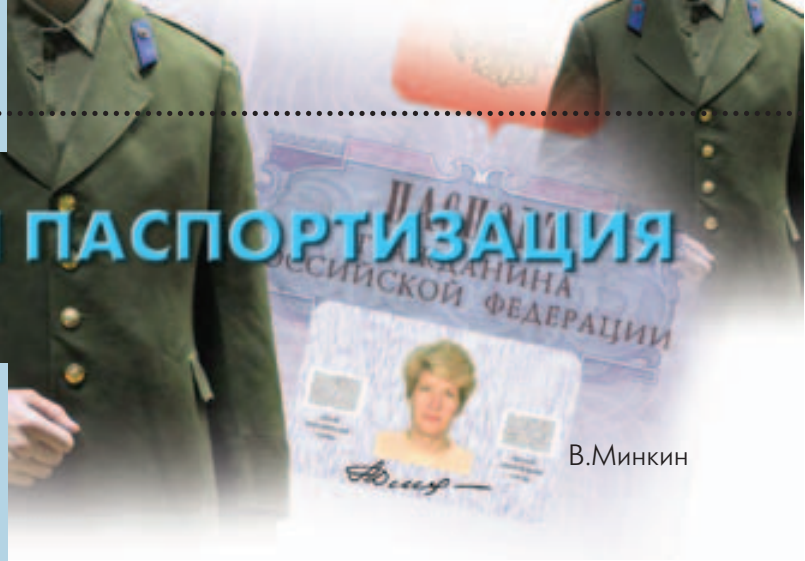

БИОМЕТРИЧЕСКАЯ ПАСПОРТИЗАЦИЯ

МИФЫ И РЕАЛЬНОСТЬ

В.Минкин

Сегодня, когда биометрическая паспортизация* становится объективной реальностью, на передний план выходят вопросы конкретного ее внедрения и определения принципов построения биометрических паспортных систем. В связи с этим необходимо рассмотреть и развенчать технические и политические мифы, которые сознательно формируются вокруг этих систем.

Миф 1. *Чем сложнее система биометрической паспортизации (чем больше в ней закодировано информации на уровне биометрических удостоверений личности), тем она лучше и надежней (тем лучше защищена от подделок и фальсификаций).*

Для начала определим, кому выгодно данное утверждение. Прежде всего, оно выгодно крупным электронным компаниям, разрабатывающим и использующим технологию смарт-карт, а также технологии кодирования и декодирования информации. Эти компании обладают огромными возможностями и капиталами для лоббирования своих идей.

Тезис о необходимости кодирования ключевой информации, справедливый для обычных систем безопасности, оказывается просто бессмысленным для биометрических систем. Биометрическая информация никогда не бывает скрытой, ее достаточно просто получить с ее носителя, т.е. с живого человека. Не случайно никому раньше не приходило в голову печатать фото лица человека в паспорте в закодированном виде, поскольку это лицо видно всем. Аналогичная ситуация и с другими биометрическими признаками, например с отпечатками пальцев. Конечно, их не так просто скопировать, как лицо человека, но их легко снять с любого предмета, которого касается человек. Именно поэтому кодировать известное биометрическое изображение в удостоверении для повышения секретности так же бессмысленно, как прятать ключ под ковриком перед сейфом. Тот, кто захочет иметь ваши биометрические параметры, всегда может получить их непосредственно с человека, а не с удостоверения. Получается, что **для биометрических систем самым важным является** не кодирование биометрической информации в носителе, а **возможность отличить живой носитель биометрической информации от поддельного**. Именно это свойство характеризует и обеспечивает реальную надежность и безопасность любой биометрической системы, в том числе паспортной.

Надежность системы безопасности определяется, прежде всего, средствами, которые необходимы для прохождения (взлома) данной системы относительно средств, затраченных на создание самой системы. Стоимость национальной биометрической паспортной системы, построенной по любой технологии, оценивается огромными суммами (предварительная оценка только организации биометрического контроля на основных пунктах въезда в США составляет 5 млрд. долл.), и, конечно, государство хочет получить определенные гарантии безопасности за эти деньги. Однако практически все биометрические сканеры могут быть легко фальсифицированы поддельным носителем биометрического изображения [1]. Например, получив дактилоскопический отпечаток нужного человека, легко изготовить тонкий трехмерный поддельный силиконовый носитель дактилоскопического изображения. Приклеив его к пальцу, можно успешно пройти почти через любой дактилоскопический сканер, имея при этом чужое биометрическое удостоверение личности, и никакое кодирование информации не поможет установить фальсификацию. Таким образом, огромные средства на создание глобальной паспортной системы могут быть истрачены впустую, если биометрический сканер не сможет уверенно отличить живой биометрический параметр от поддельного.

Миф 2. *Существуют реальные альтернативы дактилоскопической идентификации.*

По данным International Biometric Group [2], самой крупной биометрической организации в мире, включающей в себя более 500 биометрических компаний, дактилоскопические технологии составляют примерно 50% от общего рынка биометрических систем идентификации (без учета рынка АДИС, который делает перевес дактилоскопических технологий еще большим). Причем эта цифра относительно стабильна в течение последних пяти лет, и ее изменение в будущем маловероятно. Остальные 50% относительно равномерно распределены между примерно десятью другими биометрическими технологиями. Лучшие из альтернативных дактилоскопии биометрических технологий уступают лидеру примерно в десять раз по объему рынка и по основным рабочим параметрам. Конечно, можно говорить о том, что **дактилоскопическая идентификация не идеальна, но она значительно лучше любой другой**, хотя всегда существует определенная вероятность ошибки – как пропуска чужого, так и непропуска своего. Эти ошибки всегда присутствуют при биометрической идентификации, и у других биометрических технологий они в сотни раз больше. Во многом справедливы упреки в том, что дактилоскопическую информацию относительно легко подделать и большинство дешевых сканеров легко фальсифицировать. В то же время, изготовление поддельных биометрических носителей для альтернативных биометрических технологий – задача более простая, которой мало кто занимается, потому что она так же малоинтересна, как писать вирусы не под Windows, а для DOS или Linux. Естественно, что основную группу противников дактилоскопической паспортизации возглавляют компании-приверженцы других технологий биометрической идентификации. Еще одна группа считает, что дактилоскопия должна быть дополнена другим биометрическим параметром, чтобы усложнить систему (см. Миф 1) и сделать более надежной.

Наиболее логичные рекомендации дает институт стандартизации США [3]. Они предлагают хранить на биометрическом документе дактилоскопическую информацию о двух пальцах владельца и его фотографию. Отпечатки должны храниться в виде, предназначенном для

*ЭЛЕКТРОНИКА: НТБ, 1999, №1, с.30–32; 2000, №6, с.30–32.

автоматического считывания, а фотография лица может применяться для опознания без технических средств. Такой подход обеспечит как минимальную вероятность ошибки, так и простоту, и надежность в работе. Причем открытие эффекта объемного пульса в кончиках пальцев [4] позволяет уверенно отличать поддельные дактилоскопические носители от живых пальцев и потенциально делает дактилоскопические технологии наиболее защищенными от подделок.

Миф 3. *Биометрическая паспортизация выгодна спецслужбам и опасна для простых граждан.*

Это мнение поддерживается чаще всего самими спецслужбами и, естественно, решает обратную задачу, прежде всего потому, что органы внутренних дел (во всех странах) завалены текущей работой, и биометрическая паспортизация – это проблема, которую нужно будет решать дополнительно к существующим. Во-вторых, отсутствие быстродействующей системы идентификации личности позволяет задерживать подозреваемых на значительное время, продолжать борьбу с терроризмом традиционными и привычными методами, т.е. за счет увеличения штатов и заработной платы, а не привлечением современных технических средств.

Автоматическая система идентификации может не только выявлять преступников, но и способствовать выявлению многих ошибок, просчетов и проблем в работе МВД. Для рядовых граждан введение такой системы может привести только к уменьшению риска быть задержанным для выяснения личности на долгое время, сокращению времени на прохождение паспортного контроля, покупки билетов, т.е. на любой операции, где это удостоверение личности считывается автоматически. **Биометрический паспорт отличается от обычного только возможностью автоматической (т.е. более быстрой и объективной) идентификации, а значит более удобен для пользователя.**

Согласно опросам общественного мнения, более 80% американцев после событий 11 сентября 2001 г. согласились проходить биометрическую идентификацию, так как она позволяет повысить безопасность граждан и государства. Никому не приходит в голову отказываться от телефонных разговоров, потому что голос (такой же биометрический признак, как и отпечаток пальца) может быть похищен. Однако некоторые "защитники" свободы выступают против помещения биометрических признаков в паспорта. Более логичным можно было бы назвать протесты против любых паспортов, но выступать против биометрических паспортов аналогично выступлению против цветных телевизоров и в поддержку черно-белых.

Миф 4. *Биометрический паспорт должен быть универсальным документом, включающим в себя как можно больше различной информации.*

Данный миф противоположен предыдущему. Стремление насытить паспорт всей информацией о человеке иначе как отклонением от нормы не назовешь. Записывать в паспорт информацию обо всех болезнях человека, его финансовом состоянии, родственниках и друзьях, в принципе, при современном уровне развития техники возможно (конечно, не бесплатно). Однако какие бы гарантии разработчики ни давали о сохранности данных в паспорте и базе данных, это будут только слова. Любая информация, хранящаяся в цифровом виде, может быть прочитана, и биометрические базы данных, а не биометрические документы, следует защищать и кодировать как можно надежней. **Поэтому биометрический паспорт должен содержать только ту информацию, которая действительно необходима для уверенной идентификации личности.**

Загрузка биометрического паспорта любой другой дополнительной информацией будет приносить вред самому гражданину и снижать надежность работы системы.

Миф 5. *Необходимо создать единый биометрический паспорт, действующий во всех странах мира.*

Основной лидер в биометрической паспортизации – безусловно, правительство США и крупнейшая биометрическая компания Identix, которая пытается навязать всему миру чиповую смарт-карту с объемом памяти не менее 64 Кбит в качестве идентификационного документа. Однако даже в планах правительства США развитие биометрической паспортизации не предполагается проводить сверхбыстрыми темпами. При 280-миллионном населении США паспорта сейчас имеют только 55 млн. человек, и выдачу биометрических паспортов для этих граждан правительство предполагает осуществить в течение пяти лет, т.е. выдавать примерно 10 млн. биометрических паспортов в год. Кроме того, чиповый вариант паспортизации, который, вероятно, выберут США, достаточно дорогой. Стоимость одного такого паспорта будет составлять примерно 10 долл., а затраты на введение всей системы в США в этом случае составят десятки миллиардов долларов.

Другой полюс паспортизации – Китай, который планирует выдать 900 млн. новых паспортов в течение ближайших пяти лет и установить 10 млн. биометрических сканеров. Если бы Китай шел по пути США, то ему потребовалось бы 100 лет (!) на осуществление биометрической паспортизации. Китайское правительство стремится подогнать технологии под финансовые возможности и ограничить стоимость удостоверения 1–1,5 долл. Первоначально продекларировав введение информации об отпечатках пальцев в чипы, китайское правительство в дальнейшем было вынуждено отказаться от этой идеи из-за технико-финансовых проблем.

Российское правительство выбрало в этом вопросе выжидательную позицию, намериваясь сделать скорее политический, чем технический выбор. Это достаточно обидно – ведь в России есть собственные биометрические разработки, например система ДактоПост (Bicard) [4], запатентованная в РФ, Индии, Китае, Вьетнаме, Европе и США, которая по своим технико-экономическим показателям превосходит зарубежные аналоги (стоимость биометрического удостоверения, содержащего информацию о двух отпечатках пальцев и фото лица, менее 1 долл.). ДактоПост – единственная система в мире, которая позволяет считывать как живой палец, так и биометрическое удостоверение (паспорт) с помощью одного сканера и хранить биометрическую информацию в самом материале пластиковой карты без применения дополнительных средств памяти.

Для реального функционирования глобальной всемирной сети биометрической идентификации достаточно согласовать стандарты, оговаривающие основные принципы совместимости различных биометрических систем, причем каждая страна или группа стран может идти по своему пути создания биометрического документа.

При всей неизбежности биометрической паспортизации только ее технически правильное осуществление позволит решить те политические задачи, которые перед ней стоят. В противном случае огромные суммы денег будут просто выброшены на реализацию честолюбивых замыслов определенных политиков и компаний.

ЛИТЕРАТУРА

1. Stephanie A.C. Schuckers. Spoofing and Anti-Spoofing Measures. – Information Security Technical Report, 2002, Vol.7, No 4, p. 56–62.
2. www.bio1.com
3. Summary of NIST standards for biometric accuracy, tamper resistance, and interoperability. November 13, 2002.
4. www.elsys.ru