АВТОМАТИКА. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 004.7.056 *МРНТИ 50.37.23*

БИОМЕТРИЧЕСКИЕ УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ ШАГОВОЙ ДОСТУПНОСТИ[1]

***Б. С. Ахметов*[1]**, д.т.н., проф., ***А. И. Иванов*[2]**, д.т.н., доцент,
***С. Е. Трифонов*[2]**, к.т.н., доцент

Казахский национальный технический университет
им. К. И. Сатпаева[1]

Пензенский научно-исследовательский электротехнический институт[2]

Показано, что демократия создаваемого в России и Казахстане информационного общества может быть обеспечена только, если будет поддерживаться конфиденциальность, обезличенность или анонимность персональных данных человека при его высоконадежной биометрико-криптографической авторизации в открытых информационных пространствах. Одним из путей достижения этого является создание сети биометрических удостоверяющих центров шаговой доступности, имеющих оборудование, удовлетворяющее требованиям пакета стандартов ГОСТ Р 52633.хх.хх.
Ключевые слова: биометрический образ, преобразователь биометрия-код, конфиденциальность, анонимность, обезличенность персональных биометрических данных.

Ресей мен Қазақстандағы ақпараттық қоғамда құрылған демократия - егер жеке адамның құпиялылық, бөгделенген немесе анонимді (жасырын) мәліметтері оның ашық ақпараттық кеңістікте сенімділігі жоғары биометрикалық-криптографиялық авторландыруында қолдауға ие болса ғана қамтамасыз етіле алатыны көрсетілген. Бұған қол жеткізудің бірден-бір жолы, МемСТ Р 52633.хх.хх. стандарт пакеттерінің талабына сәйкес қанағаттандыратын жабдықтары бар биометриялық қадам қатынасының куәлік орталықтары желісін құру болып табылады.
Түйінді сөздер: Биометриялық бейне, биометрия-код түрлендірушісі, құпиялылық, жасырындық, жеке биометриялық деректердің бөгделенуі.

*Статья подготовлена в рамках выполнения комплексного проекта «Разработка и подготовка производства телекоммуникационного оборудования, разработка программного сетевого, прикладного и специального обеспечения для создания цифровых сетей связи с персонализированным доступом» в соответствии с Постановлением Правительства № 218 от 09.04.2010 г.

It was shown that democracy of the information society, created in Russia and Kazakhstan can be provided only if confidentiality, impersonality or anonymity of the personal data is supported at its highly reliable biometric-cryptographic authorization in open information fields. One of the ways of its achievement is creation of a network of the biometric identifying centers of the stepwise accessibility having the equipment meeting Standards requirements of GOST P 52633.xx.xx.
Key words: Biometric image, biometrics-code converter, confidentiality, anonymity, impersonality of the personal biometric data.

В настоящее время активно идут процессы информатизации России и Казахстана. Создается информационное общество, разрабатываются электронные правительства двух государств, развивается система электронных услуг органов региональной и муниципальной власти, активно создаются электронные витрины предприятий, происходит интеллектуализация городов, обсуждаются проблемы создания интеллектуального дома.

Одной их базовых технологий создания информационного общества является технология электронной цифровой подписи под электронным документом. Сегодня эта технология строится на асимметричной криптографии (используется пара из открытого и личного ключа), базирующаяся на системе удостоверяющих центров, выдающих сертификаты открытых ключей. Казалось бы, что удостоверяющие центры – это вполне коммерциализируемые проекты, однако это далеко не так. На сегодня нет коммерчески успешных удостоверяющих центров, все они убыточны. Их убыточность обусловлена тем, что они не повышают информационную безопасность рядового пользователя, а наоборот, снижают ее (создают дополнительную угрозу компрометации личного ключа). Бизнес-модель современных удостоверяющих центров ущербна, так как они пытаются продавать дополнительные риски, связанные с массовым использованием ЭЦП, личных ключей, асимметричной криптографии. Криптография надежна только, если секрет личного ключа надежно хранится и транспортируется. Личный ключ используется только в доверенной вычислительной среде и не может быть скомпрометирован.

Обычный пользователь не может обеспечить надежное хранение своего личного ключа и его применение только в доверенной вычислительной среде. В связи с этим демократическое информационное общество должно обеспечить своих граждан надежными хранителями их личных ключей и доверенной вычислительной средой для их применения.

Технологии высоконадежной биометрико-криптографической авторизации личности

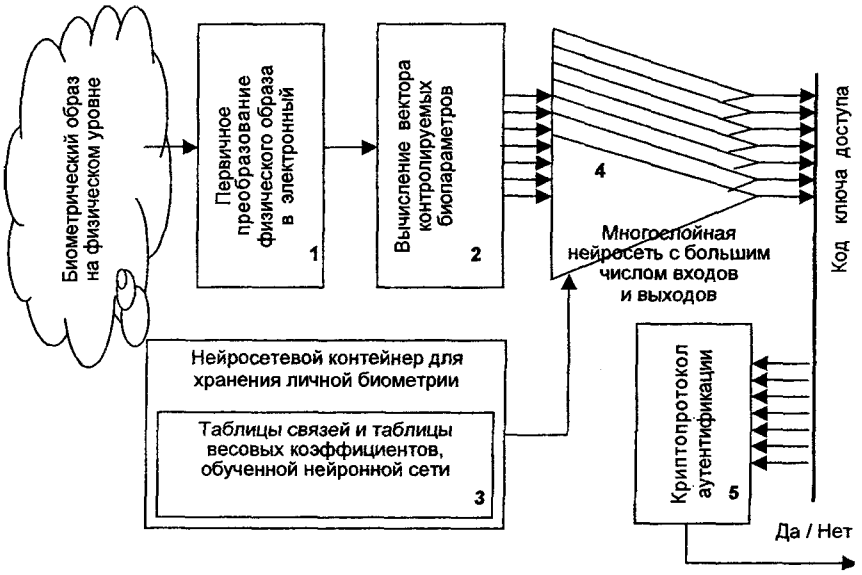
США, страны НАТО, а также Россия, Казахстан и Беларусь активно развивают биометрические технологии. США и страны НАТО значительные усилия прилагают к созданию средств коллективной биометрии. Основным постулатом подобных средств является изъятие у пользователя части его биометрии, например, в виде рисунка отпечатка пальца, цифровой 2D или 3D фотографии, рисунка радужной оболочки глаза. На базе этих данных формируется биометрический шаблон, который подписывается ЭЦП и публикуется (хранится) в системе биометрической идентификации личности [1,2].

Шифровать биометрический шаблон нельзя, так как он должен использоваться системой идентификации. Этот подход к решению задачи потенциально опасен из-за угрозы утраты базы биометрических шаблонов. Однако он вполне приемлем для полицейских приложений паспортно-визового контроля и приложений корпоративного биометрического ограничения доступа.

Для исключения угрозы компрометации биометрических шаблонов необходимо создавать новые биометрические технологии, которые, с одной стороны, позволяют надежно (высоконадежно) аутентифицировать человека по его биометрии, а с другой стороны, делают биометрию человека недоступной для наблюдения и понимания. Лидерами по созданию этих новых биометрических технологий являются Россия, Казахстан и Беларусь. На данный момент результаты усилий этих стран СНГ оформлены в виде пакета из нескольких национальных стандартов России с номерами ГОСТ Р 52633.xx.xx, которые в ближайшее время будут переводиться в ранг межгосударственных стандартов стран СНГ (аналогов этих стандартов у стран НАТО пока нет) [3,4].

Принципиальным отличием средств высоконадежной биометрии является то, что биометрические образы людей не публикуются, технология строится на сохранении биометрии человека в тайне. Для этой цели приходится менять структурную схему средств биометрической аутентификации личности. Новая схема приведена на рисунке.

Средства обычной биометрии не могут обеспечить тайну используемого биометрического образа и соответственно не могут быть надежными. Средства, выполненные по блок-схеме рисунка, являются высоконадежными, так как построены на применении нейросетевого преобразователя биометрия-код (блок 3 и блок 4).



Типовая блок-схема организации средств высоконадежной биометрической аутентификации

Нейросетевой преобразователь биометрия-код (блок 3 и блок 4) по ГОСТ Р 52633.0 должен быть заранее обучен преобразовывать тайный биометрический образ «Свой» в личный ключ пользователя. Любой иной биометрический образ «Чужой» нейросетевой преобразователь биометрия-код должен преобразо-

вывать в случайный ключ. Если личный ключ и биометрический образ «Свой» неизвестен стороннему наблюдателю, то подобрать его злоумышленник может после 1 000 000 000 попыток (стойкость к атакам подбора 10^9) степени. На подбор у злоумышленника должно уходить $3 \cdot 10^9$ с, или примерно 300 лет, если злоумышленнику разрешено предъявлять один из случайных биометрических образов в трехсекундный интервал времени.

Если биометрический образ человека оказывается скомпрометированным, то его остаточная стойкость к атакам подбора падает до величины 10^3 попыток (время подбора сокращается до 1 ч). Обеспечение тайны биометрии намного эффективнее самой биометрии.

Тайна биометрии при использовании блок-схемы обеспечивается за счет того, что по таблицам связей обученной нейронной сети и таблицам весовых коэффициентов восстановить биометрический образ человека (найти человека по базе биометрических образов) технически крайне сложно. Конфиденциальность биометрии, размещенной в нейросетевом контейнере, обеспечивается на уровне, сопоставимом с конфиденциальностью, обеспечиваемой шифрованием.

Обучение нейросетевых преобразователей биометрия-код в доверенной вычислительной среде биометрического удостоверяющего центра

По требованиям ГОСТ Р 52633.0-2006 и ГОСТ Р 52633.5-2011 обучение преобразователя биометрия-код должно осуществляться автоматически. При обучении используются от 12 до 21 примера биометрического образа «Свой», а также порядка 256 случайных биометрических образов «Чужой». Обучение нейросетевого преобразователя биометрия-код следует осуществлять только в доверенной вычислительной среде, предоставляемой биометрическим удостоверяющим центром.

Перед обучением пользователь генерирует для себя пару из открытого и личного ключа. Нейросетевой преобразователь биометрия-код может быть обучен на открытом биометрическом образе человека и его открытом ключе. Эта технология по-

зволяет третьим лицам проводить биометрическую идентификацию личности человека, имея его электронное удостоверение личности (аналог сертификата открытого ключа). Электронное удостоверение личности должно иметь в своем составе не только открытый ключ человека, но и его нейросетевой контейнер с размещенным в нем открытым биометрическим образом.

Кроме того, биометрический удостоверяющий центр создает нейросетевой преобразователь биометрия-код, связывающий тайный биометрический образ человека (например, рукописный пароль) с его личным ключом. Это позволяет человеку безопасно формировать свою ЭЦП в его личной доверенной вычислительной среде или в доверенной вычислительной среде биометрического удостоверяющего центра (терминала биометрического удостоверяющего центра).

При своей регистрации в биометрическом удостоверяющем центре пользователь предоставляет свои персональные данные, которые далее шифруются на его личном ключе и открытом ключе гаранта конфиденциальности (анонимности, обезличенности).

Институт гарантов сохранения конфиденциальности, анонимности, обезличенности персональных биометрических данных

В связи с тем, что биометрический удостоверяющий центр является коммерческой организацией, предоставляющей доверенную вычислительную среду и сертификаты открытых ключей пользователь не должен доверять ему хранение своей тайной биометрии. Исключение возможных злоупотреблений со стороны персонала биометрического удостоверяющего центра обеспечивается привлечением внешних гарантов анонимности (конфиденциальности, обезличенности). Гаранта конфиденциальности (анонимности, обезличенности) своей биометрии и других персональных данных пользователь выбирает сам [5]. Гарантом может быть любое лицо, согласившееся выполнять эту функцию и имеющее сертификат открытого ключа.

Если требуется сохранить конфиденциальность, аноним-

ность, обезличенность персональных данных человека, они шифруются на открытом ключе гаранта и личном ключе пользователя. Далее этот шифротекст хранится в биометрическом удостоверяющем центре в связке с открытым ключом донора биометрии. Персонал биометрического удостоверяющего центра не может расшифровать персональные данные, так как не обладает личным ключом гаранта анонимности и своего клиента.

Если требуется дезавуировать конфиденциальность (обезличенность, анонимность) биометрии и персональных данных человека помимо его воли, то правоохранительные органы должны обратиться в биометрический удостоверяющий центр и получить шифротекст биометрии и персональных данных. Далее они должны обратиться к гаранту конфиденциальности (обезличенности, анонимности), который, пользуясь своим личным ключом, способен расшифровать персональные данные.

Гарант анонимности (конфиденциальности, обезличенности) не способен злоупотребить своим положением, так как не обладает шифротекстом персональных данных. Он получает шифротекст только при обращении к нему правоохранительных органов или биометрического удостоверяющего центра.

Таким образом, биометрические удостоверяющие центры имеют намного более жизнеспособную бизнес-модель. Они не пытаются продавать дополнительные риски. Биометрические УС предоставляют пользователям дополнительно электронные удостоверения личности, свою доверенную вычислительную среду (например, в виде выносных терминалов дистанционной биометрической аутентификации). Опираясь на услуги биометрических УС, рядовые пользователи оказываются способны обеспечивать свою анонимность при электронном голосовании или обезличенность ведения своих историй болезни. Из-за роста объемов услуг биометрические УС оказываются способны снизить свои расценки до микроплатежей и полностью снять угрозу компрометации тайных биометрических образов гражданина в связке с его личными ключами.

Электронное правительство и электронный бизнес в лице биометрических удостоверяющих центров фактически имеет посредника, специализирующегося не предоставлении безопас-

ных криптографических и биометрических услуг гражданам информационного общества. Микроплатежи за предоставление этих услуг возникают в связи с тем, что затраты на поддержание работоспособной доверенной вычислительной среды и высоконадежной биометрии перекладываются на всех пользователей биометрических УС. Новая бизнес-модель становится работоспособной, если биометрические УС или его терминалы оказывается в шаговой доступности.

Литература

1. *Болл Руд* и др. Руководство по биометрии / Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Эндрю У. - М.: Техносфера, 2007. - 368 с.

2. *Волчихин В. И., Ахметов Б. С., Иванов А. И.* Преимущества биометрико-нейросетевого хранения конфиденциальной информации мобильного пользователя // Вестник КазНТУ. - 2011. - № 3. - С. 173-178.

3. *Волчихин В. И., Иванов А. И., Фунтиков В. А.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. - Пенза: Пензенский гос. ун-т, 2005. - 273 с.

4. *Фунтиков В. А., Назаров И. Г., Бурушкин А. А.* Национальные стандарты России: конфиденциальность персональных биометрических данных // Стандарты и качество. - 2010. - № 7. - С. 28-33.

5. Пат. 2371765 Российская Федерация. Способ анонимной биометрической регистрации человека / Иванов А.И. - № 2008101520/09; заявл. 14.01.2008; опубл. 27.10.2009.