
начальник сектора отдела ФКУ НИЦ «Охрана» МВД России, подполковник полиции,
Колосков Алексей Анатольевич
старший научный сотрудник ФКУ НИЦ «Охрана» МВД России, подполковник полиции,
Дронов Юрий Иванович
старший научный сотрудник ФКУ НИЦ «Охрана» МВД России

В первой статье «Основные параметры биометрических систем» (Алгоритм безопасности. 2015. № 5) мы прошли долгий подготовительный путь, и уже настало время поговорить о самих системах биометрии.

ОСНОВНЫЕ СИСТЕМЫ БИОМЕТРИИ

Основные системы биометрии можно разделить на следующие классы:

1. Биометрия по голосу.
2. Биометрия по чертам лица (характерные точки на лице человека).
3. Биометрия по папиллярному рисунку пальца человека.
4. Биометрия по строению вен пальца или ладони.
5. Биометрия по строению радужной оболочки глаза.
6. Биометрия по сетчатке глаза.
7. Биометрия по ДНК.
8. Биометрия по почерку.
9. Биометрия по особенностям набора текста на клавиатуре ПК.
10. Биометрия по термограмме лица.
11. Биометрия по форме ушной раковины.
12. Биометрия по походке.
13. Биометрия по отражению ИК потока от кожи.
14. Биометрия по движению губ.
15. Биометрия по запаху тела.
16. Биометрия по кардиограмме.
17. Биометрия по геометрии кисти руки.

Биометрические признаки, а значит и способы биометрической регистрации, постоянно расширяются, поэтому следует ожидать появление биометрических устройств, основанных на новых признаках. На практике широко используются биометрические устройства на принципах с № 1 по № 6 из перечисленного в списке.

Биометрия по ДНК имеет самые высокие показатели по верификации, но требует специализированной лаборатории для своей реализации. За данным способом биометрии будущее, осталось пождать, чтобы такая лаборатория смогла поместиться в объем, хотя бы равный объему банкомата.

Биометрия по почерку и по набору на клавиатуре используется, но показывает достаточно скромные характеристики, в первую очередь, из-за плохой повторяемости признака самим человеком. К сожалению, человек не является машиной и для него характерно непостоянство поведенческих признаков.

Биометрия по термограмме лица для своей реализации требует тепловизора, цена на который начинается от \$ 1,5 тыс., при этом разрешение матрицы не превышает 480x640 пикселей, что сильно осложняет практическое использование данного метода.

Биометрия по форме ушной раковины недостаточна изучена, да и идентификационных признаков не так уж много.

Биометрию по походке следует отнести к категории экзотики. Видится, что данное направление является типичным из-за плохой повторяемости признака и его слабой идентификации.

О биометрии по отражению ИК потока от кожи человека практически ничего не известно, кроме того что подсветка осуществляется в средневолновой ИК области ($\lambda = 6 \text{ мкм}$), что требует специализированного ИК приемника. Пока данная технология не вышла из стадии лабораторных исследований.

Также не вышла из стадии лабораторных исследований и биометрия по кардиограмме, несмотря на то, что метод признан достаточно перспективным. Думается, что пока количество инфарктов в мире говорит об обратном.

Биометрия по движению губ имеет проблемы, сходные с проблемами биометрии по походке.

Биометрия по запаху тела имеет перспективы развития, так экспериментально доказано, что собака безошибочно отличает запах одного человека от другого, но газоанализатора, близкого по характеристикам с носом собаки, пока нет

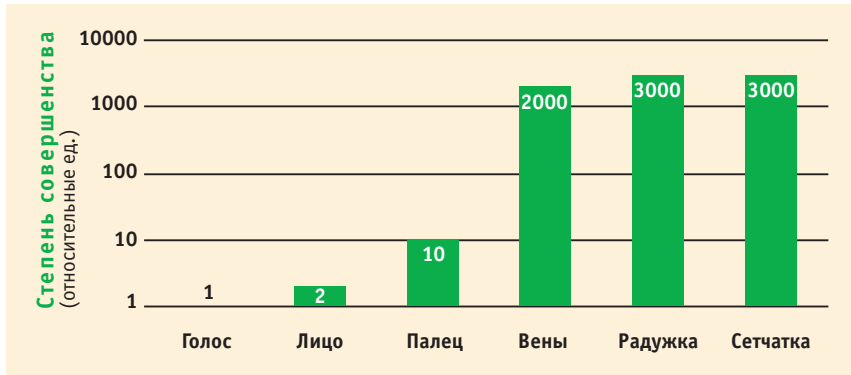


Рис. 1. Степень совершенства биометрических технологий (логарифмический масштаб)

и в ближайшей перспективе его создание не предвидится.

Биометрия по геометрии кисти руки в настоящее время не оправдала возложенных на нее надежд. Действительно, что делать, если кисть руки опухла?

Рассмотрим оставшиеся биометрические технологии по степени их совершенства. Для этого воспользуемся материалами с сайта <http://eyelock.com/index.php/products/hbox>, оставив на их совести данные характеристики (хотя сам автор склонен им верить). На рисунке 1 изображен график в условных единицах, отображающий приведенные зависимости, большее значение показателя (числа) характеризует более высокую степень совершенства технологии, т. е. меньшее количество ошибок.

Таким образом, биометрия по строению вен пальца или ладони совместно с биометрией по строению радужной оболочки глаза или по сетчатке глаза уверенно лидируют в этом негласном хит-параде, причем отрыв составляет не в разы, а на порядки. Данные технологии являются доступными по своим стоимостным и техническим параметрам.

Биометрия по строению вен достаточно точна и сложна для создания муляжа биометрического признака. Технология основана на регистрации вен человека или на принципе отражения при подсветке, или на принципе просвета биологической ткани (рис. 2-3).

Биометрия по строению радужной оболочки глаза (рис. 4-5) по степени технического совершенства конкурирует с биометрией по строению вен. Уязвимым звеном данной технологии является дистанционное считывание биологического признака и возможность создания муляжа по высококачественной фотографии. В данном направлении происходит постоянное соперничество «меча и щита». Живой человеческий глаз реагирует на изменение светового потока, сужая или расширяя зрачок, совершает произвольные хаотические перемещения (благодаря чему человек имеет периферическое зрение), реальный зрачок имеет отблеск от подсветки

и т. д. Вот эти признаки и использует биометрия по строению радужной оболочки для защиты от муляжа.

Биометрия по сетчатке глаза (рис. 6) в настоящее время считается лидером с точки зрения технического совершенства и практически не поддается обходу с помощью создания муляжей биометрического признака. Ранее такая биометрия использовалась на особо важных объектах. В настоящее время стоимость данной биометрии упала, и она стала доступна в бытовом применении.

Биометрия по папиллярному рисунку пальца человека является самой распространенной и самой дешевой по реализации биометрией, что и определяет ее широкое распространение. Уязвимым местом данной биометрии является простота создания биометрического муляжа. Действительно, снять отпечаток пальца легального пользователя достаточно просто даже без его ведома. Первые системы биометрии по отпечатку пальца взламывались мгновенно, поскольку работали только по сравнению оптического одномерного рисунка. Затем биометрические системы стали анализировать объемную структуру отпечатка пальца, на что злоумышленники ответили травлением рисунка муляжа для создания объемной формы бороздок пальца. В настоящее время соревнование «щита и меча» продолжается. В частности, разработчики стали использовать несколько типов подсветки: традиционная – снизу через призму, и вторая – через палец с каждой стороны пальца, увеличилось и общее разрешение системы, стали регистрировать пульс и изменение уровня освещенности при наложении пленки с муляжом на сканер. Примером такого типа считывателей служит сканер Sonda LS1FP. Однако нам кажется, что победа биометрии по папиллярному рисунку пальца здесь неокончательна.

САМОЕ ГЛАВНОЕ ИЗ ПЕРЕЧИСЛЕННОГО В РАЗДЕЛЕ

1. Биометрия по строению вен пальца или ладони совместно с биометрией



Рис. 2. Строение вен руки человека



Рис. 3. Устройство для регистрации строения вен руки человека



Рис. 4. Внешний вид регистратора радужной оболочки глаза



Рис. 5. Регистратор радужной оболочки глаза (встроен в «мышь» ПК)

Рис. 6. Внешний вид регистратора сетчатки глаза





Рис. 8. Сканирование сразу двух отпечатков пальцев

по строению радужной оболочки глаза или сетчатки глаза уверенно лидируют по своим техническим возможностям.

2. При ограничении по финансовым возможностям рекомендуется использовать биометрию по папиллярному рисунку пальца более поздних разработок.

БИМОДАЛЬНЫЕ ТЕХНОЛОГИИ

Бимодальные технологии (от лат. bis – дважды, modus – способ). Как бы ни были совершенны биометрические системы, лучше использовать две технологии одновременно, чем одну. Резкое снижение цен на биометрические технологии позволяет использовать две биометрические системы без существенных потерь для массового применения в быту (рис. 8-11).

Основное назначение бимодальных технологий – резко увеличить техниче-



Рис. 9. Банкомат фиксирует клавиатурный код и строение вен пальца

ские характеристики за счет одновременного использования различных технологий, на рисунке 14 изображена DET (К00) характеристика бимодального решения для смартфона с использованием верификации по голосу и изображению лица.

Обратите внимание, насколько улучшились характеристики (рис. 12).

МНОГОМОДАЛЬНЫЕ И МНОГОРУБЕЖНЫЕ СИСТЕМЫ БИОМЕТРИИ

Развитие биометрии несомненно будет происходить по принципу многомодальности, т. е. будут использоваться сразу несколько различных биометрических технологий, что резко снизит вероятность как ошибок первого рода, так и ошибок второго рода. Видится, что наиболее перспективными будут технологии биометрии по строению вен совместно с биометрией по строению радужной оболочки гла-



Рис. 10. Гибридный сканер нового поколения анализирует одновременно отпечаток пальца и строение вен пальца

за или сетчатки глаза. При использовании биометрии по венам пальца необходимо использовать идентификацию по нескольким пальцам одной или двух рук. В данных вариациях возможно использовать биометрические признаки по принципу «два совпадения из трех», строить различные схемы анализа, используя логические сочетания «И», «ИЛИ», «И + ИЛИ».

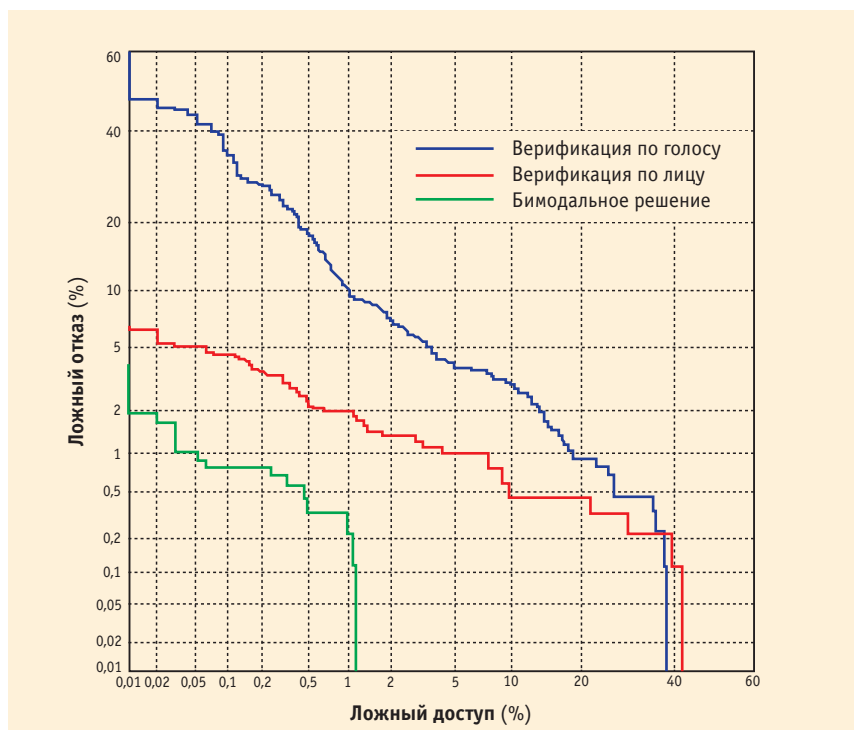
При использовании технологий с различными характеристиками по вероятностям ошибок, например, биометрия по вене + по лицу человека + по отпечатку пальца, принятие решения должно осуществляться с учетом весовых коэффициентов того или иного параметра для каждой биометрической технологии.

Для еще большего повышения надежности возможно использование многорубежной биометрической охраны. Сразу оговоримся, что в таких системах охраны будем использовать только верификацию пользователя, что резко

Рис. 11. Считыватель для распознавания лиц и идентификации по Проху-картам



Рис. 12. DET-график для лицевой, голосовой и бимодальной верификации



ПЕРЕЧЕНЬ ДЕЙСТВУЮЩИХ НАЦИОНАЛЬНЫХ СТАНДАРТОВ (БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ)

(по состоянию на 01.10.2014)

ОБОЗНАЧЕНИЕ НАЦИОНАЛЬНОГО СТАНДАРТА	НАИМЕНОВАНИЕ НАЦИОНАЛЬНОГО СТАНДАРТА
ГОСТ Р ИСО/МЭК 19794-1-2008	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 1. Структура
ГОСТ Р ИСО/МЭК 19794-2-2013	Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки
ГОСТ Р ИСО/МЭК 19794-3-2009	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца
ГОСТ Р ИСО/МЭК 19794-4-2006	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца
ГОСТ Р ИСО/МЭК 19794-5-2013	Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица
ГОСТ Р ИСО/МЭК 19794-6-2006	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза
ГОСТ Р ИСО/МЭК 19794-7-2009	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи
ГОСТ Р ИСО/МЭК 19794-8-2009	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 8. Данные структуры остова отпечатка пальца
ГОСТ Р ИСО/МЭК 19794-9-2009	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 9. Изображения сосудистого русла
ГОСТ Р ИСО/МЭК 19794-10-2010	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки
ГОСТ Р ИСО/МЭК 19795-1-2007	Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура
ГОСТ Р ИСО/МЭК 19795-2-2008	Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний
ГОСТ Р ИСО/МЭК ТО 19795-3-2009	Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях
ГОСТ Р ИСО/МЭК 19795-4-2011	Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость
ГОСТ Р ИСО/МЭК 19784-1-2007	Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса
ГОСТ Р ИСО/МЭК 19784-2-2010	Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 2. Интерфейс поставщика биометрической функции архива
ГОСТ Р ИСО/МЭК 19785-1-2008	Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных
ГОСТ Р ИСО/МЭК 19785-2-2008	Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии
ГОСТ Р ИСО/МЭК 19785-4-2012	Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 4. Спецификация формата блока защиты информации
ГОСТ Р ИСО/МЭК 24708-2013	Информационные технологии. Биометрия. Протокол межсетевое обмена БиоАПИ
ГОСТ Р ИСО/МЭК 24709-1-2009	Автоматическая идентификация. Идентификация биометрическая. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 1. Методы и процедуры
ГОСТ Р ИСО/МЭК 24709-2-2011	Информационные технологии. Биометрия. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 2. Тестовые утверждения для поставщиков биометрических услуг
ГОСТ Р ИСО/МЭК 24709-3-2013	Информационные технологии. Биометрия. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 3. Тестовые утверждения для инфраструктур БиоАПИ
ГОСТ Р ИСО/МЭК 24713-2-2011	Информационные технологии. Биометрия. Биометрические профили для взаимодействия и обмена данными. Часть 2. Физический контроль доступа сотрудников аэропорта
ГОСТ Р ИСО/МЭК 29109-1-2012	Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенных в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщенная методология испытаний на соответствие
ГОСТ Р ИСО/МЭК 29109-5-2013	Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенных в комплексе стандартов ИСО/МЭК 19794. Часть 5. Данные изображения лица
ГОСТ Р ИСО/МЭК 29794-1-2012	Информационные технологии. Биометрия. Качество биометрических образцов. Часть 1. Структура
ГОСТ Р ИСО/МЭК 29141-2012	Информационные технологии. Биометрия. Одновременное получение изображений отпечатков десяти пальцев с помощью БиоАПИ
ГОСТ Р 54412-2011/ISO/IEC TR 24741:2007	Информационные технологии. Биометрия. Обучающая программа по биометрии
ГОСТ Р 54411-2011/ISO/IEC TR 24722:2007	Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии

повышает технические возможности систем биометрии.

Рассмотрим принцип построения трехрубежной охраны, хотя эти принципы можно развить и на большее число рубежей охраны.

Первый рубеж охраны (предполагается достаточно большой объем допущенных людей и, соответственно, необходима достаточно высокая пропускная способность биометрической системы). Здесь будем осуществлять пропуск с помощью биометрической системы по вене пальца. Верификацию на первом рубеже охраны будем осуществлять с помощью Проху-карты.

Второй рубеж охраны (число допущенных людей гораздо ниже, чем на первом рубеже, и пропускная способность не является критической величиной). Осуществлять пропуск будем с помощью биометрической системы по вене другого пальца руки и другому вспомогательному биометрическому признаку (радужная оболочка глаза или лицо). Верификацию на втором рубеже охраны будем осуществлять с помощью ввода буквенно-цифрового пин-кода (не менее 6 знаков). Доступ ко второму и третьему рубежу охраны будет заблокирован, если человек не прошел первый рубеж охраны (не зарегистрирован проход через него).

Третий рубеж охраны предназначен для избранных. Здесь используется правило двух (трех) лиц. Допуск возможен только при одновременном проходе только двух носителей тайны третьего уровня. Первоначально необходимо применить новую Проху-карту, чтобы иметь доступ к биометрическому терминалу, далее два носителя допуска в ограниченное время должны ввести новый буквенно-цифровой пин-код и осуществить считывание сетчатки глаза. Разумеется, все действия пользователей контролируются охраной визуально на каждом рубеже (биометрия своим чередом, а без человека не обойтись) и фиксируется видеосъемкой. Будем использовать и запрет повторного прохода, суть которого заключается в том, что если пользователь не покинул зону, то никто не может по его идентификатору (в том числе и биометрическому) войти в данную зону.

Думается, что преодолеть многорубежную систему биометрической верификации будет практически невозможно.

Теперь немного реабилитируем биометрию по голосу (в том числе и по телефонным звонкам) и по чертам лица. Несомненное достоинство этих технологий в возможности осуществлять идентификацию людей без их желания, что открывает определенные возможности для борьбы с терроризмом и криминалом. Однако в настоящее время не следует воспринимать эти технологии как панацею от терроризма. Дело в том, что чем больше база

сравнения, тем меньше достоверность результата. Для видеобиометрии требуется высококачественное изображение лица, но террористы не стремятся попасть в объектив видеокамеры, да и расстояние до объекта съемки или освещение обычно далеки от оптимальных.

Тем, кто уверен, что за ним следит «Большой брат», можно успокоиться. Если вы не террорист и не мафиози, то за вами биометрические системы идентификации не следят, они просто не способны на это технически. Обычно для выборочной слежки используются другие технические возможности, но это не является темой нашего обсуждения.

Наилучшие свои возможности биометрия по голосу и по чертам лица может реализовать при стационарных проверках, например, паспортного контроля на границе. Кроме того, биометрия по голосу считается самой дешевой из представленных типов биометрии.

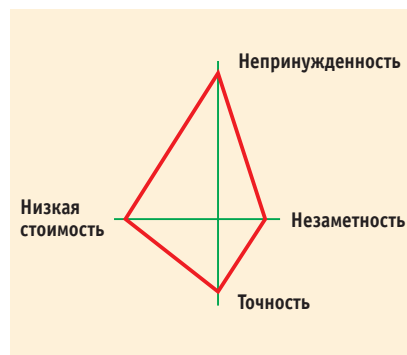
САМОЕ ГЛАВНОЕ ИЗ ПЕРЕЧИСЛЕННОГО В РАЗДЕЛЕ

1. Многомодальные и многорубежные системы биометрии способны обеспечить практически любую степень защиты объекта охраны.
2. Биометрия по голосу и по чертам лица имеет свою устойчивую нишу применения.
3. Реальные биометрические системы далеки от возможностей, демонстрируемых нам Голливудом.

ВЫБОР БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

Выбор биометрической системы для конкретного приложения является непростой задачей и, несмотря на достаточные категоричные рекомендации, изложенные выше, является сплавом компромиссов. К сожалению, в технике, выигрывая в одном параметре, мы проигрываем в другом. Для комплексной оценки биометрической системы используется график Зефира (рис. 13). Считается, что чем больше площадь изображенной фигуры, тем лучше, однако, масштаб по осям выставляет сам

Рис. 13. Пример графика Зефира



пользователь, и если для вас точность является приоритетом, то шаг единицы масштаба по этой оси у вас будет максимальным. В другом случае приоритетом будет являться стоимость, а значит и площади фигур для одних и тех же систем биометрии будут разными. Поэтому данный выбор требует взвешенности и обдуманности. Анализ материалов из различных независимых источников, представленные технические параметры от производителя, понимание сути и возможностей технологии, четкое осознание ваших собственных приоритетов в биометрической системе позволят сделать правильный выбор. В этом выборе смогут помочь и международные организации, занимающиеся тестированием биометрических систем, например: FVC 2006 (тест-отпечатки пальцев), MBE 2010 (тест-лицо), NIST 2012 (тест-голос), ICE 2006 (тест-радужная оболочка глаз) и т. д. Кто ищет — тот всегда найдет.

Говоря о биометрии, нельзя не сказать об общей проблеме биометрических признаков. Эти признаки нельзя изменить. Если буквенно-цифровой код можно изменить за 10 секунд, то изменить сетчатку глаза еще никому не удалось. Допустим, вы зарегистрировались в биометрической системе проходной предприятия и через неделю уволились, так вот, ваш биометрический признак навсегда остался (или может остаться) в биометрической базе сотрудников предприятия, и точно таким же биометрическим признаком вы будете снимать деньги с банковского депозита. Вывод — не стоит «разбрасываться» биометрическими признаками. Правда, тут проблема лежит не в сфере техники, а в сфере морального состояния общества. Следует учесть, что биометрический признак человека в любой системе биометрии хранится в защищенном цифровом виде и извлечь его не так просто, однако, такая возможность есть.

Объективности ради надо сказать, что такая проблема есть и в настоящее время. Вспомните, сколько раз отсканировали за вашу жизнь ваш паспорт? Для сотрудников силовых ведомств проблема усугубляется тем, что они поголовно проходят дактилоскопию, якобы для упрощения опознания их останков, но что-то нам подсказывает, что дактилоскопию проводят не только для этого.

ЗАКЛЮЧЕНИЕ

Тема биометрии настолько обширна, что ее невозможно с большей или меньшей полнотой изложить в одной статье, но хочется надеяться, что читатели смогут почерпнуть для себя полезное из представленного материала.

Как и всем людям, авторам свойственны ошибки, но мы были искренни в своих заблуждениях.

ЛИТЕРАТУРА И ИСПОЛЬЗОВАННЫЕ МАТЕРИАЛЫ

1. <http://www.1zagran.ru>
2. <http://fingerprint.com.ua/>
3. <http://habrahabr.ru/post/174397/>
4. <http://sonda.ru/>
5. <http://eyelock.com/index.php/products/hbox>
6. <http://www.bmk.spb.ru/>
7. <http://www.avtelcom.ru/>
8. http://www.nec.com/en/global/solutions/security/products/hybrid_finger.html
9. <http://www.ria-stk.ru/mi> «Мир измерений» 3/2014
10. <http://www.biometria.sk/ru/principles-of-biometrics.html>
11. <http://www.biometrics.ru>
12. <http://www.guardinfo.ru/> «Система физической защиты (СФЗ) ядерных материалов и ядерно-опасных объектов».
13. <http://cbsrus.ru/>
14. <http://www.speechpro.ru>
15. Poter J. F. *On the 30 error criterion*, 1997.
16. ГОСТ Р ИСО/МЭК19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура».
17. Болл Р. М., Коннел Дж. Х., Ратха Н. К., Сеньор Э. У. *Руководство по Биометрии. Из-во ЗАО «РИЦ Техносфера», 2006.*
18. Симончик К. К., Белевитин Д. О., Матвеев Ю. Н., Дырмовский Д. В. *Доступ к интернет-банкингу на основе бимодальной биометрии. Из-во «Мир измерений». 2014. № 3.*
19. Дунин-Барковский И. В., Смирнов Н. В. *Теория вероятностей и математическая статистика в технике. М.: Из-во технико-теоретической литературы, 1955.*

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. ЗАКОНОДАТЕЛЬСТВО

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ГОСЗАКУПОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В целях реализации положений постановления Правительства РФ от 16.11.2015 N 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» принят ряд нормативно-правовых актов.

Так, приказом Минкомсвязи России от 30.12.2015 № 614 определено, что официальным сайтом оператора единого реестра российских программ для ЭВМ и баз данных в информационно-телекоммуникационной сети «Интернет» является сайт reestr.minsvyaz.ru (реестр.минсвязь.рф).

В свою очередь, приказом Минкомсвязи России от 31.12.2015 № 621 утвержден Классификатор программ для электронных вычислительных машин и баз данных. Классификатор содержит ряд разделов (встроенное программное обеспечение (ПО); системное ПО; средства разработки ПО; прикладное ПО и базы данных), подразделяющихся на классы, а также описание классов программ для ЭВМ и баз данных.

Кроме того, приказом Минкомсвязи России от 31.12.2015 № 622 утверждены Правила применения классификатора программ для электронных вычислительных машин и баз данных. Как следует из Правил, Классификатор является базой данных нормативно-справочной информации, элементами которой являются наименования, коды, функциональные, технические и/или эксплуатационные характеристики, по которым определяется соответствие программ для ЭВМ классу программного обеспечения, а также указание на соответствие классов программ для ЭВМ (программного обеспечения) кодам Общероссийского классификатора продукции по видам экономической деятельности. Согласно Правилам использование кода, не внесенного в Классификатор, не допускается. Определение соответствия программного обеспечения одному или нескольким классам производится Экспертным советом по российскому программному обеспечению при Минкомсвязи России одновременно с принятием решения о включении сведений о программном обеспечении в Реестр.

В РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДОБАВЛЕНО 84 ПРОДУКТА

Министерство связи и массовых коммуникаций сообщает о том, что по решению Экспертного совета по российскому программному обеспечению (ПО) при Минкомсвязи России 84 программных продукта включены в единый реестр российских программ для электронных вычислительных машин и баз данных (реестр российского ПО). Соответствующий приказ подписал сегодня глава Минкомсвязи России Николай Никифоров. На сегодняшний день в реестре – 87 позиций.

В реестре российского ПО представлены следующие классы программных продуктов: операционные системы, системы управления процессами организации, системы управления базами данных, средства обеспечения облачных и распределительных вычислений, средства виртуализации и системы хранения данных, серверное и связующее ПО, поисковые системы, системы мониторинга и управления, средства обеспечения информационной безопасности, офисные приложения, системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных, системы управления проектами, исследованиями, разработкой, проектированием и внедрением, а также лингвистическое программное обеспечение.

Полный перечень добавленных в реестр программных продуктов опубликован на сайте министерства.

<http://minsvyaz.ru>

