Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, с. 65-69 (http://пниэи.рф/activity/science/BIT/T8-p65.pdf)

СОВРЕМЕННЫЕ ОТЕЧЕСТВЕННЫЕ ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ.

Колючкин А.В., Трифонов С.Е., Секретов М.В. (г. Пенза)

В настоящее время очень бурно развиваются цифровые технологии, в том числе в области услуг и сервисов, предоставляемых населению. На основе этих технологий создаются и реализуются:

- электронные платежи;
- электронные справочные службы;
- электронный документооборот;
- электронные телекоммуникационные сервисы;
- услуги электронной почты;
- цифровые удостоверения личности;
- электронные пропуска и средства охраны помещений, в том числе, электронные сторожа и системы контроля допуска;
- электронные системы голосования (как при сборе голосов, так и при закрытом голосовании);
- электронные технологии медицинских консультаций, в том числе на расстоянии;
- электронные сервисы медицинских учреждений и по обслуживанию больных и т.д. и т.п.

Перечень подобных услуг является практически неограниченным и постоянно пополняется.

Однако, массовое внедрение современных цифровых технологий в социальную сферу резко обострило актуальность и выдвинуло на первый план необходимость решения ряда сопутствующих технологических проблем, большая часть которых связана с понятиями идентификации, аутентификации и авторизации, а также доказуемости и неотказуемости.

Суть этих проблем заключается в необходимости установления подлинности и/или неизменности электронных сообщений, документов, запросов, сведений и т.п., являющихся объектами опосредованного взаимодействия людей между собой, а также людей и технических средств (или инфраструктурных образований).

Весьма специфичными в этой области являются прикладные задачи ряда медицинских и социальных учреждений, когда требуется решать проблемы достоверной аутентификации с соблюдением анонимности личности. Например, в тех случаях, когда анонимность должна быть в числе гарантированных прав человека (голосование, медицинское обслуживание).

В традиционных системах, не использующих средства автоматизации, обозначенные проблемы решались, как правило, с помощью документов, удостоверяющих личность, или с помощью различных справок и форм, заверяемых подписью ответственного лица и его печатью.

Во всех подобных документах имеется материальный носитель информации – бумага, на которую накладывается личная подпись и печать и которая объединяет в единый документ содержащуюся на ней информацию и

биометрические признаки человека, утверждающего этот документ. В этих случаях рукописная подпись является носителем биометрических и идентифицирующих параметров ответственного лица, заверяющего документ, а на паспорте, кроме того, имеется фотография его владельца – также носитель биометрических параметров человека в виде изображения его внешности.

В современных автоматизированных системах, использующих цифровые технологии, обозначенные проблемы решаются лишь частично – с помощью электронной цифровой подписи (ЭП), применяемой в составе инфраструктуры открытых ключей. В указанных системах согласно действующих нормативных актов человек, как личность, фигурирует только в начальной фазе при регистрации. В специально создаваемых для этих целей центрах регистрации в составе инфраструктуры открытых ключей фиксируются его паспортные персональные данные и производится идентификация личности.

Во всем дальнейшем взаимодействии человека с автоматизированной системой его аутентификация производится опосредованно, а, следовательно, его идентификация является также условной. Гарантами подлинности и достоверности идентификации здесь выступают только условия корректности политики безопасности и соблюдения организационно-технических и регламентных мероприятий. Причина тому – отсутствие биометрических параметров и индивидуальных признаков в сертификатах ключей ЭП, а также в отсутствии современных высоконадёжных электронных технологий биометрической идентификации личности.

Например, согласно требованиям по организации и обеспечению безопасности персональных данных при их обработке в информационных системах, утвержденных ФСБ России 21.02.2008г. №149/6/6-622 пользователи обязуются:

- не разглашать информацию о ключевых документах ЭП;
- не допускать снятие копий с ключей ЭП;
- не допускать установки ключевых носителей в других ПЭВМ;
- не допускать вывод ключей ЭП на дисплей ПЭВМ и т.п.

Уже при однократном нарушении этих требований, которые зачастую можно решить только организационными мерами, под угрозу будут поставлены свойства аутентичности электронных документов, неотказуемости участия человека или, наоборот, доказуемости событий, а электронная подпись будет продолжать оставаться юридически значимой и приравненной к собственноручной подписи гражданина. При этом парадоксом является тот факт, что в случаях нарушений эту подпись смогут сформировать посторонние лица, в том числе – нарушители и злоумышленники.

Полностью исключить подобные явления можно только при условии, что в автоматизированном цифровом процессе идентификации, аутентификации и авторизации будут использоваться биометрические индивидуальные параметры человека, как это происходит, например, при формировании рукописной подписи. Но для этого должны быть созданы и грамотно применены высоконадежные инновационные технологии, позволяющие автоматизировано обрабатывать биометрические параметры человека и использовать результаты вычислений в процессах идентификации, аутентификации и авторизации, выполненной в соответствии с ГОСТ Р 52633-2006.

Таким образом, результатами применения данной технологии являются**:**

– решение технологических задач внедрения биометрических параметров человека в форматы электронных сообщений, справок и цифровых документов, в том числе подписываемых ЭП;

– решение технологических задач автоматизированной обработки

биометрических параметров человека в процессах идентификации, аутентификации и авторизации;

– использование созданных современных наукоемких инновационных технологий автоматизированной обработки биометрических параметров человека в ответственных процессах высоконадежной идентификации, аутентификации и авторизации в составе инфраструктуры открытых ключей во всех процессах оказания цифровых услуг населению, предприятиям, электронному правительству.

Суть новой технологии заключается в применении обучаемых нейронных сетей в целях преобразования рукописной подписи человека и любых иных биометрических данных в заданное двоичное число большой размерности. Подпись формируется с помощью обычного цифрового пера или электронного планшета, находящихся в свободной продаже. Для снятия других биометрических данных используются другие первичные преобразователи. В качестве двоичного числа в рассматриваемых приложениях целесообразно использовать электронный формат ключевого контейнера ЭП[1].

Таким образом, принципиальным отличием, в случае применения новой технологии, будет отсутствие ключевого контейнера ЭП пользователя на каком-либо материальном носителе. Формат ключевого контейнера будет формироваться каждый раз для использования его в целях вычисления ЭП под электронным документом. Но это будет возможно только в случае корректного исполнения пользователем рукописной подписи, других биоданных, содержащих его биометрические параметры.

Таким образом, новая, вновь разработанная инновационная технология в сочетании с сертифицированными СКЗИ, позволит формировать ЭП с учетом требований действующего федерального закона №63-ФЗ «Об электронной подписи» от 06.04.2011 и ГОСТ Р 52633-2006 во всех возможных приложениях, но с использованием биометрических параметров человека (рукописная подпись, папиллярный отпечаток пальца и т.п.).

Продукт

Продукт, созданный на базе описываемой технологии, будет представлять собой программный продукт, интегрирующийся с СКЗИ, в составе инфраструктуры открытых ключей. Но только пользователи, желающие стать участниками инфраструктуры открытых ключей, вместо ключевого контейнера ЭП на материальном носителе будут получать прикладную программу на базе СКЗИ, настроенную на биометрические параметры (рукописную подпись или иные биопараметры) данного пользователя. С помощью этой программы человек сможет формировать свою индивидуальную и уникальную ЭП под любым электронным документом, с помощью его рукописной собственноручной подписи на планшете. При этом получатель электронного документа сможет убедиться в её подлинности с помощью технологий инфраструктуры открытых ключей, широко используемых в настоящее время. После положительного результата верификации подлинности ЭП под электронным документом получатель сообщения может быть уверен, что документ является подлинным, что он не изменен, не искажён. Кроме того, верифицированная ЭП является гарантом того, что этот электронный документ подписан именно тем человеком, за которого он себя выдаёт, и никем другим.

На базе описанной технологии в ОАО «ПНИЭИ» разработан Удостоверяющий центр с интегрированными технологиями биометрико-нейросетевой

[1] *В имеющихся системах инфраструктуры открытых ключей ключевой контейнер ЭП обычно хранится на каком-либо электронном носителе, например, USB-flash. При этом на пользователя налагаются дополнительные обязанности, связанные с хранением и использованием персонального носителя ключевой информации.*

идентификации пользователей. В настоящее время ведутся работы по опытной эксплуатации данного продукта в рамках системы делопроизводства предприятия.

Отличительные особенности

Предлагаемый продукт позволяет безопасно осуществлять идентификацию человека. Стойкость предлагаемого продукта к атакам физического взлома в 100 раз выше, чем у лучших обычных сейфов (5 часов у сейфов высшего класса), стойкость внутреннего программного нейросетевого контейнера хранения ключа составляет от 10^{12} до 10^{18} попыток подбора. В ручном режиме подбор займет несколько тысяч лет.

Эта новая технология в данный момент есть только в России. ОАО «ПНИЭИ» принимал непосредственное участие в разработке национального российского ГОСТ Р 52633-2006, введенного в действие с 01.04.07. Обозначенный стандарт формулирует требования по сертификации продуктов, использующих описанную технологию. За рубежом подобной технологии пока нет. Основой технологии является быстрое автоматическое обучение больших и сверхбольших искусственных нейронных сетей (на данный момент используются трехслойные нейронные сети с 416 входами и 256 выходами), которые автоматически обучаются преобразовывать рукописный пароль пользователя в его ключ шифрования или формирования ЭП. Время обучения нейронной сети не превышает 1 минуты. При воспроизведении рукописного пароля больного на 256 выходах большой нейронной сети возникает личный ключ больного. После использования ключа он уничтожается, ключ не храниться. Он появляется только после написания хозяином рукописного слова пароля и только на время шифрования или подписи электронного документа. Как следствие, пользоваться продуктом может только его хозяин, ранее обучивший ее большую нейронную сеть. Любой другой, пытающийся воспроизвести случайное слово, будет получать случайный код на выходах нейронной сети. Обученные нейронные сети можно хранить во всех компьютерах, доступных пользователю, на обычных флешках или в интернете.

Область применения

Таким образом, *одно из направлений применения продукта* - это обеспечение возможности каждого гражданина формировать ЭП под электронными документами с помощью своей собственноручной индивидуальной подписи, содержащей его уникальный биометрический параметр – динамику рукописной подписи.

В рамках данного направления могут быть решены следующие проблемные задачи:

- обеспечение криптографической защищенности, достоверной идентификации и аутентификации человека при электронных банковских платежах, при автоматизированном оформлении кредитов;
- обеспечение персонализации и криптографической защищенности конфиденциальных электронных E-mail сообщений;
- обеспечение персонализации в системах голосования со сбором голосов.

Другие возможные направления применения продукта на базе рассматриваемой технологии будут связаны с другими возможными приложениями ЭП, формируемой из биометрических параметров человека. Здесь в качестве биометрических параметров могут быть использованы кроме рукописной подписи, например, папиллярные отпечатки пальцев человека.

В рамках этих направлений могут быть решены следующие проблемные задачи обеспечения достоверной аутентификации человека без его идентификации, например, в тех случаях, когда анонимность является его правом:

- закрытое электронное голосование;
- анонимное медицинское обслуживание социально значимых больных.

Литература:

1. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

2. Фунтиков В.А., Назаров И.Г., Бурушкин А.А. Национальные стандарты России: конфиденциальность персональных биометрических данных. «Стандарты и качество» № 7, 2010 г. с. 28-33.

3. Язов Ю.К., Волчихин В.И., Фунтиков В.А., Иванов А.И., Назаров И.Г. Нейросетевая защита персональных биометрических данных. М.: Радиотехника. 2012 г., 160 с.

4. Ашенбренер И.В., Иванов А.И., Рыбалкин С.Б. Нейросетевое обезличивание медицинского документооборота – эффективный прием биометрической защиты песональных данных. «Нейрокомпьютеры: разработка, применение» №12, 2007, с.80-82.

5. Буханик А.А., Рыбалкин С.Б., Секретов М.В. Биометрико-нейросетевое обезличивание пациентов при первичном анонимном обращении в медучреждение «Нейрокомпьютеры: разработка, применение» №3, 2012 с. 70-73

Материалы поступили 23.11.2012, опубликовано в Интернет 12.12.2012 по положительной рецензии д.т.н., профессора Малыгина А.Ю. (Пенза).