

УДК 683.34

ОБЕСПЕЧЕНИЕ ГАРАНТИРОВАННОЙ АНОНИМНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКОГО ОБРАЗА ПОЛЬЗОВАТЕЛЯ

А.И. Иванов, И.Г. Назаров, Ю.К. Язов, Е.С. Остроухова

Рассматривается комплекс мер, позволяющий осуществить анонимную биометрическую регистрацию пользователей информационной системы с возможностью отложенной на неопределенное время процедурой дезавуирования анонимности. Показано, что использование биометрии пользователя эквивалентно использованию его имени. При этом имя пользователя нельзя зашифровать без утраты его функциональности, а биометрия может быть зашифрована путем размещения ее в защищенный нейросетевой биометрический контейнер без ущерба для ее функциональности

Ключевые слова: анонимность, регистрация, ключ

Закон РФ «О персональных данных» [1] ставит перед производителями средств защиты информации ряд новых задач, которые не могут быть полностью решены традиционными технологиями. Рассмотрим эту проблему на примере защиты персональных данных больных социально значимыми заболеваниями такими, как: СПИД, венерические болезни, гепатит, туберкулез. Корень проблемы состоит в том, что потенциальные больные (лица только предполагающие сдавать анализы или только проходящие тестирование на наличие заболевания) должны быть абсолютно уверены в своей анонимности [2]. Потенциальные больные должны иметь гарантии государства, достигаемые применением соответствующих механизмов технической поддержки и проведением некоторой системы организационно-технических мероприятий. В случае уверенности потенциальных больных в высоком уровне гарантий их анонимности они смогут инициировать процедуры своего обследования при первых подозрениях о своем возможном заболевании. Это должно сократить число заболевших социально значимыми заболеваниями, убеждающихся в своем диагнозе со значительным опозданием из-за естественной для большинства боязни компрометации своего имени.

Рассмотрим подробнее комплекс мер, обеспечивающих гарантированную анонимность потенциальных больных социально значимыми заболеваниями. На первой стадии, когда человек только приходит сдавать анализы, он должен зарегистрироваться. При этом регистрируемому больному нет необходимости предъявлять документы и объявлять свое подлинное имя. Современные биометрические технологии позволяют зарегистрировать уникальную биометрию человека и в дальнейшем использовать ее для идентификации больного при каждом его обращении в медицинское учреждение.

При регистрации технически возможно использование любой из хорошо отработанных на сегодня биометрических технологий [3]. Могут быть использованы рисунок радужной оболочки глаза, геометрические параметры особых точек на лице, особенности рисунков отпечатков пальцев, особенности рукописного почерка человека, особенности голоса проверяемого. При использовании любого типа биометрических образов человека гарантированно анонимная регистрация человека должна проводиться в соответствии со специальными правилами. Один из вариантов структурной схемы такой биометрической регистрации приведен на рисунке.

При анонимной биометрической регистрации, регистрируемый человек должен предъявить свой биометрический образ (например, приложить к сканеру свой палец). Рисунок отпечатка пальца должен пройти

Иванов Александр Иванович – начальник лаборатории Пензенского Электротехнического института, профессор, д-р техн. наук, e-mail: leo@otd4.vsi.ru

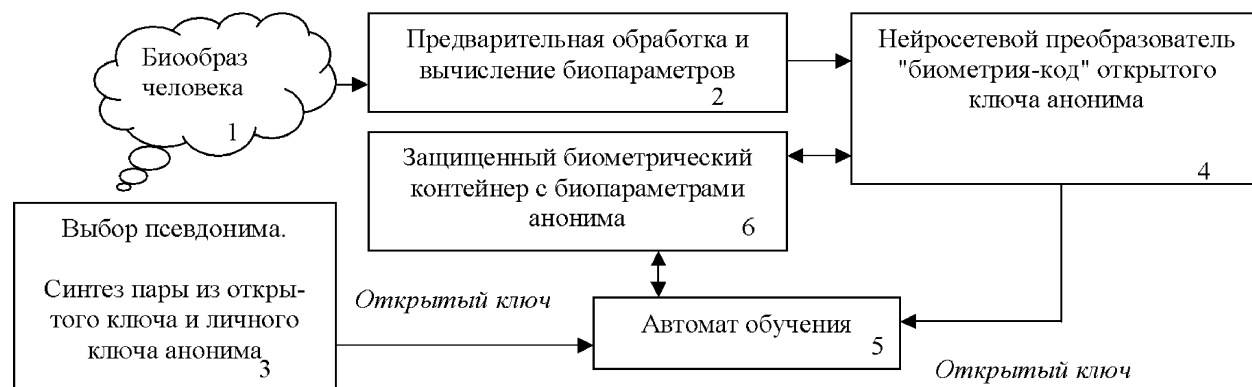
Назаров Игорь Григорьевич – начальник отдела Центрального аппарата ФСТЭК России, с.н.с., канд. техн. наук, e-mail: leo@otd4.vsi.ru

Язов Юрий Константинович – начальник 3 научно-технического центра ГНИИИ ПТЗИ ФСТЭК России, e-mail: leo@otd4.vsi.ru

Остроухова Елена Сергеевна – ГНИИИ ПТЗИ ФСТЭК России, научный сотрудник, e-mail: leo@otd4.vsi.ru

предобработку и по нему должны быть вычислены контролируемые системой биометрические параметры (блок 2). Хранить биометрические параметры анонима в открытой форме нельзя, так как по ним сравнительно

легко можно восстановить сам рисунок отпечатка пальца. В связи с этим в соответствии с требованиями ГОСТ Р 52633-2006 необходимо применить нейросетевой преобразователь "биометрия-код" (блок 4).



Структурная блок-схема анонимной биометрической регистрации человека

Нейросетевой преобразователь "биометрия-код" (блок 4) необходимо обучить преобразовывать входной биометрический образ 1 в нужный код. В анонимных биометрических системах используется асимметричная криптография [4]. Соответственно, при идентификации для каждого анонимного пользователя должна быть создана своя пара: открытый и личный ключи. На рисунке псевдоним для регистрируемого и пару его ключей вырабатывает специальный генератор (блок 3). Далее автомат обучения (блок 5) должен подобрать весовые коэффициенты нейросетевого преобразователя биометрия-код таким образом, чтобы при предъявлении биометрического образа «Свой» на выходе преобразователя появлялся открытый ключ регистрируемого анонима. При этом по требованиям ГОСТ Р 52633-2006 биометрические образы случайных людей «Чужие» должны на выходах блока 4 давать случайные коды.

Подчеркнем, что блоки 2, 3, 4, 5 могут быть выполнены в виде некоторой универсальной программы, которая до и после обучения не имеет никаких индивидуальных признаков регистрируемого. Имеет смысл систематизировать весовые коэффициенты обученных нейронов преобразователя биометрия-код и выделить их в специальный блок 6. В этом случае все индивидуальные особенности обученного преобразователя "биометрия-код" сосредоточиваются в одном

блоке 6. Так как по значениям весовых коэффициентов нейронов блока 6 невозможно восстановить сам биометрический образ, блок 6 следует рассматривать как защищенный контейнер биометрических данных анонимного пользователя.

Таким образом, по завершении анонимной биометрической регистрации потенциального больного в информационной системе лечебного учреждения должны появиться: псевдоним проверяемого, его открытый ключ, защищенный контейнер с его биометрическими данными. У самого проверяемого на руках должен остаться его личный ключ. При этом анонимный больной может не опасаться компрометации его анонимности персоналом лечебного учреждения. Медицинские работники не могут скомпрометировать анонимность больного, так как не знают его имени и не могут извлечь его биометрический образ из защищенного контейнера биометрических данных.

Тем не менее, имеющейся в информационной системе лечебного учреждения информации вполне достаточно, чтобы исключить подмену одного человека другим. При любой значимой лечебной процедуре медицинский персонал, защищая данные от подмены, должен требовать проведения процедуры биометрической аутентификации. Проверяемый должен указать свой псевдоним и предъявить свой биометрический образ. В том случае, если биометрический образ дает

нужный открытый ключ заявленного псевдонима, то аутентификация считается успешной. При этом врач точно знает, что перед ним находится именно тот больной, который первоначально проходил регистрацию при сдаче анализов.

Рассмотренная выше процедура регистрации не является полной. Она защищает от взаимных злоупотреблений только врача и потенциального больного. Для обеспечения эпидемиологической безопасности населения законодательством предусмотрена процедура, когда органами обеспечения правопорядка анонимность больного социально значимым заболеванием может быть дезавуирована. С этой целью потенциальный больной при регистрации должен оставить свои персональные данные (например, в форме файла с отсканированной третьей страницей своего паспорта).

Очевидно, что хранить персональные данные больного в такой форме нельзя. Для того чтобы обезопасить хранение своих персональных данных, больной должен зашифровать их и доверить их расшифровку лицу, пользующемуся безусловным доверием больного. Опрос больных показал, что примерно 32% из них доверяет хранение тайны своей анонимности главному врачу лечебного учреждения по сложившейся практике. Примерно, 46% больных согласны доверить хранение тайны своей анонимности нотариусу. Оставшиеся 22% больных склонны доверить защиту своей анонимности только своему личному адвокату.

Современные технологии позволяют предоставить больному возможность выбрать для себя любого гаранта его анонимности из целого списка уважаемых всеми адвокатов, нотариусов, врачей. Естественно, что каждый из будущих гарантов анонимности должен заранее выразить согласие на выполнение этой функции и оговорить условия ее выполнения. Кроме того, каждый гарант анонимности должен разместить в информационной системе лечебного учреждения сертификат своего открытого ключа. В частности это может быть сертификат, выданный любым удостоверяющим центром для проверки электронной цифровой подписи гаранта анонимности.

При выполнении этих условий потенциальный больной выбирает сам себе гаранта анонимности. Далее, потенциальный больной должен, используя свой личный ключ и открытый ключ гаранта анонимности, выработать общий секретный ключ [4] и зашифровать на нем свои персональные данные. Это обычная процедура асимметричной криптографии, широко используемая при аутентификации. После выполнения такой процедуры расшифровать персональные данные больного смогут только сам больной (обладающий своим личным ключом) и гарант его анонимности (обладающий своим личным ключом и получивший от больного или от лечебного учреждения открытый ключ больного). Остальные и в том числе органы обеспечения правопорядка или персонал лечебного учреждения расшифровать персональные данные больного не смогут. Зашифрованные асимметричной криптографией персональные данные могут безопасно храниться в информационной системе лечебного учреждения.

После зашифровывания своих персональных данных больной может отказаться от хранения своего личного ключа. Лично для больного целесообразно уничтожить свой личный ключ, так как у него, как правило, нет надежных технических средств для безопасного хранения ключей.

В итоге информационная система лечебного учреждения должна иметь псевдоним больного, защищенный контейнер с его биометрическими параметрами, шифрограмму его персональных данных. Этого вполне достаточно для обеспечения информационной безопасности анонимного лечебного процесса.

В случае предусмотренного законодательством дезавуирования анонимности больного органы обеспечения правопорядка должны обратиться за открытым ключом анонимного больного, шифрограммой его персональных данных и именем гаранта анонимности этого больного. Далее органы обеспечения правопорядка должны обратиться к гаранту анонимности, объяснить ему причины дезавуирования анонимности и получить от гаранта анонимности ключ расшифровывания персональных данных боль-

ного.

Гарантиями сохранения анонимности являются четыре фактора:

1. Высокая стойкость использованного средства шифрования персональных данных, подтвержденная соответствующими сертификатами;

2. Отсутствие у медицинского персонала возможности расшифровать персональные данные;

3. Отсутствие у гаранта анонимности возможности расшифровать персональные данные, так как их шифрограмма передается гаранту только при ситуации официального дезавуирования анонимности;

4. Сертификация информационной системы лечебного учреждения, гарантирующая отсутствие недекларированных возможностей и гарантированное уничтожение опасной информации.

Таким образом, современные технологии защиты информации позволяют гарантированно обеспечить анонимность больных социально значимыми заболеваниями. Одних только технических средств для этого оказывается недостаточно. Необходимо проведение специальных организационно-технических мероприятий. Однако поставленная задача по обезличиванию электронных историй болезни и гарантированному обеспечению анонимности больных оказывается практически реализуемой. Решить весь перечисленный комплекс задач удастся только при условии совершенствования отечественных технологий биометрической аутентификации и усиления ее поддержки соот-

ветствующими нормативно-методическими документами.

Для больных социально значимыми заболеваниями затронутая проблема наиболее остра, однако она характерна для всех систем электронного голосования и ряда схем электронной торговли. Подлинное имя пользователя и его биометрия связаны между собой по своей природе, в информационных системах они способны замещать друг друга и, если это необходимо, обеспечивать анонимность проверяемого. В отличие от шифрования имени человека на неизвестном ключе, которое полностью лишает имя его функциональности, биометрия сохраняет функциональность данных и ими можно пользоваться.

Литература:

1. Закон Российской Федерации "О персональных данных" от 27 июля 2006 г. N 152-ФЗ.

2. Нейросетевое преобразование биометрического образа человека в код его личного криптографического ключа. Коллективная монография под редакцией А.Ю. Малыгина. М.: Радиотехника (ИПРЖ), книга №29 научной серии "Нейрокомпьютеры и их применение", 2008 г. - 87 с.

3. Руд Б. Руководство по биометрии. / Болл Руд, Коннел Джонатан, Панканти Шарат, Ратха Налини. – М.: Техносфера, 2007. - 368 с.

4. Смит Э.Р. Аутентификация от паролей до открытых ключей / Э.Р. Смит. – М.: Изд-во Вильямс, 2002. - 424 с.

Государственный научно-исследовательский испытательный институт Федеральной службы по
техническому и экспортному контролю
State science research experimental institute of technical information protection problems of Federal ser-
vice of technical and export control

ENSURING ANONYMITY GUARANTEED OF THE PERSONAL DATA WITH USE OF THE USER BIOMETRIC IMAGE

A.I. Ivanov, I.G. Nazarov, Y.K. Yazov, E.S. Ostroukhova

The complex of the measures allowing to carry out anonymous biometric users registration of information system with an opportunity by procedure, postponed on uncertain time, anonymity disavowal is considered. Is shown, that utilization user biometrics is equivalent to use of his name. Thus the name of the user cannot be ciphered without loss it functionality, and biometrics can be ciphered by accommodation it in protected neuronet biometric container without damage to it functionality

Key words: anonymity, registration, key