СТАТЬИ

Почему так важна тайна биометрических образов и как необходимо хранить свой личный ключ формирования ЭЦП

Иванов А.И.

Почему так важна тайна биометрии защищаемого человека?

В 2007 году в России вышла монография с крайне претенциозным названием «Руководство по биометрии» [1], в ней группа авторов из США излагает основы биометрии (классику). В этой монографии есть почти все кроме, тайны биометрии. Американская биометрическая школа, одна из самых сильных, США потратили на биометрию больше, чем все другие вместе взятые страны. По сути дела монография [1] может рассматриваться, как попытка обобщить имеющийся на 2004 год у исследователей США научно-технический опыт.

В российской биометрии иные подходы и иные традиции [2]. Коренным отличием российского и американского подходов является то, что в русскоязычной литературе принято делить биометрию на открытую и тайную. Причина здесь крайне проста: Россия вынуждена была тратить в сотни раз меньше на свою биометрию в сравнении с США и в то же время ставила перед собой задачу иметь эффективную биометрическую защиту. Единственный путь, который позволяет добиться высокой эффективности биометрии – это перейти к использованию тайных биометрических образов.

Покажем на сколько эффективен может быть переход от использования открытого биометрического образа к тайному биометрическому образу. В качестве примера будем рассматривать идентификацию человека по его открытому автографу, обычно воспроизводимому людьми под документом. Сегодня производители систем идентификации человека по его автографу заявляют их стойкость к атаке подбора на уровне 10 000 попыток подделки. Это означает, что система сможет выявить попытку подделки с вероятностью 0.9999. Кажется, что такая вероятность выявления подделки достаточно высока и снимает множество проблем, однако это далеко не так.

Проблемы снимаются только в том случае, когда владелец автографа воспроизводит его в присутствии проверяющего (например, в присутствии служащего банка). Если служащий банка не видит процесс воспроизведения автографа, то вполне вероятна его подмена на уже имеющуюся на документе подпись. Автограф является автографом, если он воспроизведен в присутствии проверяющего и похож на авторский оригинал, уже имеющийся у проверяющего.

В том случае, если проверяемый человек недоступен для его прямого контроля (например, находится далеко от проверяющего) биометрия должна быть очень надежна (высоконадежна). Обеспечить резкое повышение надежности может только тайна используемого при идентификации биометрического образа. Нужно сделать так, что бы никто не знал Ваш биометрический образ. В место вашего автографа, который известен всем, Вам нужно использовать парольное рукописное слово. Если такое слово будет состоять из 5 букв русского языка, то стойкость самого пароля составит $(64)^5 \approx 10^9$. Стойкость обычного пароля оказывается на 6 порядков (в миллион раз) выше стойкости к атакам подбора открытого биометрического образа.

Если пароль сделать биометрическим и потребовать писать его почерком проверяемого человека, то его стойкость к атакам подбора еще раз резко увеличивается. Предположим, что биометрическая система способна различать между собой 100 индивидуальных почерков, тогда стойкость биометрического пароля составит $(6400)^5 \approx 10^{19}$. Происходит скачек повышения стойкости еще на 10 порядков (в 10 миллиардов раз).

Получается, что тайна биометрического образа в миллиарды раз сильнее самой биометрии. Так же как в криптографии все построено на тайне криптографического ключа, в высоконадежной биометрии все построено на тайне биометрического образа. Если тайна биометрического образа не обеспечена, то говорить о сильной или высоконадежной биометрии нельзя. Биометрия открытых образов всегда будет слабой вне зависимости от технических ухищрений. Если

злоумышленник знает биометрический образ, то он рано или поздно найдет способ изготовления его муляжа.

В связи с вышеизложенным, основная классификация биометрических образов – это их деление на открытые и тайные. Именно эта классификация является основной. Часто используемая классификация биометрических образов по технологии снятия биометрических данных являются вторичной и не очень существенно влияет на конечный результат. Принципиальным является то, что любой биометрический образ может быть сделан тайным. Если биометрический образ динамический (голос или рукописный почерк) сделать его тайным крайне просто, достаточно никому не рассказывать о своем рукописном или голосовом пароле. Статические биометрические образы (рисунок отпечатка пальца, трехмерная геометрия лица, форма уха, ДНК, рисунок радужной оболочки глаза, геометрия кровеносных сосудов глазного дна или руки) сделать тайными гораздо сложнее, но вполне возможно.

Естественно, что человек не может по своему желанию изменить рисунок своего отпечатка пальца, однако в большой системе человека можно сделать анонимным, а данные отпечатка пальца могут быть сделаны изменяющимися при каждом сеансе аутентификации. В этом случае внешний наблюдатель (например, Интернет провайдер) не может узнать, что за биометрический образ использован и кто его хозяин. Обеспечивая анонимность человека в больших информационных системах, мы создаем условия, для того, что бы использовать его статические биометрические образы как тайные. Естественно, что это может быть сделано только в больших и сверхбольших информационных системах. В малых информационных системах с ограниченным числом пользователей, да еще и локально расположенных использовать рисунки отпечатков пальцев, как тайные биометрические образы нельзя.

При каждом сеансе аутентификации человек оставляет следы своих пальцев на датчике съема биометрии, на клавиатуре, на компьютере,…. Если злоумышленник знает с какого компьютера была осуществлена аутентификация, то он может собрать следы отпечатков пальцев своей будущей жертвы. Как только, тайный биометрический образ человека частично или полностью скомпрометирован, высоконадежная биометрическая защита перестает быть высоконадежной.

Для скомпрометированного биометрического образа следует использовать такой параметр как остаточная стойкость к атакам подбора. Для рассматриваемого выше примера рукописного пароля из 5 букв его полная стойкость к атакам подбора может составлять до 10^{19} попыток, однако если рукописный образ слова-пароля скомпрометирован (злоумышленник увидел какое слово вы пишете), то остаточная стойкость будет составлять не более чем 1000 или 10 000 попыток. Утрата биометрической тайны приводит к катастрофическому снижению стойкости биометрической защиты.

В этом отношении американцы [1] лукавят, когда начинают обсуждать достоинства своих биометрических продуктов, построенных на анализе рисунков отпечатков пальцев. Стойкость к атакам подбора рисунка отпечатка пальца может составить 10 000 000 попыток только при условии обеспечения анонимности его владельца. Если анонимность человека системой не обеспечена, то отпечаток пальца следует считать открытым биометрическим образом, а его остаточная стойкость к атакам подбора не может быть высокой. Заметим, что в монографии [1], нет раздела по обеспечению анонимности пользователей. То есть наши американские коллеги нас Всех просто разводят по поводу качества предлагаемой ими биометрической защиты. Все это касается не только монографии [1], для создания системы паспортно-визового биометрического контроля были разработаны десятки стандартов, которые изначально создавались как национальные биометрические стандарты США. Все эти стандарты грешат тем же, что и монография [1], они решают только одну задачу полицейского контроля граждан. Естественно, что обеспечение анонимности граждан, обезличенности и конфиденциальности их биометрии для решения полицейских задач не нужны.

Почему каждому из нас понадобится доверенная вычислительная среда?

То, что тайна биометрического образа сильна и эффективна я попытался обосновать в предыдущем параграфе. Там же показано, что компрометация тайной биометрии приводит к

катастрофическому снижению, обеспечиваемого ею уровня информационной безопасности. В связи с этим высоконадежные биометрические системы должны изначально строиться таким образом, что бы обеспечивать сохранение биометрической тайны при практическом использовании биометрии.

Анализ технологии высоконадежной биометрической аутентификации, показывает, что для сохранения тайны биометрического образа пользователь должен иметь свою личную доверенную вычислительную среду [3, 4]. Одной из основных проблем является проблема перехвата тайного биометрического образа при его вводе в доверенную вычислительную среду. Для того, что бы исключить перехват биометрии придется личную доверенную вычислительную среду физически совместить со сканером биометрии. Наиболее просто эту концепцию удается пояснить на примере доверенного цифрового пера. Структура такого цифрового пера приведена на рисунке 1.

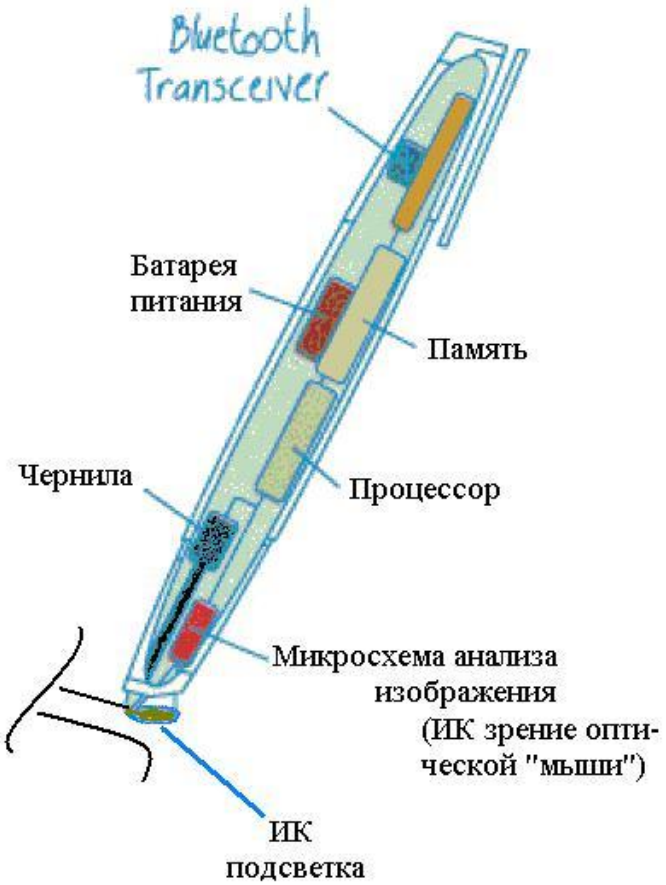


Рис. 1. Цифровое перо с доверенной вычислительной средой для формирования электронной цифровой подписи

Из рисунка 1 видно, что доверенное цифровое перо имеет инфракрасную подсветку подстилающей поверхности и микросхему ИК зрения оптической «мыши». То есть цифровое перо можно рассматривать как доверенную оптическую мышку, выполненную в виде цифрового пера. При письме таким пером ее процессор запоминает движения руки, формирующие рукописный текст. То есть таким пером можно писать на обычной бумаге и в нутрии него будет формироваться, воспроизведенный на бумаге рукописный текст. На этом принципе начиная с 2005 года ряд фирм создали подобные устройства и они заняли свое место на рынке. На рисунке 2 приведен внешний вид цифровых перьев созданных тремя разными фирмами.

Рис. 2. Внешний вид «цифровых перьев» трех фирм: HP, Logitech, Nokia

Объем продаж цифровых перьев пока невелик. Это скорее всего связано с тем, что мы все отучились писать рукописные тексты. Клавиатура стала для многих из нас привычнее обыкновенной ручки. Тем не менее, такие цифровые перья должны стать востребованными, если они начнут играть роль доверенной вычислительной среды, где выполняются потенциально опасные биометрико-криптографические операции.

Одной из потенциально опасных криптографических операций является формирование юридически значимой электронной цифровой подписи (ЭЦП) под цифровым документом. Опасность формирования ЭЦП связана с тем, что необходимо использовать личный (секретный) ключ. Если формировать Вашу личную ЭЦП в чужом компьютере, то Ваш личный (секретный) ключ может быть перехвачен. То есть формировать Вашу ЭЦП следует только в Вашей личной доверенной вычислительной среде, которую Ваш личный ключ не покидает.

Доверенная вычислительная среда, например, может быть выполнена цифрового пера. Структурная блок-схема цифрового пера, осуществляющего формирование ЭЦП приведена на рисунке 3. Программное обеспечение цифрового пера организовано таким образом, что в память цифрового пера можно загрузить пока не подписанный цифровой документ по интерфейсу Bluetooht и дать команду на подпись этого документа. При этом подписать цифровой документ программное обеспечение не может, так как в нем нет личного ключа владельца ЭЦП. В памяти доверенной вычислительной среды находится нейросеть, обученная преобразовывать рукописный биометрический образ «Свой» в код контейнера с личным ключом владельца ЭЦП. Для того, что бы извлечь личный ключ пользователю необходимо цифровой ручкой воспроизвести известное ему слово-пароль. Пример использования рукописного слова «Пенза» в качестве биометрического пароля отображен на рисунке 4.

Если обладатель цифрового пера действительно является его хозяином, то он без особого труда воспроизведет рукописный пароль своим личным почерком, а нейронная сеть превратит его в код контейнера с личным ключом. Если цифровое перо оказалось в чужих руках, то «Чужой» будет пытаться воспроизвести случайные рукописные слова, соответственно, нейронная сеть будет выдавать на своих выходах случайные коды.

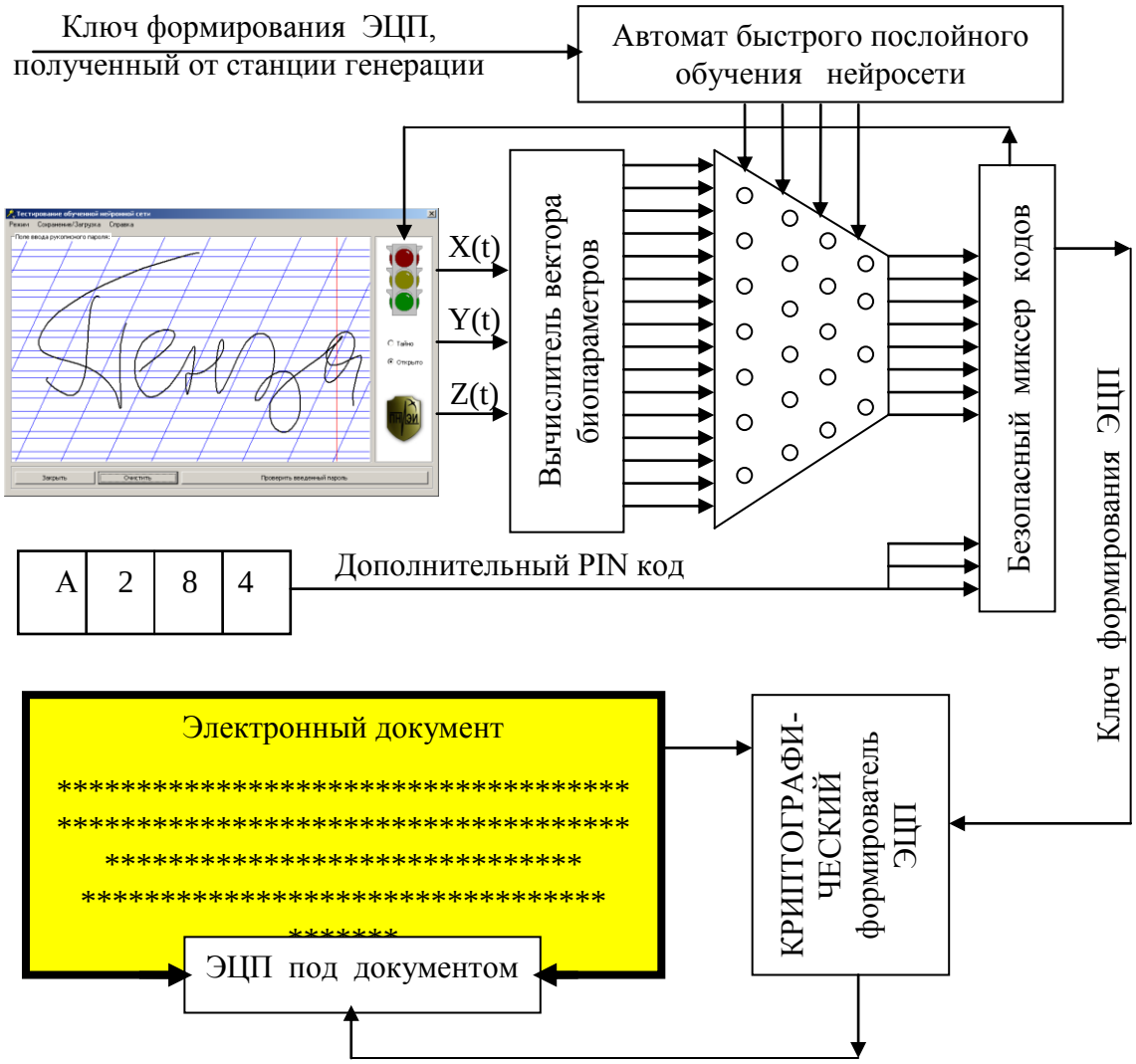


Рис. 3. Структурная блок-схема цифрового пера, способного осуществлять формирование ЭЦП с доступом к контейнеру с личным ключом пользователя через высоконадежную рукописную биометрию

Получается, что только пользователь «Свой» может получить верный код контейнера с ключом. Для того, что бы раскрыть контейнер и извлечь из него свой личный ключ пользователь должен набрать дополнительно свой ПИН код (это стандартный прием защиты, когда контейнер закрывается ПИН кодом пользователя). Личный ключ пользователя верно извлеченный из правильного кода контейнера уже может быть использован для формирования ЭЦП по указанным документом. Саму ЭЦП под цифровым документом далее проверяют обычным способом по открытому ключу. Если ЭЦП верна, то процедура формирования ЭЦП выполнена правильно. Любая ошибка ПИН кода или ошибка при воспроизведении рукописного слова пароля приводит к неверному формированию ЭЦП. Проверка ЭЦП осуществляется уже вне цифрового пера в не доверенной вычислительной среде, операции с сертификатом открытого ключа относительно безопасны.

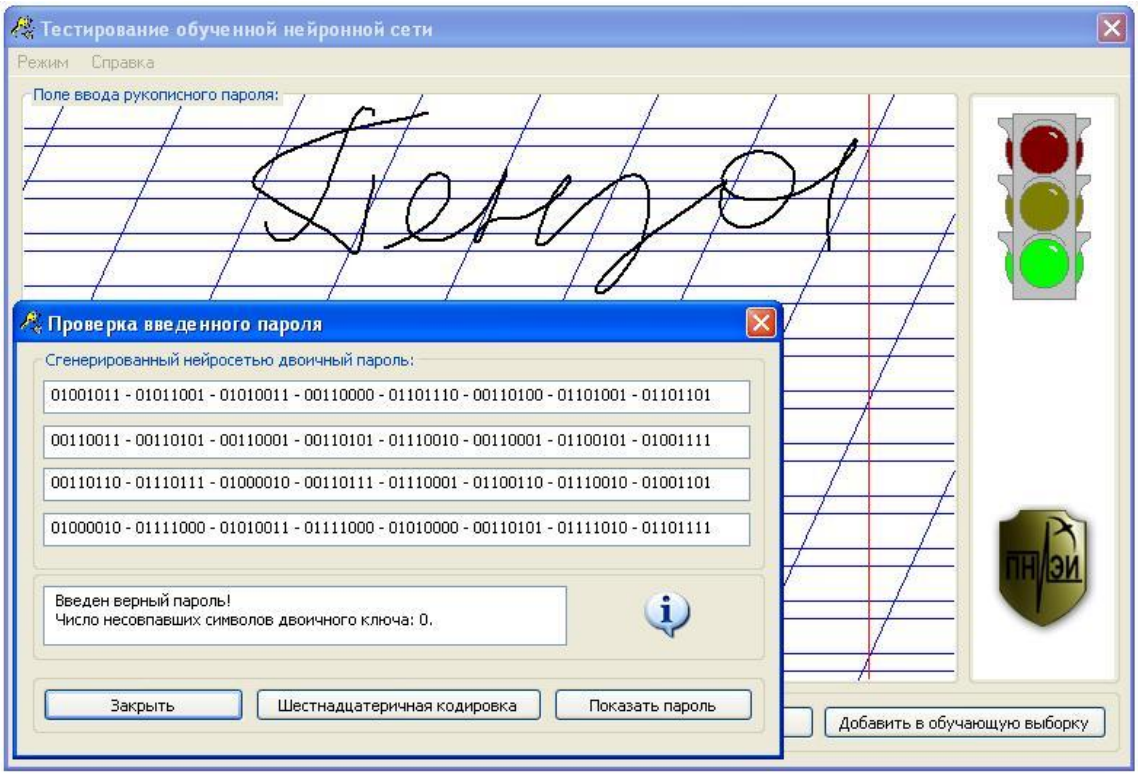


Рис. 4. Пример нейросетевого связывания рукописного слова пароля «*Пенза*» с контейнером личного ключа пользователя длинной 256 бит

Принципиально важным моментом при проектировании доверенного цифрового пера является то, что его внутреннее программное обеспечение делают недоступным для внешнего воздействия. То есть по внешнему интерфейсу Bluetooht можно только загружать цифровые документы на подпись и выгружать уже подписанные цифровые документы. Добраться до нейросети или формирователя ЭЦП внешнее программное обеспечение не может (физически сожжены перемычки доступа). Для того, что бы добраться до внутреннего программного обеспечения цифрового пера нужно сошлифовывать некоторые фрагменты микросхемы процессора. Это крайне сложно сделать, если микросхема выполнена в защищенном варианте. Тогда попытки сишлифовывания приведут к уничтожению внутреннего доверенного программного обеспечения.

Высокая надежность доверенной вычислительной среды, выполненной в форме цифрового пера, обусловлена тем, что для его вскрытия квалификации обычного «медвежатника» не хватает. Если вы храните свой личный ключ в обычном сейфе 1-го класса стойкости, то медвежатник доберется до ключа через 1 час. Для того, что бы добраться до вашего личного ключа в цифровом пере потребуется «карманник» или «домушник», при этом он должен физически доставить похищенное цифровое перо в центр, обладающий оборудованием для сошлифовывания нужных участков микросхемы. Само послойное сошлифовывание микросхемы является очень медленным и очень дорогим процессом. Для того, что бы добраться до доверенного программного обеспечения цифрового пера потребуется примерно 500 часов высоквалифицированного труда на уникальном оборудовании. То есть физическая защита цифрового пера оказывается примерно в 500 раз надежнее физической защиты обычных сейфов. При этом габариты и вес цифрового пера оказываются в 10 000 раз меньше, чем у сейфа, а стоимость в 50 раз ниже.

В дополнение следует подчеркнуть, что преодоление физической защиты цифрового пера – это только малая часть затрат времени необходимого на атаку компрометации Вашего личного (секретного) ключа. Из доверенного программного обеспечения цифрового пера далее потребуется извлечь параметры нейросети, далее из параметров нейросети нужно будет извлечь ключ или образ биометрического рукописного пароля. Если биометрико-нейросетевая и биометрико-криптографическая защита ключа выполнены правильно, то на извлечение личного ключа из программного обеспечения цифрового пера потребуется еще примерно 500 суток (при наличии у злоумышленников высокопроизводительной вычислительной машины взлома).

В свою очередь пользователь, обнаруживший пропажу своего цифрового пера должен обратиться в удостоверяющий центр, выдавший ему сертификат открытого ключа и аннулировать свой сертификат открытого ключа. При аннулировании сертификата открытого ключа его парный секретный ключ утрачивает свои юридические полномочия. На аннулирование действующего сертификата открытого ключа потребуется несколько минут.

ЛИТЕРАТУРА:

1. Болл Руд и др. Руководство по биометрии. / Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Сеньор Эндрю У. // Москва: Техносфера, 2007. -368 с.
2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
3. Патент RU 2365047, заявка № 2007120788/09(022642) авторов Иванова А.И., Фунтикова В.А. «Способ формирования электронных документов и устройство для его реализации», приоритет от 04.06.2007.
4. Патент RU 2355307, заявка № 2007118896/09(020584) авторов Иванова А.И., Фунтикова Д.А. «Способ аутентификации личности по рисунку отпечатка пальца и устройство для его реализации», приоритет от 21.05.2007.

Дружественный биометрико-нейросетевой формирователь ЭЦП служащего с высоконадежной степенью авторизации

Статья журнала «Специальная техника средств связи»
В.А. Фунтиков, А.И. Иванов, В.В. Федулаев, О.В. Ефимов

В настоящее время идут активные процессы информатизации современного общества. Одним из его направлений является использование биометрических технологий аутентификации личности. Современная биометрическая аутентификация личности [2] позволяет передать от людей искусственному нейросетевому интеллекту способность с высокой надежностью узнавать конкретного человека. Особую важность биометрические технологии идентификации получают в связи с введением в ближайшем будущем нового поколения загранпаспортов и визовых документов. С этой целью в ближайшее время должно быть подготовлено несколько десятков международных биометрических стандартов. Более 37 международных стандарта касаются различных особенностей биометрии. Они описывают то, как нужно снимать, хранить, обрабатывать: отпечатки пальцев, изображения лица, рукописные образы. Целый ряд международных стандартов посвящается вопросам тестирования биометрических устройств и технологий. Практически все страны, имеющие значимый национальный научно-технический потенциал пытаются решать эти задачи. Лидерами технологий защиты информации являются две страны – Россия и США.

США идут по пути использования нечеткой математики [3], ученые этой страны предлагают мировому сообществу специализированные «fuzzy» обогатители (экстракторы) превращающие бедную неоднозначную размытую биометрическую информацию в сильный личный ключ пользователя.

В настоящее время мировое сообщество, ведомое США, в лице международного комитета по стандартизации ISO/IEC JTC1 SC37 разрабатывает порядка 30 биометрических стандартов, регламентирующих требования к биометрическим фрагментам нового поколения паспортно-визовых документов. Все эти стандарты ориентированы на использование относительно слабых классических решающих правил с окончательной формализацией решения в форме «последнего» бита ДА/НЕТ. Из-за слабости биометрии с классическими решающими правилами она не предназначена для работы в полностью автоматическом режиме. Все международные биометрические стандарты ориентированы на то, что соответствующая система полуавтоматической биометрической идентификации человека работают под управлением контролирующего их человека. Контролирующий должен убедиться в том, что проверяемый правильно предъявляет биометрический образ «Свой» и если автомат ошибся, то контролирующий человек в праве отменить решение автомата. Данное обстоятельство порождает целый ряд проблем: контролирующий человек может отвлечься, проверяемый («Чужой») пытаться списать отрицательный результат на ошибку автомата и т.д.

В связи с принятой выше идеологией для систем с относительно слабой биометрии не предусмотрено их экспресс тестирование после каждого обучения. По умолчанию предполагается, что общего тестирования системы достаточно [5-9]. Эти стандарты нельзя использовать для дистанционной биометрической идентификации человека, например, через Интернет.

Для того, что бы обеспечить высоконадежную дистанционную идентификацию человека необходимо привлекать биометрические технологии способные безопасно взаимодействовать с криптографическими механизмами. Положение резко меняется при переходе к использованию средств полностью автоматической высоконадежной биометрической аутентификации.

Россия предлагает мировому сообществу иной путь использования больших и сверхбольших искусственных нейронных сетей, которые заранее обучаются преобразовывать размытые биометрические данные пользователя в его личный криптографический ключ. Теория создания подобных преобразователей биометрия/код [2] позволяет надеяться на их высокую стойкость по отношению к атакам подбора и попыткам изучения. Правильно построенный преобразователь биометрия/код ведет себя как классическая необратимая хэш-функция.

Случайные входные биометрические образы нейросетевой преобразователь биометрия/код перемешивает (хэширует), а заранее известное множество нечетких образов «Свой» преобразователь свертывает в единственное значение личного криптографического ключа. При этом достаточно сложная нейронная сеть с 256 выходами позволяет обеспечивать стойкость к атакам случайного подбора на уровне 10^{22} (22 степень) попыток.

Предполагается, что уже в очень близком будущем электронный документооборот получит широкое распространение. Как следствие повсеместно станет использоваться электронная цифровая подпись (ЭЦП).

Необходимо подчеркнуть, что по мере дальнейшей информатизации и развития современного общества проблемы его информационной безопасности будут только усиливаться. В частности, по прогнозам специалистов, уже в ближайшее время, обществом будет ощущаться проблема «цифрового неравенства» граждан. Проблему “цифрового неравенства” можно рассматривать в нескольких аспектах. Интересно, что в Европейских странах не рассматриваются глубинные аспекты этого явления, говорится только о доступности Интернета для широких слоёв населения, о возможности голосовать, не выходя из дома и тому подобных вещах. Однако, реальное “цифровое равенство” это не только свободный доступ в Интернет, но и равные цифровые права всех членов общества.

Например, если рассматривать цифровые права банкира и домохозяйки, то юридически они равны, однако практически это далеко не так. Доверие к электронной цифровой подписи банкира намного выше доверия к ЭЦП домохозяйки. Это связано с тем, что у банкира есть сейф, охрана, таким образом, он может обеспечить надежное хранение своего личного криптографического ключа, формирующего электронную цифровую подпись электронного документа. Да и сам статус, опыт и ответственность банкира намного выше, чем у домохозяйки. В отличие от банкира, ключ формирования ЭЦП которого всегда хранится в сейфе, домохозяйка не может себе этого позволить. Её ключ формирования ЭЦП, скорее всего, будет храниться в сумочке, что автоматически ставит домохозяйку в более уязвимое положение.

Именно это обстоятельство и называется действительным “цифровым неравенством”, когда декларированная для всех одинаковая юридическая значимость электронной цифровой подписи на деле будет иметь разный уровень доверия.

Рассмотрим возможные способы решения данной задачи.

Итак, мы подошли к необходимости широкого использования механизма электронной цифровой подписи для документального подтверждения/проверки авторства (целостности) электронного документа, а так же для надежной дистанционной взаимной аутентификации пользователей в открытом информационном пространстве. Одной из основных проблем использования криптографических механизмов является необходимость обеспечить надежное хранение криптографических ключей. Особенно эта проблема обостряется для мобильных пользователей, физически оторванных от контролируемой территории с сейфами и другими организационно техническими мероприятиями обеспечения информационной безопасности и физической защиты.

Проблема обостряется тем, что дорогостоящие сейфы, расположенные вне непрерывно контролируемой территории, фактически не являются защитой. Их скорее следует рассматривать как иллюзию защищенности, лишающую пользователя мобильности без предоставления ему соответствующих гарантий. Наиболее надежные сейфы высокой стоимости и высокого веса имеют 5 класс стойкости, то есть на взлом такой физической защиты потребуется всего порядка 5 часов, подготовленному взломщику.

Единственным способом сохранения мобильности пользователя и обеспечения ему достаточно высоких гарантий защиты его личного криптографического ключа формирования ЭЦП является применение нейросетевых контейнеров [1,2,4], реализованных программно в доверенной вычислительной среде. В этом случае стойкость нейросетевого хранителя к атакам подбора может быть сделана сопоставимой со стойкостью растворенного в параметрах нейросети криптографического ключа. Для исключения атак на стык криптографического формирователя ЭЦП и нейросетевого хранителя ключа их целесообразно размещать в одной доверенной вычислительной среде физически выполненной в виде невскрываемого малогабаритного модуля со средствами самоуничтожения информации при попытках вскрытия.

Например, государство может обеспечить всех своих граждан специальными надежными и мобильными средствами хранения конфиденциальной информации. В качестве такого надежного средства хранения может быть использован специализированный нейросетевой контейнер. Нейросетевой контейнер – это программа, способная преобразовывать легко запоминаемый человеком пароль в криптографический ключ ЭЦП или очень длинный обычный пароль доступа. В качестве легко запоминаемого пароля может использоваться рукописная или голосовая фраза-пароль. Всё зависит от конкретной реализации. Единственное обстоятельство, влияющее на высокую надежность криптографического ключа ЭЦП - тайна легко запоминаемого пароля, что довольно просто реализуемо.

На рисунке 1 приведён пример такого нейросетевого контейнера. Данная программа преобразовывает рукописный пароль пользователя в его личный ключ.

Действительный хозяин этой программы (хозяин упакованного в нее ключа) всегда может извлечь ключ из нейросетевого контейнера, так как он помнит свой пароль и умеет воспроизводить свой почерк (свою уникальную динамику почерка). На рисунке показан пример извлечения легальным пользователем длинного ключа длиной 256 символов из короткого парольного слова “*Пенза*”.

Таким образом, человеку не нужно запоминать огромные последовательности символов (длинные пароли) или записывать свой ключ на бумагу. Имея при себе такой контейнер, пользователь всегда сможет получить свой ключ или длинный пароль, что избавляет его от необходимости иметь специальный сейф или охрану.

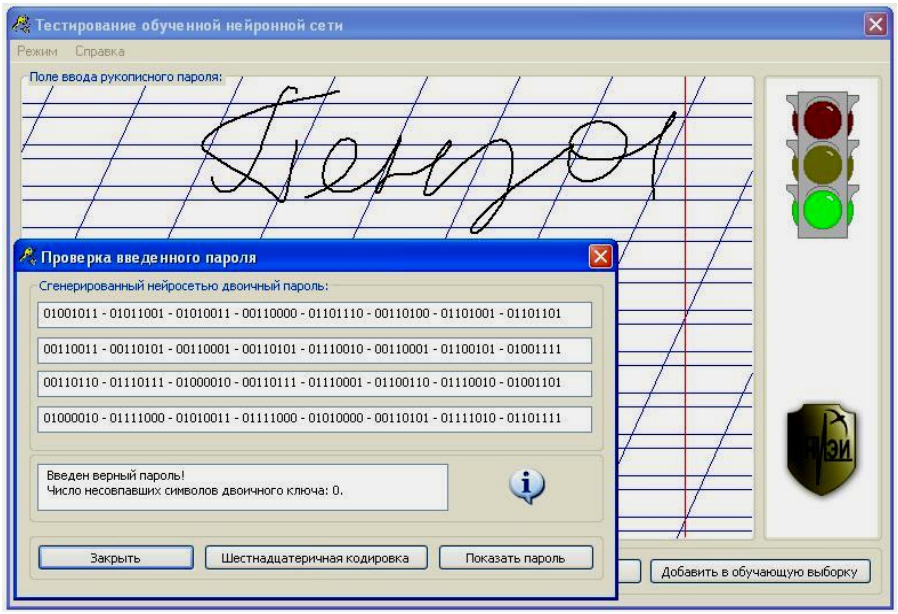


Рис. 1. Пример получения легальным пользователем криптографического ключа длиной 256 бит

Главным достоинством нейросетевых хранителей паролей является невозможность извлечения нелегальным пользователем (“Чужим”) личного ключа легального пользователя. То есть нелегально извлечь из программы рукописный пароль или ключ пользователя практически невозможно. Для получения личной информации легального пользователя “Чужой” будет вынужден перебирать все возможные варианты рукописных паролей, что является задачей сопоставимой по сложности с подбором криптографического ключа. Даже в том случае, когда «Чужой» знает слово-пароль и воспроизводит его своим почерком, извлечь верный ключ он не может. В дело вступает динамика подписи, индивидуальная для каждого человека.

Если промоделировать попытку “Чужого” извлечь личный ключ “Своего”, предъявляя скомпрометированный рукописный образ “*Пенза”*, мы убедимся, что количество неверно угаданных разрядов лежит в пределе 50-80. Предполагается, что “Чужой” знает не только скомпрометированный рукописный образ, представляет его начертание, но не знает динамику воспроизведения пароля “Своим”. Не смотря на то, что пароль скомпрометирован, “Чужой” не в состоянии извлечь правильный ключ из нейросетевого контейнера. Если бы он вообще не знал пароля, то было бы близко к 128.

Расчеты показывают, что, даже используя высокопроизводительные атакующие компьютеры, реальная атака подбора занимает примерно 21 год.

Получается, что пользователь, сохраняющий в тайне свой биометрический пароль “*Пенза”* (см. рисунок 1), имеет в своем распоряжении преобразователь биометрия-код со стойкостью к атакам подбора порядка $10^{15,8}$. Такая стойкость эквивалентна использованию ключа симметричного криптографического преобразования длиной 52 бита. Биометрико-нейросетевой защиты такой стойкости вполне достаточно для многих практических приложений. Естественно, что стойкость биометрической защиты будет сильно зависеть от самого рукописного слова-пароля, стабильности и уникальности почерка. После каждого обучения нейросетевого преобразователя необходимо его автоматическое тестирование с выдачей результатов о значении реальной стойкости биометрического образа.

Пример реализации модуля личного формирователя ЭЦП приведен на рисунке 2 и он ориентирован на биометрическую аутентификацию пользователя по динамике воспроизведения рукописного слова-пароля. Подобный модуль целесообразно выполнять в виде так называемого «цифрового пера». В настоящее время подобные перья выпускаются несколькими зарубежными фирмами (Hewlett-Packard, Logitech, Nokia, Hitachi-Maxell и др.), внешний вид подобных устройств приведен на рисунке 3. Современные «цифровые перья» работают автономно, способны запоминать до 100 листов рукописного текста с рисунками. Выпуск аналогичных устройств имеет смысл наладить и в России в связи с их перспективностью для безопасного хранения криптографического ключа формирования ЭЦП госслужащих и частных лиц. Доступ к информации в виде подписанных текстовых файлов, расположенных в формирователе ЭЦП «цифрового пера», видимо должен осуществляться через USB порт.

В связи с тем, что процессор «цифрового пера» имеет малый вычислительный ресурс, автоматическое обучение искусственной нейронной сети должно осуществляться одним из быстрых послойных алгоритмов [2]. Применение обычных алгоритмов обучения нейросетей (например, таких как алгоритм обратного распространения ошибки) нецелесообразно, так как затягивает обучение на несколько суток.

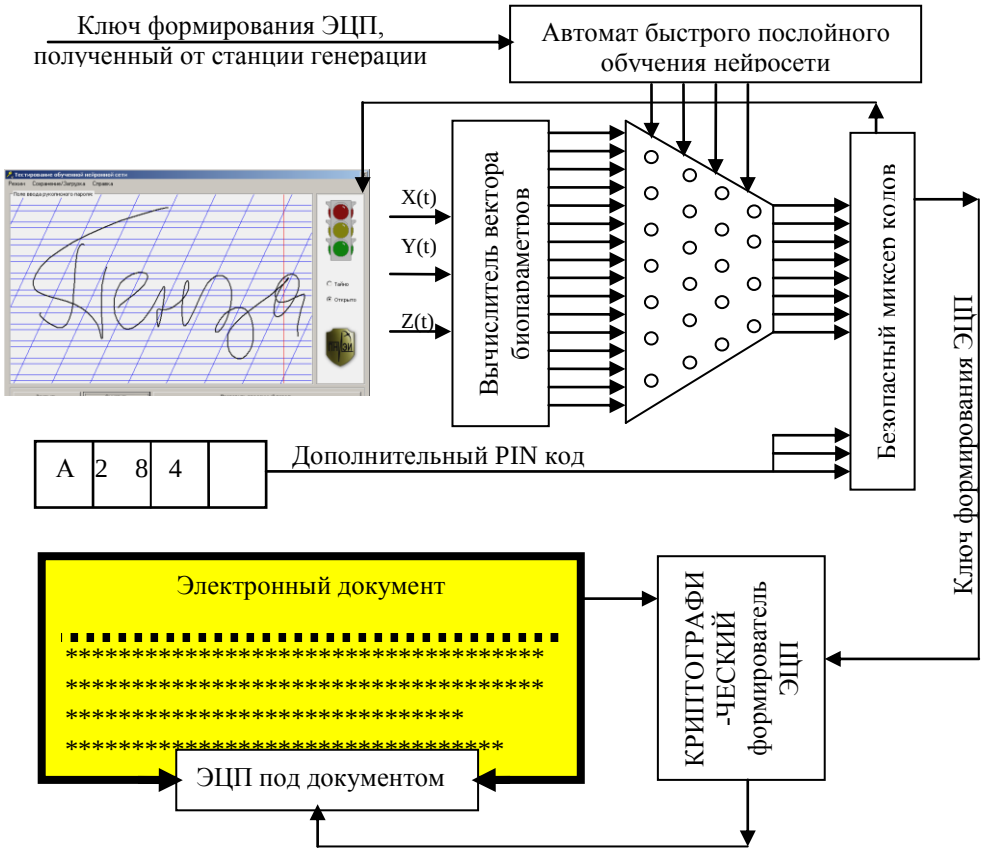


Рис. 2. Структура личного формирователя ЭЦП госслужащего с высоконадежной биометрической авторизацией

Рис. 3. Внешний вид «цифровых перьев» трех фирм: HP, Logitech, Nokia

Следует подчеркнуть, что обучение биометрико-нейросетевого формирователя ЭЦП должно вестись в режиме подключения «цифрового пера» к ПЭВМ или КПК, реализующих графический интерфейс связи с пользователем. В соответствии с таблицами приложения «А» к стандарту [4] интерфейс доступа к управлению формирователем ЭЦП может быть сделан высоконадежным и одновременно высокодружественным при использовании двух-трех коротких рукописных слов (составного пароля) родного языка пользователя, дополненных коротким PIN кодом. На рисунке 2, как пример одного из таких слов рукописного пароля отображено слово «*Пенза*». Практика показывает, что при увеличении числа рукописных слов в составном пароле дружественность системы падает, существенно увеличивается вероятность ошибки первого рода (ошибочного отказа «Своему» в аутентификации).

Значительный интерес для потребителей в настоящее время имеет задача защиты данных карманных персональных компьютеров (КПК). Для этой цели во ФГУП «ПНИЭИ» создается продукт «Нейрокриптон-КПК». Он ориентирован на использование парольной защиты ОС Windows CE/Mobile 2003/Pocket PC 2000 и выше. Основная экранная форма демоверсии «Нейрокриптон-КПК» приведена на рисунке 4.

Рис. 4. «Нейрокриптон-КПК» - основная экранная форма.

В соответствии с требованиями стандарта [4] несколько малых секретов должны объединяться в один большой безопасным способом. Запрещается использовать однозначные индикаторы правильности воспроизведения одного из малых секретов. В связи с этим в блок схеме формирователя выходы нескольких нейросетей, преобразующих несколько слов пароля в коды подключены к безопасному миксеру кодов. К этому же безопасному миксеру кодов подключены выходные разряды, набранного на графической панели PIN кода. Выход безопасного миксера дает ключ формирования ЭЦП. Ключ формирования ЭЦП вводится в устройство при обучении нейронных сетей и уничтожается после обучения. В программе храниться только хэш

ключа. После каждой процедуры биометрической аутентификации полученный код хэшируется и его хэш сравнивается с эталоном. При их совпадении зажигается зеленый свет светофора (рисунок 1), и может быть осуществлена процедура формирования ЭЦП под текстовым документом, находящимся в флеш памяти «цифрового пера».

В том случае, если хотя бы один разряд PIN кода или кодов на выходе нейросетей не совпадает с кодом ключа формирования ЭЦП зеленого света светофора появиться не может. Индикация верного результата «Свой» однозначна (зеленый сигнал светофора) появляется только при тождестве вычисленного хэша и его эталона. Иначе работает индикатор близости биометрического образа к заданному (желтый свет светофора). Желтый свет построен на нечетком (приближенном) анализе биометрических данных. При малых отклонениях биометрии от эталона индицируется «желтая» зона, однако такая индикация верна только для образов «Свой». «Чужой», не знающий рукописного пароля, попадает в «желтую» зону с вероятностью 10^{-3}. Такие попадания носят нерегулярный характер и порождены множеством коллизий нечеткого нейросетевого индикатора «желтой» зоны. Корректный синтез нечеткого нейросетевого индикатора «желтой» зоны необходим дружественным средствам биометрической аутентификации, однако решение этой задачи экспоненциально усложняется при линейном росте сложности биометрического образа (при линейном росте длины рукописной парольной фразы).

Ввод в действие национального стандарта [4] является знаменательным событием. То, что Россия раньше своих соседей по Европе и раньше США имеет эффективные механизмы противодействия “цифровому неравенству”, позволяет ей уже сейчас правильно закладывать фундамент будущей информационной безопасности. При закладке фундамента безопасности будущей информационной России точно повторять решения Европы и США нельзя. Уже сейчас видно, что их технические решения по биометрической защите очень дороги и крайне уязвимы. Мы не так богаты как они. Нам нужны менее дорогие, но гораздо более эффективные технические решения. Имеет прямой смысл тратить национальные ресурсы на свои биометрические паспорта и удостоверения личности, учитывая не только требования международных биометрических стандартов, но и требования своего собственного национального стандарта [4]. Более того, имеет смысл продвигать Российский национальный стандарт [4] как международный, через соответствующие подкомитеты ISO/IEC JTC1.

Ликвидировать подобное неравенство может только государство, предпринимая специальные меры, уравнивающие цифровые права всех граждан независимо от их социального статуса. Предвидя возникновение и усиление «цифрового неравенства» государству необходимо создавать специальные механизмы, сглаживающие изначальное неравенство.

В плане противодействия «цифровому неравенству» своих граждан Россия по праву занимает лидирующее положение, формальным подтверждением является разработка ею своего национального стандарта [4], регламентирующего требования к средствам высоконадежной биометрии. Одним из главных требований ГОСТа [4] является наличие средств встроенного контроля вероятности ошибок средств защиты или вероятности удачи атаки подбора. Проблема состоит в том, что биометрический пароль (рукописный или голосовой) пользователь должен сохранить в тайне от всех. Пользователь должен сам придумать удобную для него цифровую комбинацию, слово, фразу. При этом пользователю нельзя доверять среднестатистическим характеристикам, заявленным производителем.

Тайный биометрический образ может оказаться слабым и обеспечивать низкую стойкость защиты к атакам подбора. Что бы убедиться в стойкости нейросетевой защиты на конкретном биометрическом образе после обучения нейросети необходимо протестировать стойкость преобразователя. Для этого необходимо использовать специальные методы ускоренного тестирования стойкости биометрико-нейросетевой защиты [3].

Возникает целый комплекс вопросов, связанных с ускоренным тестированием средств биометрико-нейросетевой защиты. Кроме того, к этому комплексу примыкают вопросы сертификации и полного (неускоренного) тестирования средств защиты самим производителем или некоторым независимым (например, государственным) органом сертификации (испытаний). В свою очередь испытательный центр (лаборатория) должна иметь соответствующие методики испытаний и большие базы случайных биометрических образов, верно отражающих реальную статистику распределения биометрических параметров «Своих» пользователей и наиболее

вероятную статистику (тактику) организации потенциальным злоумышленником атак подбора.

При применении полностью автоматической высоконадежной биометрической аутентификации национальный стандарт РФ [4] безоговорочно требует проведения экспресс тестирования после каждого их обучения. Последнее связано с тем, что пользователь может неосознанно выбрать очень слабый биометрический пароль, и в место высоконадежной защиты получит очень слабую биометрическую защиту. При этом сам пользователь будет уверен в высокой степени защиты. После каждого обучения высоконадежное средство биометрической защиты должно автоматически осуществлять экспресс контроль своей стойкости и предупреждать пользователя о значении реальной стойкости его биометрического образа.

При решении перечисленных выше вопросов в Пензе сложился уникальный коллектив исследователей и создателей новых технологий, члены которого работают в Пензенском государственном университете, ФГУП «Пензенский научно-исследовательский электротехнический институт», ОАО «Научно-производственное предприятие «Рубин» и других предприятиях и организациях. Научно-технический потенциал коллектива позволяет решать вопросы фундаментальных исследований в новой области, разработке, производстве, сертификации и внедрении новых средств высоконадежной биометрико-криптографической аутентификации личности.

Подытоживая вышесказанное, необходимо отметить, что в настоящее время в России начали появляться надежные нейросетевые хранители биометрической и конфиденциальной криптографической информации. Для обеспечения не только юридического, но и реального “цифрового равенства” необходимо способствовать дальнейшему развитию и продвижению подобных нейросетевых хранителей. Возможны два пути развитии нейросетевых технологий. Первый путь, когда всё финансовое бремя ложится на плечи конкретных пользователей, в данном случае существует вероятность затягивания перехода на новую технологию на неопределённый срок. Второй путь, когда все первоначальные затраты на развитие и продвижение новых технологий берет на себя государство. Государству выгоднее своевременно позаботиться о создании безопасной среды, чем в дальнейшем бороться со злоупотреблениями.

ЛИТЕРАТУРА:

1. Иванов А.И., Анисимова Л.Ю., Акмаев А.А. Механизмы противодействия «цифровому неравенству» граждан информационного общества /Защита информации INSIDE. № 4, 2006, с. 26-29.

2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.

3. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2006 г. Издательство Пензенского государственного университета, 121 с.

4. ГОСТ Р ТК 362-2007 «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации»

5. ISO/IEC 1.37.19795 Процедуры выполнения тестирования и отчетов в биометрии.

6. ISO/IEC 1.37.19795.1 Процедуры выполнения тестирования и отчетов в биометрии.
Часть 1: Принципы и структура.

7. ISO/IEC 1.37.19795.2 Процедуры выполнения тестирования и отчетов в биометрии.
Часть 2: Методики тестирования.

8. ISO/IEC 1.37.19795.3 Процедуры выполнения тестирования и отчетов в биометрии.
Часть 3: Специальные методики тестирования.

9. ISO/IEC 1.37.19795.4 Процедуры выполнения тестирования и отчетов в биометрии.
Часть 4: Специальные программы тестирования.

Совмещение решения задачи высокоавторизованного биометрического доступа к информации высокого уровня секретности и задачи контроля текущего психофизического состояния доверенного лица

Статья журнала «Специальная техника средств связи»
А.И. Иванов

В соответствии с [1] нейросетевые преобразователи биометрия-код могут быть по разному сбалансированы по соотношению их стойкости к атакам на входы и к атакам на выходной код ключа управления. В случае, когда авторизованный биометрический доступ к коду ключа управления осуществляется на контролируемой территории в специально оборудованном помещении, требования к стойкости нейросетевых хранителей со стороны биометрии могут быть существенно ниже, чем требования к стойкости криптографического ключа шифрования. Однако, если доступ к ключу шифрования осуществляется вне контролируемой территории и вне специально оборудованных помещений, то тогда требования к стойкости преобразователя биометрия-код к атакам подбора должны быть сопоставимы со стойкостью криптографического ключа к атакам подбора.

Требования, сформулированные в [1] распространяются на преобразователи биометрия код гражданского применения и отражают ситуацию 2005-2006 года. В частности, таблица А2 приложения «А» к [1] отражает связь длины (сложности) биометрического пароля с эквивалентной длиной симметричного криптографического ключа. Фрагмент таблицы А2 [1] приведен ниже.

Из таблицы 1 следует, что для получения входной стойкости биометрии эквивалентной стойкости симметричного ключа длинной 256 бит необходимо рукописно воспроизводить парольную фразу, состоящую из 32 букв. Как показано в [2, 3], проще всего длинные биометрические пароли формировать из коротких, легко запоминаемых PIN кодов и производных от чисел. Например, рукописный пароль «1367 слонов» при рукописном воспроизведении его содержания не цифрами, а буквами даст рукописный пароль из 33 букв: «Тысяча триста шестьдесят семь слонов».

Безошибочно написать пароль из 5 слов длинной в 33 буквы достаточно сложно. Ошибка даже в одном слове приведет к необходимости повторного написания этого слова. В соответствии с требованиями [1] механизмы контроля правильности написания каждого из слов не должны строиться на классических четких хэш-функциях выходных кодов, соответствующих каждому слову. Необходимо использовать специальные нечеткие хэш-функции, которые не позволят противнику разделить задачу подбора на независимые части.

Фактически в системах высокоавторизованного биометрического доступа необходимо существенно усложнить интерфейс за счет его интеллектуализации. Интерфейс должен указывать пользователю в случае неудачи на его наиболее вероятные ошибки, не раскрывая при этом конфиденциальной биометрической информации.

Преобразователи биометрия-код имеют высокую дружественность только в слабом исполнении. Тогда они позволяют извлекать ключ любой длины из нейросетевого преобразователя без особых затрат ресурсов со стороны человека. Если стойкость слабых преобразователей биометрия-код начать усиливать, то их дружественность по отношению к пользователям будет падать. Если стойкость биометрии должна быть высокой, то пользователь должен потратить вполне определенные усилия на преодоление биометрической защиты. Так или иначе, пользователю для своей высоконадежной биометрической авторизации придется прилагать некоторые усилия.

Таблица 1. - Рекомендуемые длины ключей (паролей) для среднестатистического пользователя в зависимости от числа букв биометрического пароля или от информативности тайного биометрического образа (данные ФГУП «ПНИЭИ» 2006 года)

Число букв (цифр) в пароле, образующем биометрический образ без учета пробелов между словами	**Длина ключа (пароля), получаемого из рукописного пароля (бит)**	**Длина ключа (пароля), полученного из голосового пароля (бит)**	**Длина ключа (пароля), полученного из динамических параметров клавиатурного почерка (бит)**
8	64	21	------
9	72	23	------
10	80	26	------
12	96	31	------
14	112	36	-----
16	128	42	7
18	144	47	8
20	160	52	10
24	192	64	11
26	224	76	14
32	256	88	17
36	288	100	20
40	320	112	23

Весьма интересным фактом является то, что предел дружественности биометрико-нейросетевых технологий пока неизвестен. Видимо, дружественность высоконадежных биометрических систем, выполненных в соответствии с требованиями [1], может быть существенно увеличена. Например, в место анализа двух координат Y(t), X(t) может учитываться третья координата Z(t) – давление на подложку (данные таблицы №1 отражают характеристики имеющихся на 2006 год у ФГУП «ПНИЭИ» двухкоординатных макетов преобразователей рукописных биометрических образов в код). С учетом этого дружественность биометрии может быть увеличена примерно на одну треть, и пользователю придется воспроизводить рукописный пароль из 3, 4 слов включающих 22 буквы. Для сбалансированных по стойкости вход/выход преобразователей их дружественность становится одним из важнейших технических показателей.

В ответственных приложениях, запускаемых вне контролируемой территории и вне специально оборудованных помещений, наряду с проблемой высоконадежной авторизации актуальной является проблема контроля психофизического состояния доверенного лица.

Задача контроля психофизического состояния проверяемого может решаться параллельно задаче высоконадежной авторизации. Например, возможен синтез специальных «нечетких» распознавателей статистик (аналогов нечеткой хэш-функции), характерных для естественного психофизического состояния испытуемого. Далее, зная точку «норма» (меру расстояния от нормального, естественного состояния), всегда можно оценить текущее психофизическое состояние человека.

С математической точки зрения контроль текущего психофизического состояния человека сводится к контролю стабильности его действий при воспроизведении одного и того же рукописного слова. Фактически необходимо заставить человека написать порядка 10,…., 20 раз одно и то же контрольное слово. Далее необходимо оценить разброс контролируемых биометрических параметров в тестовой выборке и сравнить с эталонным разбросом. Увеличение разброса будет свидетельствовать о нахождении испытуемого в стрессовом состоянии (состоянии усталости, алкогольном, наркотическом опьянении, наличии какой-либо болезни...). Уменьшение разброса в сравнении с контрольным наоборот свидетельствует о высоком уровне текущего

психофизического состояния испытуемого.

Таким образом, задача контроля психофизического состояния испытуемого при его рукописном написании 5 рукописных слов является вполне корректной и технически может быть решена. Однако при этом основными проблемами, которые необходимо решить являются:

1.синтез достоверных шкал психофизического состояния человека;

2.синтез эталонных воздействий, имитирующих стрессовое и иные нежелательные состояния контролируемого человека;

3.синтез и обучение специальных нечетких нейросетевых функций контроля многомерных статистик человека в его нормальном психофизическом состоянии.

Все перечисленные выше задачи могут быть решены в относительно короткое время, однако для их решения необходима постановка соответствующей научно-исследовательской работы. В случае выполнения НИР и последующих ОКР по параллельному контролю психофизического состояния доверенного лица у российского государства в лице должностных лиц ВС РФ (ГРУ), ФСБ появится техническая возможность локального и дистанционного контроля психофизического состояния доверенного лица. Фактически появляется техническая возможность контроля факта «захвата» доверенного лица и его работы под «Чужим» контролем, например, в измененном психофизическом состоянии.

ЛИТЕРАТУРА:

1. Окончательная редакция проекта ГОСТ Р ТК 362 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». Публичное обсуждение с 9.09.05 по 30.12.05, окончательная редакция одобрена голосованием на заседании ГОСТ Р ТК362 31.05.06.

2. Иванов А.И., Ефимов О.В., Фунтиков В.А. Оценка усиления стойкости коротких цифровых паролей (PIN кодов) при их рукописном воспроизведении / «Защита информации. INSIDE» № 1, 2006 г., с. 55-57.

3. Фунтиков В.А., Иванов А.И. Усиление коротких PIN кодов голосовой биометрией пользователя //«Современные технологии безопасности» №1(12), 2005 г., стр. 32-34.

Нейросетевая технология защиты личных биометрических данных

Статья журнала «Нейрокомпьютеры»
Ю. К. Язов, И. Г. Назаров, А. И. Иванов, О. В. Ефимов

Существенный толчок развитию биометрических технологий дала программа создания паспортно-визовых документов нового поколения. На данный момент по этой программе международная организация по стандартизации ISO/IEC, комитет JTC1 (Information Technology), подкомитет SC37 (Biometrics) создали более 20 международных биометрических стандартов и порядка 40 стандартов находятся в стадии обсуждения и разработки. Ранее в период 1998-2002 гг. большинство уже принятых сегодня международных биометрических стандартов разрабатывались как национальные стандарты США.

Основой активно продвигаемых США биометрических технологий и действующих биометрических стандартов ISO/IEC JTC1 SC37 является использование классических решающих правил. Схема процедур биометрической аутентификации построенных на использовании классических решающих правил приведена на рисунке 1.

Для реализации подобных технологий необходимо иметь биометрический шаблон (блок 3, рис. 1), отражающий стабильную и нестабильную часть контролируемого биометрического образа. Например, биометрический шаблон может быть получен в форме вектора математических ожиданий контролируемых параметров и в форме второго вектора допустимых значений отклонений контролируемых параметров. При такой постановке задачи классическое решающее правило должно сравнивать вектор контролируемых биометрических параметров с их шаблоном и принимать решение «Да/Нет». Очевидно, что продукты, реализованные по блок-схеме, представленной на рисунке 1 крайне уязвимы. Для реализации успешной атаки на биометрическую защиту достаточно:

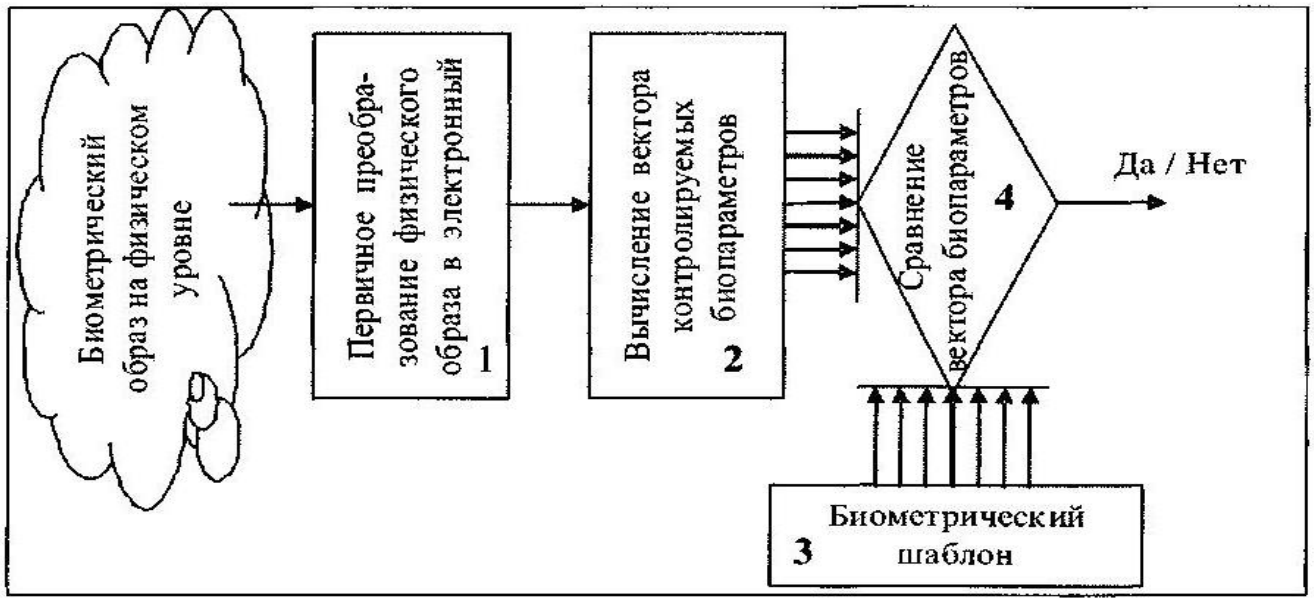
подменить на нужный биометрический шаблон;

скомпрометировать биометрический шаблон для изготовления электронного или физического муляжа биометрического образа «Свой»;

загрубить решающее правило (например, расширить допуски);

изменить последний бит решающего правила.

Рис. 1. Схема процедур биометрической идентификации, выполненных с классическим решающим правилом



Положение усугубляется тем, что программы биометрической защиты создаются типовыми приемами (инструментами). Взломав одну из программ, нетрудно создать автомат для автоматизированной модификации всех программ этого типа.

За информационную безопасность биометрических приложений, видимо, придется отвечать подкомитету ISO/IEC JTC1 SC27 (Security techniques). Этот подкомитет предполагает организовать защиту биометрических приложений путем защиты биометрических шаблонов и контроля целостности наиболее важных фрагментов биометрических программ [1].

Одним из путей решения задачи защиты биометрического шаблона является использование искусственных нейронных сетей. На рисунке 2 приведена схема биометрического средства, использующего нейросетевое решающее правило.

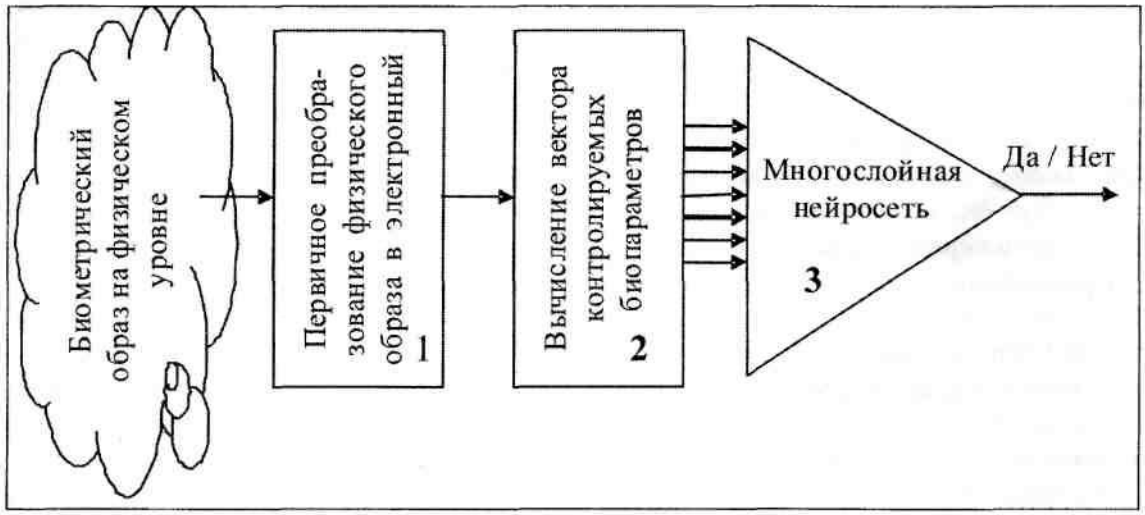


Рис. 2. Блок-схема процедур биометрической идентификации, выполненных с классическим нейросете-вым решением

Как видно из рисунка 2 биометрический шаблон как таковой при нейросетевой идентификации отсутствует. Биометрический шаблон растворился в параметрах связей нейронов многослойной нейронной сети. При технической реализации схемы (рис. 2) злоумышленник не может скомпрометировать биометрический шаблон, однако атака на последний бит нейросетевого решающего правила остается актуальной.

Для того чтобы сделать неэффективной атаку на последний бит решающего правила национальный стандарт РФ [2] рекомендует использовать преобразователи биометрия-код ключа аутентификации. Теоретически такие преобразователи могут быть построены с использованием «fuzzy» экстракторов нестабильной биометрической информации [3]. Этот путь развития предлагается тремя университетами США, как результат освоения ими нескольких правительственных грантов. В России развивается технология использования больших и сверхбольших искусственных нейронных сетей [4]. Наиболее сложным в нейросетевой технологии является многократное ускорение процедур обучения искусственных нейронных сетей и полная автоматизация процедур обучения. Переходя от использования нейросети с одним выходом к нейросети с 1024 выходами, мы должны, как минимум, в 1024 раза повысить скорость обучения нейронной сети. Время обучения и вычислительные ресурсы, затрачиваемые на автоматическое обучение, становятся крайне важными показателями безопасности технологии. На рисунке 3 приведена схема реализации процедур биометрической аутентификации, построенных на использовании нейросетевого преобразователя биометрия-код.

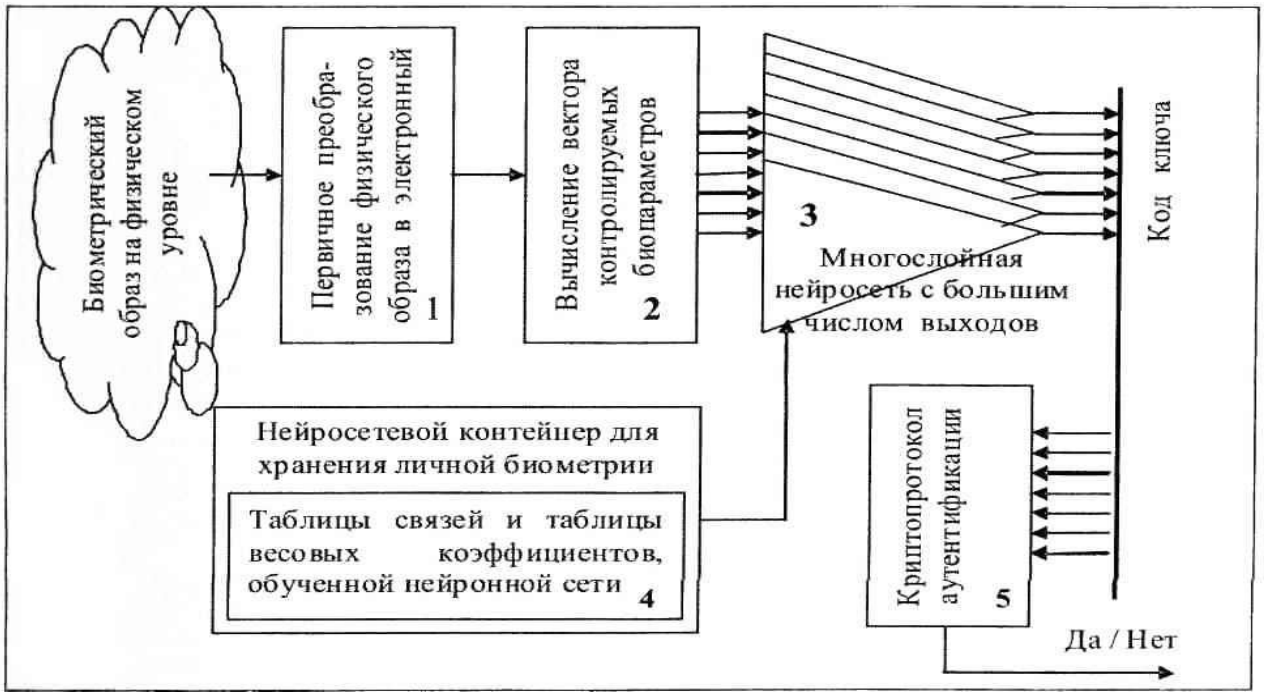


Рис. 3. Схема реализации процедур биометрической аутентификации, построенных на использовании нейросетевого преобразователя биометрия-код

Формально нейросетевой преобразователь биометрия-код может быть представлен совокупностью множества многослойных нейронных сетей (число нейронных сетей определяется длиной выходного кода и в соответствии с требованиями международных и российских криптопротоколов должно составлять 256, 512, 1024, 2048,...). В соответствии с требованиями [2] преобразователь биометрия-код должен выдавать случайные коды при воздействии на него случайными биометрическими образами «Чужой». При воздействии на нейропреобразователь примером биометрического образа «Свой» нейропреобразователь должен с высокой вероятностью выдать код личного ключа «Свой» для последующего использования его в соответствующем криптопротоколе аутентификации.

Такая структура исключает реализацию атаки на последний бит решающего правила. Если злоумышленник получил неинициированную программу биометрической защиты, то выявить последний бит он не может. В место модификации одного бита злоумышленнику приходится модифицировать 256, 512, 1024, 2048,... бит. Подбор неизвестного ключа из 256, 512, 1024, 2048,... бит является задачей гарантированно высокой вычислительной сложности, что и является гарантией защиты биометрических приложений от атаки на последний бит.

Очевидно, что после того как входной биометрический образ будет преобразован в соответствующий криптографический ключ для аутентификации, далее может быть использован любой из известных криптографических протоколов. Выполнив требования [2] и обеспечив безопасный стык биометрии с криптографией мы далее в праве применять любой криптографический протокол. В том числе могут быть использованы криптографические протоколы, как для локальной, так и для дистанционной аутентификации в Интернет.

Одним из принципиально важных технологических элементов нейросетевой биометрической аутентификации является то, что хранить личные биометрические данные человека приходится в так называемом «нейросетевом контейнере». На рисунке 4 дан фрагмент «нейросетевого контейнера» с биометрическими параметрами, соответствующими динамике воспроизведения рукописного слова пароля *«Пенза»*.

Нейросетевой контейнер для безопасного хранения биометрии

Таблица связей входов и выходов нейронов	Таблица весовых коэффициентов обученных нейронов
70 19 18 46 10 13 94 90 23 42 64 46 60	94 05 84 40 95 54 70 26 53 40 59 69 44
86 63 57 19 56 25 61 59 50 75 63 81 58	01 61 58 23 31 09 86 82 70 54 15 73 14
92 73 67 32 31 11 86 16 08 65 55 41 47	65 09 95 28 99 30 37 22 25 91 71 29 18
16 74 83 88 34 13 79 61 48 36 11 23 92	78 22 01 12 32 04 19 16 89 20 65 91 93
67 50 15 51 69 61 01 11 87 75 39 56 96	16 57 95 58 26 36 80 08 60 20 65 61 45
18 14 96 03 06 14 87 73 02 71 22 17 35	40 60 95 40 19 58 63 05 27 90 73 40 91
37 81 53 80 15 41 14 07 58 55 32 81 29	39 36 75 74 21 69 37 11 21 66 69 08 23
90 75 37 23 13 55 06 53 10 84 02 71 96	31 15 07 73 70 66 10 03 06 14 87 73 04
.....	.....
.....	.....

Рис. 4. Пример нейросетевого контейнера с биометрическими параметрами, соответствующими динамике воспроизведения рукописного слова пароля *«Пенза»*

Из рисунка 4 видно, что контейнер состоит из двух таблиц цифр весьма похожих на шифрограммы. Если нет соответствующей записи, то по этим таблицам нельзя установить, что за биометрия размещена в контейнере (голос?, рисунок отпечатка пальца?, рукописное парольное слово?,...). Нельзя так же указать чья это биометрия и какой код должен получиться в результате предъявления средству биометрической аутентификации верного биометрического образа «Свой». Все эти свойства могут быть использованы для обеспечения конфиденциальности, анонимности, обезличенности биометрических данных гражданина.

Следует подчеркнуть, что формировать базы биометрических шаблонов, например, используемых в паспортно-визовых документах нового поколения [5], строго запрещаются соответствующими положениями. Это обусловлено тем, что отпечаток указательного пальца у человека один, если его рисунок скомпрометирован, то им для своей защиты пользоваться уже нельзя. Если же разместить тот же самый рисунок отпечатка пальца в параметры нейросетевого преобразователя биометрия-код, то соответствующий этому рисунку отпечатка пальца «нейросетевой контейнер» вполне можно размещать в больших базах биометрических данных. Единственное, что нужно при этом сделать - это обезличить «нейросетевой контейнер», присвоив пользователю псевдоним или его личный номер, работающий только в этой конкретной базе биометрических данных.

Для обеспечения действительной безопасности хранения личной биометрии гражданина необходимо, чтобы во всех базах данных его рисунок отпечатка пальца выглядел совершенно непохоже. Для этого достаточно либо изменить выходной код ключа доступа, либо изменить случайным образом связи в нейронной сети.

При изменении кода доступа пользователя в систему нейросеть переобучается и, соответственно, изменяется правая таблица «нейросетевого контейнера», приведенного на рисунке. 4. Левая же таблица связей нейронов (рис. 4) остается прежней. В этом случае внешний наблюдатель способен отследить только факт изменения кода доступа, но он не знает, остался ли прежним биометрический образ «Свой». Пользователь при смене своего кода доступа вполне мог сменить и палец, по рисунку которого осуществляется доступ.

Если пользователю требуется обеспечивать свою анонимность на каждом сеансе аутентификации, то он все время должен переобучать нейросеть, каждый раз меняя структуру связей ее нейронов. В этом случае внешний наблюдатель не может отследить факт появления

биометрии одного и того же человека даже, если пользователь не меняет код своего личного ключа или свой биометрический образ.

Одним из приложений «нейросетевых контейнеров» с личными биометрическими данными является создание на их базе электронных биометрических удостоверений личности. Применительно к открытому информационному пространству термин «удостоверение личности» вводит ГОСТ Р ИСО 7498-2-99 и определяет его как «данные, передаваемые для установления заявленной подлинности логического объекта». Удостоверения личности на практике реализованы в виде различных модификаций сертификатов открытых ключей пользователей, применяемых в соответствии с ГОСТ Р ИСО/МЭК 9594-8-98. Однако использование сертификатов ключей для высоконадежного подтверждения личности граждан практически невозможно, так как сертификат не содержит данных, связанных с личностью гражданина (его биометрических данных).

При использовании обычных сертификатов требуется сохранение в тайне аутентификационной информации (ключа, длинного пароля) или аппаратного носителя секретов. Поэтому в случае аутентификации на основе обычных сертификатов ключей на аутентифицируемого гражданина возлагается дополнительная нагрузка по запоминанию ключей (паролей), либо по обеспечению безопасного хранения аппаратного носителя секретов.

Для устранения описанных выше проблем предлагается перейти от обычных сертификатов ключей к электронным биометрическим удостоверениям личности, в которые дополнительно вводятся биометрические данные, защищенные через их размещение в «нейросетевом контейнере».

Различают несколько вариантов исполнения электронных биометрических удостоверений личности.

1. Открытое электронное биометрическое удостоверение личности представляет собой сертификат открытого ключа пользователя, дополненный нейросетевым биометрическим контейнером открытого биометрического образа пользователя, связанного с его открытым ключом. Это удостоверение используется для контроля пользователя операторами системы или другими гражданами. Персональные данные пользователя (имя, адрес, полномочия, ...) размещены в открытом удостоверении открыто (без шифрования).

2. Обезличенное и анонимное электронное биометрическое удостоверение личности по сравнению с открытым дополнительно имеет нейросетевой биометрический контейнер с тайным биометрическим образом, связанным с личным ключом пользователя. Персональные данные пользователя (имя, адрес, полномочия, ...) зашифрованы на открытом ключе.

2.1. Обезличенное электронное биометрическое удостоверение предназначено для обезличенной работы пользователя в информационной системе. В обезличенном удостоверении содержится только псевдоним или наименование группы пользователя, его полномочия, а персональные данные хранятся в зашифрованном виде. При необходимости пользователь может раскрыть свою обезличенность. Это он может сделать, предъявив свой тайный биометрический образ, получив свой личный ключ и расшифровав на своем личном ключе свои персональные данные.

Обезличенное электронное удостоверение позволяет человеку доказать свою принадлежность к группе лиц, обладающих теми или иными правами, например, правом доступа на некоторый особо важный объект или право на голосование.

2.2. Анонимное электронное биометрическое удостоверение предназначено для анонимной работы пользователя в информационной системе. Отличие анонимного удостоверения от обезличенного состоит в том, что анонимное электронное биометрическое удостоверение не содержит имени, псевдонима и имени группы пользователя. Анонимное электронное биометрическое удостоверение личности, в отличие от обезличенного электронного биометрического удостоверения личности, не позволяет стороннему наблюдателю вести аудит и накапливать статистику действий пользователя в системе.

Открытые электронные биометрические удостоверения целесообразно использовать при дистанционном обращении граждан в органы государственной власти, при взаимодействии граждан с бизнесом, при взаимодействии с электронными нотариусами, а так же при взаимодействии с другими гражданами.

Обезличенные электронные биометрические удостоверения целесообразно использовать, например, в медицинских системах ведения электронных историй болезни при социально

значимых заболеваниях, системах электронного голосования, системах контроля доступа к информационным ресурсам или доступа на реальный особо важный объект.

Таким образом, новые нейросетевые технологии защиты биометрических данных позволяют надежно скрывать от посторонних личную биометрию пользователя. Получается как бы двойной эффект от применения искусственных нейронных сетей большой размерности.

Переход от одной нейронной сети (рис. 2) к 256 нейронным сетям (рис. 3) позволяет примерно в миллиард раз снизить вероятность ошибочного признания образа «Чужой» за образ «Свой». Увеличение размерности нейронной сети в 256 раз приводит к экспоненциальному росту качества принимаемых этой нейронной сетью решений. Именно это обстоятельство и послужило причиной введения в название отечественного стандарта [2] словосочетания «высоконадежная биометрическая аутентификация».

Не менее важным оказывается еще и то, что новые технологии способны обеспечить конфиденциальность, анонимность или обезличенность биометрических данных при их хранении в «нейросетевых контейнерах». При практическом использовании принципиально важно именно сочетание высокой надежности нейросетевой аутентификации с обеспечением конфиденциальности личной биометрии пользователя «нейросетевыми контейнерами».

Перспективы создания систем электронного голосования нового поколения с анонимной биометрической авторизацией голосующих и сквозным юридически значимым контролем голосующими процедур учета их голоса от местного избиркома до Центризбиркома.

Статья журнала «Специальная техника средств связи»
В.А. Фунтиков, А.И. Иванов

То, что англоязычные средства массовой информации называют «электронной демократией» к действительной демократии имеет слабое отношение. Примером того могут служить разрабатываемые в рамках проекта «Электронная Европа» процедуры электронного голосования. Во всех этих проектах голосуют не люди, а «ключи» выданные этим людям для голосования. Пользуясь этими технологиями, уважаемые депутаты Госдумы РФ не ходят на заседания, а за них голосуют их товарищи по партии. Это беда любой «современной» системы электронного голосования.

Избавиться от этого недостатка удается если:

1. жестко связать биометрию человека и его криптографический ключ голосования;
2. обеспечить высокую степень конфиденциальности биометрии голосующего;
3. обеспечить высокую степень анонимности голосующего.

Биометрические технологии США и стран Евросоюза не могут обеспечить анонимность и конфиденциальность биометрических данных и не могут надежно связывать биометрию человека с его криптографическим ключом для голосования. На данный момент анонимность и конфиденциальность биометрии надежно обеспечиваются только российскими технологиями высоконадежной биометрической аутентификации. Для того, что бы выявить суть проблемы достаточно попытаться ответить на один вопрос: что произойдет с демократическими институтами, если исчезнет анонимность и конфиденциальность при голосовании? При этом какая демократия «электронная» или классическая особой роли не играет. Рушатся основные механизмы, обеспечивающие действительную демократию. Демократия обычная или «электронная» неразрывно связаны с анонимностью голосующего (обеспечением анонимности и конфиденциальности биометрии голосующего, так как, зная биометрию всегда можно восстановить имя ее владельца).

При разработке биометрических систем для электронного голосования нельзя использовать биометрию человека, по которой можно его найти. Не годятся, отпечатки пальцев, геометрия лица, геометрия руки, рисунок радужной оболочки глаза. Необходимо использовать тайный биометрический образ человека, например, рукописный пароль, воспроизведенный почерком человека.

Активно занимаясь биометрией с 1994 г. и зная о наличии ряда принципиальных недостатков у всех существующих за рубежом биометрических технологий ФГУП «Пензенский научно-исследовательский электротехнический институт» в период с 2002-2005 г.г. создал новую технологию высоконадежной биометрико-криптографической нейросетевой идентификации личности человека. На данный момент ФГУП «ПНИЭИ» имеет опытные образцы и протоколы их испытаний. Более того, с 01.04.2007 в России введен в действие ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». Ввод в действие этого нового российского привело к существенному моральному устареванию ряда национальных биометрических стандартов США (ныне международных биометрических стандартов ISO/IEC JTC1 SC37).

Суть разработанной биометрической технологии сводится к рукописному воспроизведению слова-пароля. Например, это может быть слово «Пенза» как это показано на рисунке 1.

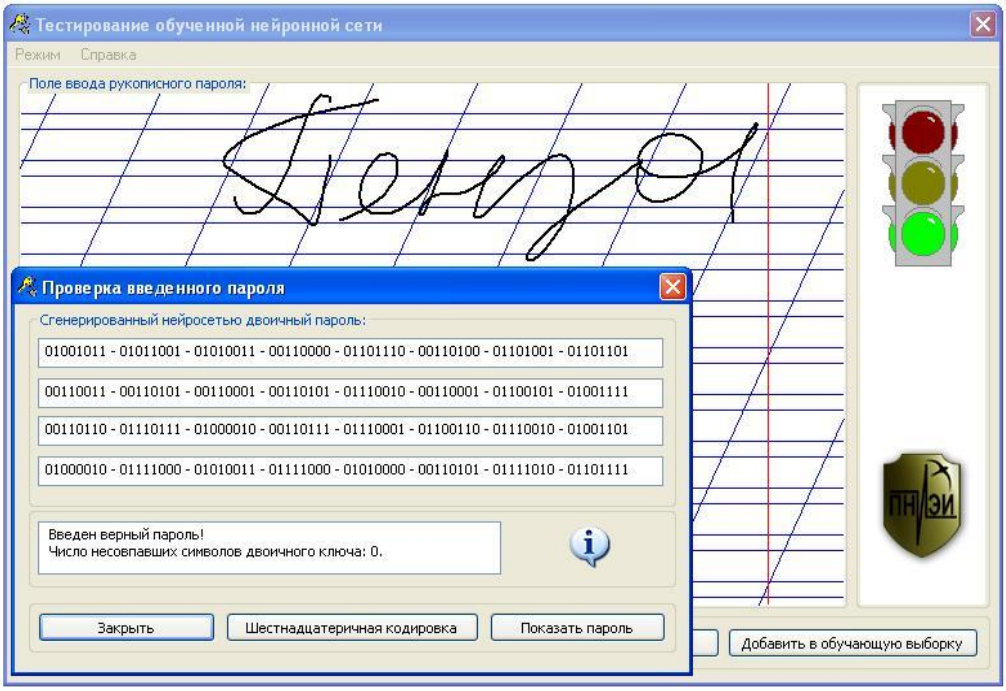


Рис. 1. Экранная форма работы нейросетевого преобразователя рукописного пароля в код ключа голосования длиной 256 бит.

Голосующему нет необходимости запоминать (хранить) длинный криптографический ключ, выданный ему для голосования. Голосующий помнит только короткий пароль, для того, что бы получить ключ, голосующий должен написать своей рукой свой пароль. При этом заранее обученная нейронная сеть преобразует биометрию пользователя в его ключ голосования. Даже если голосующий идет на нарушение и передает свой бюллетень голосования другому (открывает ему свой пароль), передать все свои полномочия он не может. Подставной, желающий голосовать за другого, не обладает уникальным почерком голосующего.

При сохранении в тайне голосующим его биометрического пароля новая технология способна обеспечить очень высокий уровень анонимности голосующего и конфиденциальности его биометрии. Из параметров обученной нейронной сети нельзя извлечь биометрию человека и выданный ему ключ для голосования.

Еще одним принципиально важным преимуществом новой технологии является то, что голосующий получает на ряду с гарантиями его анонимности возможность проконтролировать процедуры учета его голоса на любом этапе голосования. Новое поколение систем электронной демократии должно строиться таким образом, что бы каждый технологический этап голосования порождал свои юридически значимые электронные документы учености и сам голосующий при желании мог бы проверить всю цепочку электронных документов, сопровождающих движение его голоса. Появляется новый механизм, когда любой из голосующих не может отказаться (переголосовать), но может проверить местную, региональную, центральную избирательную комиссии, и найти свой анонимный голос в общих итогах голосования.

Рассмотрим один из вариантов реализации механизмов электронного анонимного голосования нового поколения с высоконадежной биометрической авторизацией голосующего. Для определенности разобьем работу механизма на 9 функционально значимых фрагментов:

1. По новой технологии Центризбирком делегирует региональным избирательным комиссиям право контроля целостности программного обеспечения и достоверности списков открытых ключей местных избирательных комиссий. Кроме того, Центризбирком контролирует начало голосования через формирование специальной метки времени «СТАРТ» и окончание процедуры голосования через сигнал «СТОП» в приеме просроченных бюллетеней голосования с низу. Подсчет числа проголосовавших может выполняться одновременно Центризбиркомом и любым голосующим, так как Центризбирком постоянно публикует списки проголосовавших анонимных открытых ключей, а после момента «СТОП» к сформированным спискам проголосовавших открытых ключей добавляется результат голосования по каждому открытому

ключу.

2. Каждый проголосовавший гражданин (голосование может быть дистанционным (из любого места) или локальным на участке голосования) может найти свой открытой ключ в списке проголосовавших своего местного избиркома или зеркала местного избиркома на сайте Центризбиркома. Если через заранее заданное время (например, 20 минут) проголосовавший избиратель не обнаружит свой открытый ключ в списке проголосовавших, он имеет право инициировать разбор ситуации «Куда делся мой голос». У каждого избирателя появляется механизм контроля того, что его голос учтен с момента «СТАРТ» до момента «СТОП». После момента «СТОП» каждый избиратель может лично убедиться в том, что его открытому ключу соответствует его голос (ДА/НЕТ), пара открытый ключ избирателя и результат его голосования публикуется открыто на сайте местного избиркома и Центризбиркома. Кроме контроля своего голоса избиратель может проконтролировать ситуацию на своем избирательном участке самостоятельно, подсчитывая опубликованные результаты голосования других людей с другими личными ключами. Анонимность голосования обеспечивается тем, что никто не может связать открытый ключ человека с его личностью, пока сам человек не захочет этого сделать.

3. Если избиратель обнаружил фальсификацию своего голоса, то он в праве в судебном порядке найти виновного и наказать его. Только в процессе судебного разбирательства избиратель в праве скомпрометировать свою анонимность во время судебного доказательства факта фальсификации его голоса. Все этапы электронного голосования юридически значимо документируются, ведутся достоверные списки проголосовавших мандатов, разбор инцидентов и возможных злоупотреблений автоматизирован.

4. Избиратель, желающий проголосовать должен заранее лично явиться в местный избирком, где у него проверяется паспорт, прописка, его права. Далее пришедший вносится в список получивших мандат и программу для голосования. Пришедший избиратель с помощью предоставленных ему средств формирует пару ключей (открытый ключ и тайный ключ голосования). Далее голосующий безопасно связывает свой биометрический образ (отпечаток пальца, голосовой пароль, рукописный пароль,…) с тайным ключом голосования в соответствии с требованиями ГОСТ Р 52633-2006.

5. Оба ключа (открытый ключ и тайный ключ голосования) избиратель никому пока не доверяет для хранения (открытый ключ избирателя становится известен только после его голосования и только в контексте его результата голосования). Для обеспечения своей анонимности избиратель формирует бюллетень для своего будущего голосования, например в следующей форме «Бюллетень № (хххх-случайное число сервера раздачи бюллетеней) Зареченского избиркома, Школа № 64, Пензенская область для последующего голосования 15 марта 2012 года гражданином РФ по выбору президента РФ». Далее избиратель формирует мандат для голосования, состоящий из зашифрованных на открытом ключе избирателя: 1-бюллетеня для голосования с уникальным числом сервера; 2- открытого ключа избирателя; 3-полных данных избирателя. Кроме того, в мандат входят 4- таблицы нейронной сети связывающей биометрию избирателя с его тайным ключом. Все 4 составляющих мандата избирателя охватываются ЭЦП сервера избиркома, выдавшего мандат. Так как ключи избирателя (открытый и тайный) никому неизвестны, никто не может сформировать и прочитать содержания шифрограммы в мандате. Открыто лежащие в мандате таблица обученной нейронной сети не могут быть использованы для компрометации анонимности избирателя (смотри таблицы 2А и 3А приложения «А» к ГОСТ Р 52633-2006). После того как мандат избирателя сформирован и подписан ЭЦП сервера избиркома, избиратель сам лично уничтожает свои ключи (открытый ключ и тайный ключ). Теперь только избиратель может прочитать мандат, воспользовавшись своей биометрией через извлечение своего секретного ключа из нейронной сети.

6. При голосовании избиратель с помощью своей биометрии извлекает свой тайный ключ, расшифровывает шифрограмму своего мандата, извлекает из нее бюллетень для голосования с уникальным номером, добавляет в бюллетень результаты своего голосования (ДА/НЕТ), добавляет в бюллетень свой открытый ключ и подписывает своей ЭЦП свой бюллетень. Далее избиратель отправляет по электронной почте свой заполненный бюллетень для голосования и свой мандат для голосования или лично формирует свой бюллетень на участке для голосования.

7. Заполненный и подписанный бюллетень в паре с мандатом являются двумя

электронными юридически значимыми документами голосования. Их наличие на сервере голосования приводит к формированию на нем результата голосования одного человека (формируется пара открытый ключ и результат), которые пересылаются в Центризбирком. Сервер голосования проверяет подлинность своего мандата (проверяет свою ЭЦП), а также берет открытый ключ избирателя и проверяет ЭЦП бюллетеня. При их совпадении делается вывод о подлинности предъявленного заполненного бюллетеня голосования. Имея только открытый ключ, сервер и все другие не могут расшифровать полностью мандат голосующего и узнать его имя. Расшифровать полностью шифрограмму мандата может только его хозяин, обладающий уникальной биометрией.

8. После того как сервер местного избиркома убедился в правильности оформления присланного ему бюллетеня, он документирует факт голосования одного из своих мандатов. Для этого результат голосования, открытый ключ, № мандата и уникальная метка времени «СТАРТ» Центризбиркома объединяются в один документ, подписываются ЭЦП сервера голосования и пересылаются в Центризбирком. Наличие в электронном документе уникальной метки «СТАРТ» свидетельствует о том, что не было голосования раньше срока. Если оформленный таким образом документ придет в Центризбирком после момента «СТОП», то голос считается просроченным. Каждая пересылка (гражданин - сервер местного избиркома; сервер местного избиркома - сервер Центризбиркома) подтверждаются квитанциями получения.

9. Каждый избиратель после момента «Стоп» может проверить правильность учета его голоса по своему мандату, но не может узнать имена владельцев других мандатов. Общий список получивших мандаты открыт, каждый может проверить отсутствие в нем совершенно незнакомых людей. Исключается вброс вымышленных голосующих, так как паспортные данные каждого получившего мандат хранятся и могут быть проверены.

Следует подчеркнуть, что описанные выше, новые технологии электронного голосования (когда голосуют люди, а не ключи) могут быть реализованы только на основе российского национального стандарта [1]. По технологиям высоконадежной биометрической аутентификации человека с преобразованием его тайного биометрического образа в ключ Россия является мировым лидером. Только технологии, выполненные по [1], обеспечивают анонимность голосующего. Сегодня США и страны НАТО (Евросоюза) эффективных технологий высоконадежной биометрии не имеют, однако они получат подобные технологии преобразования биометрии в ключ через несколько лет. Политически целесообразно опережать США и страны НАТО по разработке технологий высоконадежной биометрической авторизации ЭЦП, процедур голосования и других процедур принятия ответственных решений в гражданских и военных приложениях. Разработка Россией нового поколения процедур голосования с высоконадежной биометрической авторизацией позволит России существенно изменить свой политико-технологический имидж и поставить под сомнение превосходства США в технологическом отношении и в отношении обеспечения механизмами электронной демократии свого населения.

ЛИТЕРАТУРА:

1. ГОСТ Р 53633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

Технология биометрической идентификации обеспечения анонимности больных при ведении электронных историй социально значимых заболеваний.

Статья журнала «Современные технологии безопасности»
Иванов А.И., Рыбалкин С.Б.

В статье показано, что размещение биометрического образа человека в нейросетевом контейнере позволяет обеспечить анонимность больного и в то же время исключить возможность злоупотреблений своей анонимностью со стороны больного. Анонимный больной не может в место себя послать другого человека, так как тот не сможет пройти высоконадежную нейросетевую аутентификацию. И врач и больной одновременно оказываются защищены от возможных взаимных злоупотреблений.

Конституция Российской Федерации гарантирует всем нам доступ к информации о своем здоровье и одновременно сохранение врачебной тайны. Совместить свободный доступ к информации с сохранением врачебной тайны далеко не всегда возможно. Эти требования противоречивы, возникает классическое противоречие между свойствами доступности и конфиденциальности информации. Особую остроту эта проблема приобретает при лечения социально значимых заболеваний. В контексте борьбы с социально значимыми заболеваниями медицинскому персоналу приходится сталкиваться с нежеланием пациентов обращаться в лечебные учреждения. В частности при венерических заболеваниях больные часто занимаются самолечением или обращаются к частным «врачам», без дипломов или с сомнительной репутацией. Все это является следствием недоверия пациентов существующим механизмам обеспечения конфиденциальности медицинской информации. Последнее приводит к вероятному осложнению болезни у пациента из-за неквалифицированной медицинской помощи и к повышению вероятности инфицирования им окружающих.

Не смотря на очевидные успехи информатизации медицины, в частности ее переход на электронный документооборот, проблема обеспечения права граждан на конфиденциальность их личной медицинской информации (на врачебную тайну) только усугубляется. Электронная история болезни (любая электронная информация) гораздо более уязвима в сравнении с бумажной историей болезни. Красть бумажный архив историй болезней всей поликлиники бессмысленно – это бесполезная и крайне тяжелая работа. Электронный архив – это совсем другое дело, это уже ценная информация, размещаемая на компактном носителе. Электронный медицинский документооборот резко обостряет проблему конфиденциальности медицинской информации. Одним из путей решения этой проблемы является ее обезличивание (обеспечение анонимности пациентов). Если по электронной истории болезни невозможно определить кому она принадлежит, то шифровать информацию или тратить деньги на ее иную защиту нет необходимости. Одним из первых российских документов рассматривающих обезличивание документооборота как средство обеспечения конфиденциальности личной информации является Федеральный Закон «О персональных данных» [1].

Особенно гарантированная анонимность пациентов необходима для эффективной борьбы общества с социально значимыми заболеваниями. Только в том случае, когда больной будет абсолютно уверен в сохранении его анонимности, он будет активно сотрудничать с органами здравоохранения. В связи с этим необходимо создание специальных механизмов обеспечения анонимной идентификации заболевшего. Следует подчеркнуть, что предшествующие бумажные технологии ведения медицинского документооборота (регистрации, идентификации, выдачи справок и заключений, ведения историй болезни) не могли одновременно обеспечить полноту сведений, достоверности сведений, а так же анонимность их источника.

Кратко техническая суть проблемы отражается в противоречивом сочетании терминов «анонимная идентификация». Идентифицировать человека в обычном понимании этого термина означает узнать его, убедиться в том, что это именно тот конкретный человек с конкретным именем, фамилией, отчеством, местом жительства. Анонимная идентификация означает совсем иное. При анонимной идентификации мы должны точно знать, что перед нами находится именно

тот человек, который когда то был зарегистрирован под некоторым псевдонимом (отсутствует случайная или преднамеренная подмена больного, например с целью модификации его анализов).

Заметим, что традиционными методами идентификации человека по его паспорту или по его биометрическим данным надежно обеспечить анонимность больного невозможно. Выход из создавшегося положения может быть найден только при использовании новых технологий высоконадежной биометрико-нейросетевой идентификации человека [2, 3]. Новые технологии сводятся к тому, что используется большая сеть искусственных нейронов. Большая нейросеть автоматически обучается преобразовывать биометрический образ человека (например, рисунок отпечатка его пальца как это показано на рисунке 1) в некоторый код. Например, это может быть код учетной записи потенциального больного, обратившегося в больницу изъявившего желание сдать анализы. В этой ситуации учетная запись такого потенциально больного или код его регистрации может быть следующим: «Сергей, обращение 20.04.07 в 14 ^{35}, г. Пенза, Куйбышева 33, врач С.Б.Рыбалкин» (смотри рис. 1). При использовании искусственной нейронной сети с 512 выходами учетная запись может иметь длину до 64 знаков.

Рис. 1. Анонимная биометрическая идентификация больного с сокрытием его биометрического образа в параметрах нейросетевого преобразователя

После обучения нейронной сети биометрический образ потенциального больного гарантированно уничтожается, а большая нейросеть, обученная его распознавать и соответствующая учетная запись размещаются в электронном документе [4] в электронной истории болезни потенциального больного. Все эти предосторожности позволяют с одной стороны сохранить анонимность больного, а с другой стороны защищают врача от злоупотреблений со стороны потенциальных больных. Потенциальный больной может попытаться выдать себя за другого человека или подменить себя другим человеком при сдаче очередных анализов. Все эти злоупотребления исключены при использовании средств высоконадежной биометрико-нейросетевой идентификации [3, 4].

Безопасная структура ведения электронного долопроизводства внутри лечебного учреждения отображена на рисунке 2. После анонимной биометрической регистрации потенциальный больной перед каждым анализом должен биометрически подтвердить себя. В нашем случае он должен предъявить свой палец для опознания в присутствии проверяющего (должностного лица принимающего от больного биоматериалы на анализ). Если пришедший сдавать биоматериалы (кровь, мочу, соскоб ткани,…) действительно тот, кто ранее зарегистрировался, то на выходах нейросети появится код, соответствующий учетной записи в направлении врача. Несовпадение кода в нескольких символах свидетельствует о незначительных

ошибках нейросети из-за незначительных смещений пальца, необходимо повторно приложить палец к сканеру. Если код не читается и состоит из случайных символов, то перед нами попутка обмана или грубая ошибка (к сканеру приложен не тот палец).

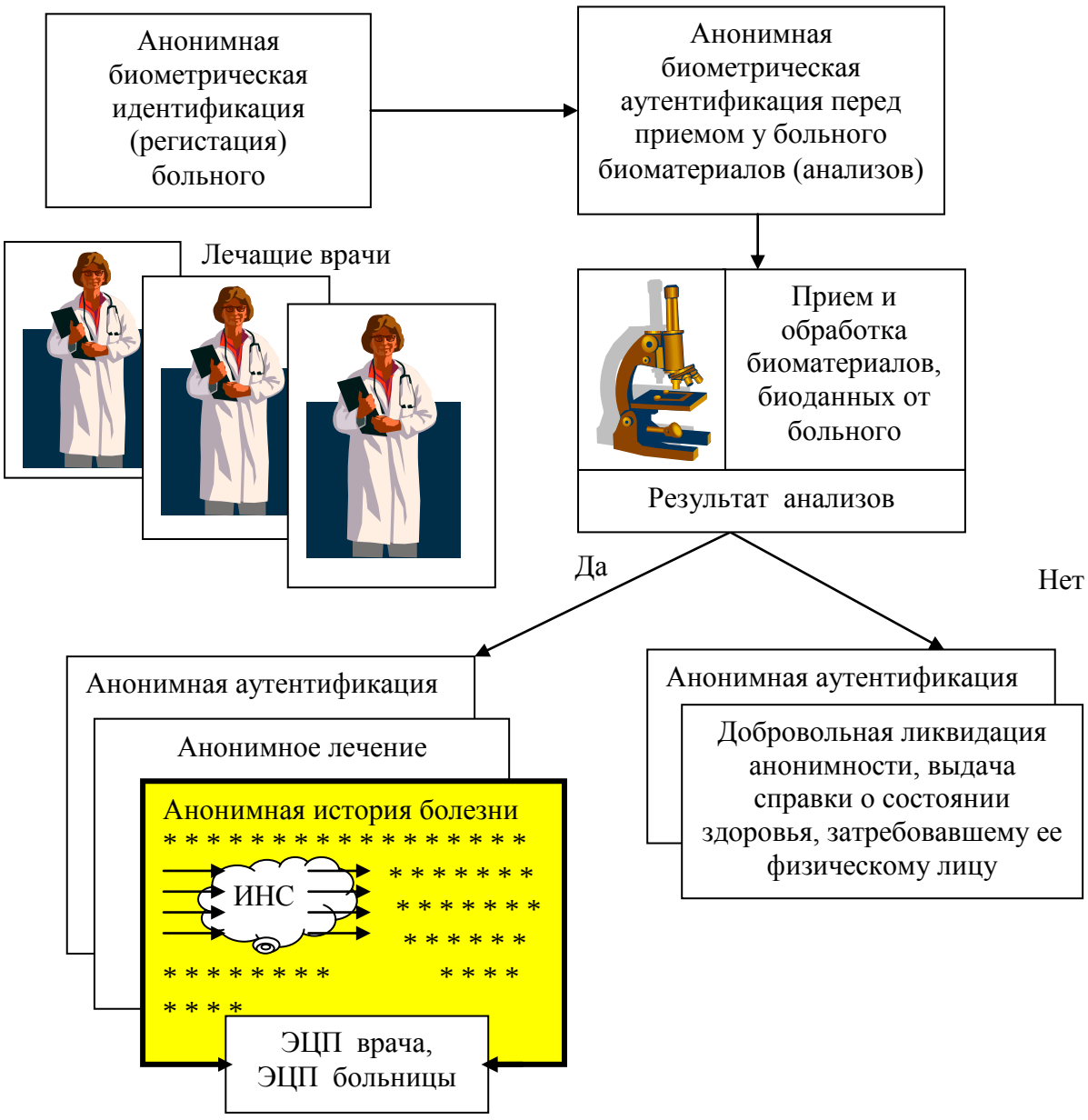


Рис. 2. Технология обеспечения анонимности больного при ведении медицинского документооборота при высокой степени авторизации больного

Заметим, что идентификация больного может быть осуществлена при его регистрации с использованием любого биометрического образа. Так в работе [5] использование для анонимной идентификации рукописной подписи больного. Может быть использована любая из современных биометрических технологий [2], хранение биометрического образа в нейросетевом контейнере гарантирует анонимность проверяемого.

После того как биометериалы для анализа приняты и помечены учетной записью они должны поступить на обработку и через наперед заданное технологическое время будет получен результат анализа. В случае отрицательного результата (социально значимое заболевание не обнаружено) несостоявшийся больной имеет право раскрыть свою анонимность по своему паспорту и получить на свое подлинное имя заверенную справку о его состоянии здоровья на текущий момент.

В случае, если результат анализов положителен (СПИД, венерическое заболевание,…) больной встает перед дилеммой: начать лечение в медучреждении или идти к

частнопрактикующему врачу. В первом случае законодательство требует от больного раскрытия его анонимности лечащему врачу при сохранении в тайне его имени для всего другого персонала лечебного учреждения. Возможны два пути реализации этого (смотри рисунок 3.)

Если больной не доверяет лечащему врачу, то он может обратиться к независимому нотариусу. В этом случае хранить тайну имени больного должен нотариус, однако для соблюдения буквы закона нотариус должен снять ксерокопию паспорта больного, запечатать ее в конверт, на конверте нанести требующуюся учетную запись. Все это предполагает, что у нотариуса есть не только лицензия на его деятельность, но и электронный документ из лечебного учреждения с нейросетевым контейнером тайного биометрического образа больного. Перед опечатыванием конверта нотариус должен проверить биометрию больного и нанести на конверт учетную запись выходного кода обученной нейронной сети. Больной опечатанный конверт должен передать врачу, который имеет право вскрыть его только в присутствии судьи или прокурора (оформляется, соответствующий акт вскрытия на основе, соответствующего, постановления).

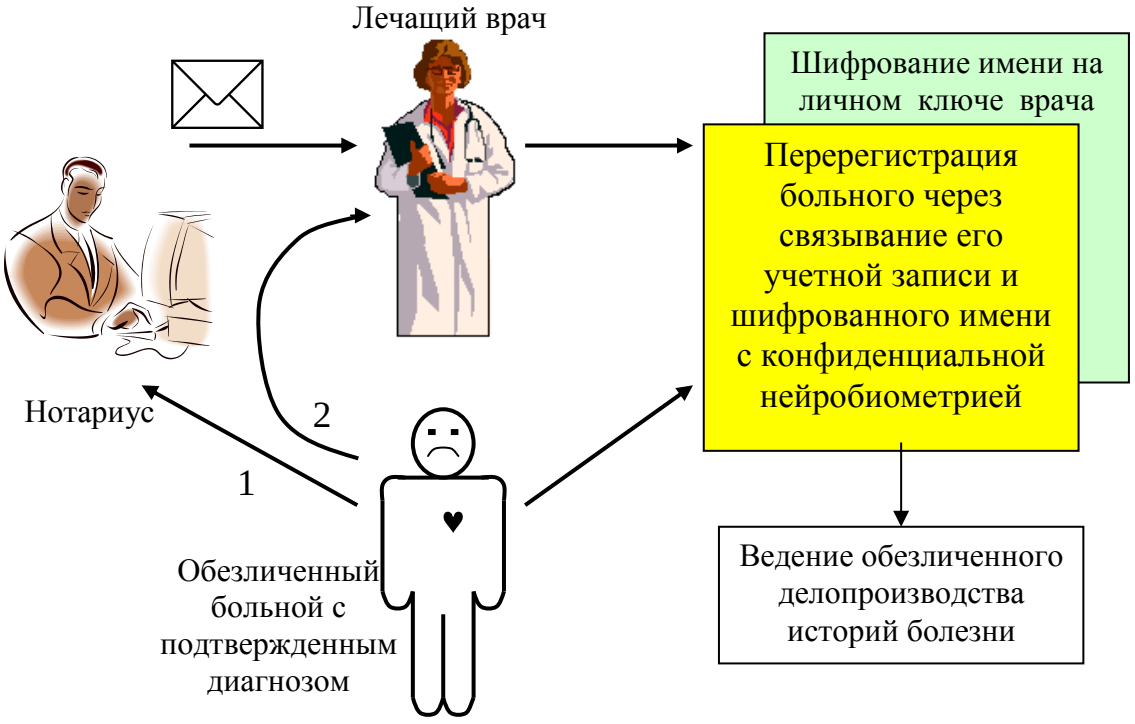


Рис. 3. Анонимная перерегистрация больного по его псевдониму и конфиденциальной биометрии с возможностью раскрытия анонимности в установленном законодательством порядке

Очевидно, что описанная выше процедура гарантированного нотариусом сохранения анонимности применима только для ВИП персон и людей неадекватно сильно заботящихся о своей анонимности. Для подавляющего большинства граждан РФ клятвы Гиппократа и порядочности лечащего врача в сочетании с системой оргтехмероприятий по сохранению анонимности больного будет вполне достаточно. В связи с этим большинство граждан будет открывать свою анонимность лечащему врачу, который должен зашифровать эту конфиденциальную информацию на своем личном ключа формирования ЭЦП, либо на производном ключе от ключа формирования ЭЦП врача. Тогда эта конфиденциальная информация будет присутствовать во множестве электронных документов медицинской отчетности, однако раскрыть ее (расшифровать шифротекст) сможет только лечащий врач. Естественно, что в этой цепочке сохранения анонимности пациентов лечащий врач начинает играть главную роль. То есть лечащий врач должен быть обеспечен средствами безопасного хранения его личного ключа, например в форме того же нейросетевого преобразователя биометрия-код, выполненного в мобильном (носимом в кармане) варианте в соответствии с требованиями нашего национального стандарта защиты информации [3].

Таким образом, требования Закона «О персональных данных» [1] технически выполнимы в контексте ведения медицинского документооборота. При этом обычное шифрование на общем

ключе всех данных делает медицинский документооборот практически бесполезным (труднонедоступным для исполнителей) из-за высоких требований к хранению ключей шифрования. Выход только один – необходимо привлекать новые технологии высоконадежной биометрико-нейросетевой защиты информации. Традиционные технологии криптографической защиты информации при массовом использовании становятся слишком тяжелыми. Необходимо защищать медицинскую информацию ее обезличиванием дополненным высоконадежной анонимной биометрико-нейросетевой идентификацией.

Внедрение новых технологий в медицинский документооборот является крайней необходимостью и, видимо, должно начинаться с разработки концепции по его обезличиванию и биометрической поддержке процедур анонимной идентификации. Для ведения работ предполагается привлекать, создаваемый в настоящее время инновационный фонд Пензенской области, который предположительно объединит усилия ряда пензенских предприятий по разработке и внедрению новых биометрических технологий. Пилотный проект новой системы ведения анонимного электронного документооборота с биометрической идентификацией больных предполагается запустить на базе ГУЗ "Пензенский областной центр специализированных видов медицинской помощи" в период 2009-2010 г.

ЛИТЕРАТУРА:

1. Закон РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ
2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
3. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
4. RU 2 292 079 - патент РФ на изобретение: «Способ идентификации человека по его биометрическому образу», авторы: Ефимов О.В., Иванов А.И., Фунтиков В.А., патентообладатель ФГУП «ПНИЭИ» (RU), приоритет от 02.02.2005.
5. Рыбалкин С.Б., Иванов А.И. Технология биометрической идентификации, обеспечивающая анонимность больных при ведении электронных историй социально значимых заболеваний /Современные технологии безопасности 2006г., № 3,4 (18,19), с.55-57.

Электронный документооборот предприятия с биометрической авторизацией криптоформирователей ЭЦП служащих

Статья журнала «Современные технологии безопасности»
Фунтиков В.А., Трифонов С.Е., Фунтиков Д.А., Иванов А.И.

В настоящее время идут активные процессы информатизации общества. Одной из важнейших является технология массового использования электронных цифровых подписей [1]. По всей России предполагается развернуть систему удостоверяющих центров открытых ключей и тем самым сделать массовый электронный документооборот в регионах юридически значимым. Принята «Концепция создания, функционирования и развития системы удостоверяющих центров органов государственной власти России».

При создании систем массового электронного документооборота не следует стремиться вводить юридически значимый документооборот в тех контрольных точках, где ранее не было обычного юридически значимого бумажного документооборота. Например, сегодня на любом предприятии формируется множество документов, однако только примерно 1% из них после, согласований, изменений, утверждений в конечном итоге становятся юридически значимыми документами (приказами, письмами, договорами,…). То есть, необходимо строго разделить внутренний служебный документооборот предприятия и юридически значимый документооборот.

При организации внутреннего документооборота не следует нарушать сложившуюся практику и загружать служащих предприятия работой с сертифицированными программными средствами формирования ЭЦП служащего. Любой служащий, находящийся на ответственной должности несомненно должен поддерживать внутренний электронный документооборот своего предприятия, создавать и подписывать свои электронные документы, но эти электронные документы должны приобретать юридическую значимость только после их прохождения полного цикла и заверения их «ЭЛЕКТРОННЫМ НОТАРИУСОМ предприятия». Типовая схема организации внутреннего электронного документооборота предприятия приведена на рисунке 1.

Из рисунка 1 видно, что на типовом предприятии должно быть организовано порядка 100 рабочих мест, оснащенных «формирователями личной ЭЦП служащего» не подлежащих сертификации с длинной ключа формирования ЭЦП не более 112 бит. Сертифицированных криптоформирователей юридически значимой ЭЦП предприятия должно быть примерно в 100 раз меньше. На рисунке 1, только один формировать ЭЦП электронного нотариуса (электронного секретаря) сертифицирован и имеет открытый ключ, зарегистрированный в региональном или национальном удостоверяющем центре. Поддерживается аналогия с печатью учреждения (предприятия), только она одна соответствующим образом зарегистрирована. Личные печати служащих могут существовать, но имеют ограниченное хождение только в нутрии предприятия (контролируются, проверяются, выдаются в строго установленном порядке).

В целом технология формирования юридически значимого электронного документа сводится к оформлению его служащим (служащими) в течение одной или нескольких итераций. Каждая итерация подписывается служащими их личными ЭЦП, документируется в архиве и не является юридически значимой. Только после прохождения всего цикла согласований, проверок, утверждений (появляется несколько ЭЦП нескольких лиц) формируется окончательный вариант юридически значимого документа, подписанный ЭЦП последнего исполнителя и ЭЦП нотариуса предприятия.

«Электронный нотариус предприятия» перед тем как сформировать ЭЦП юридически значимую ЭЦП предприятия под беем или иным документом должен проверить его историю (убедиться в подлинности всех ЭЦП служащих, принявших участие в создании документа). То есть предприятие должно иметь свой внутренний механизм контроля подлинности ЭЦП внутреннего документооборота. Эта ситуация отражена на рисунке 1. Создать программное обеспечение, реализующее технологию поддержки внутреннего документооборота предприятия технически вполне возможно, однако при этом нельзя опираться только на применение криптографических технологий, так как они не могут решить проблему безопасного хранения ключей или безопасного связывания ключей с биометрией служащего.

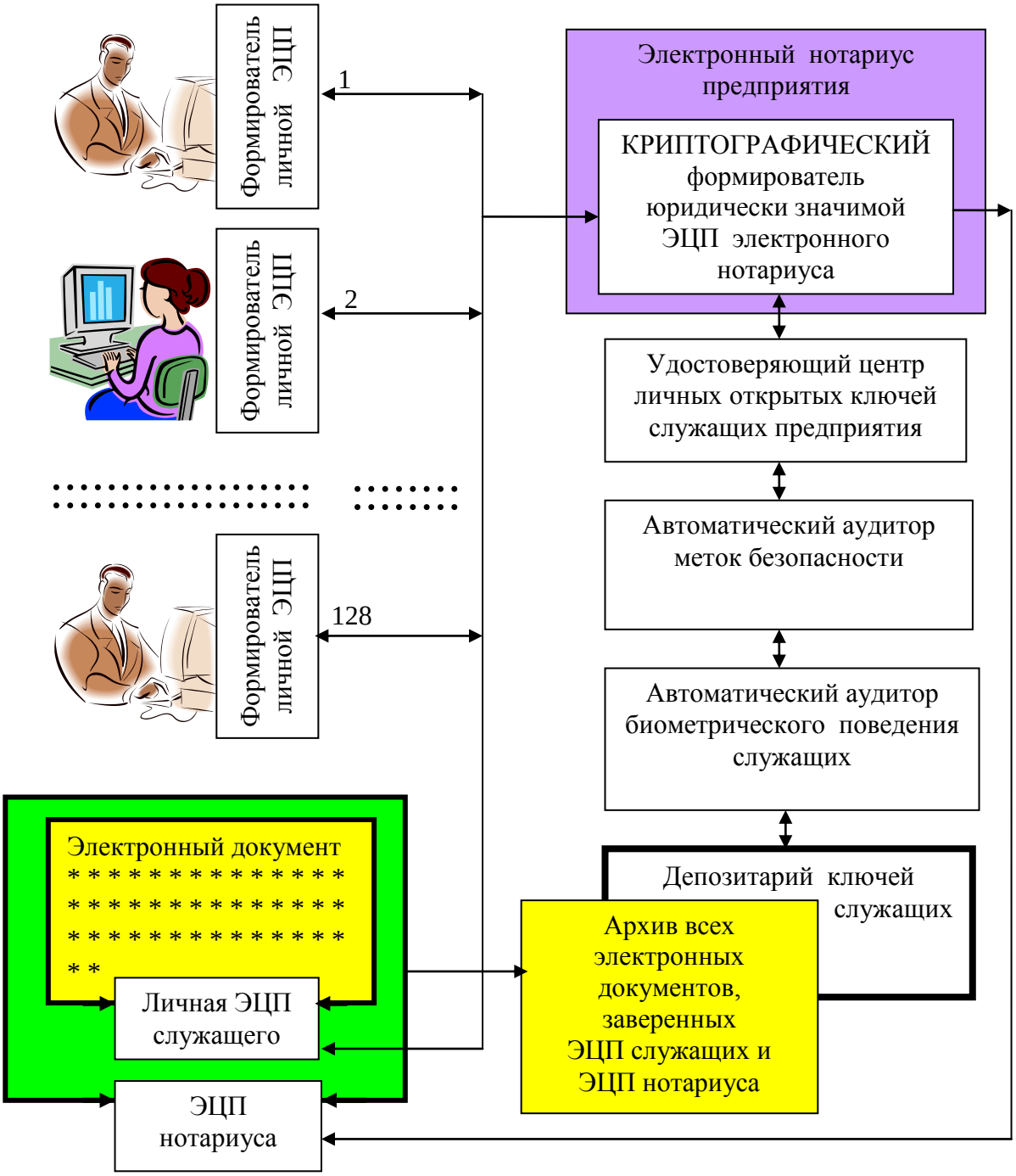


Рис. 1. Организация юридически значимого документооборота с двойным охватом электронного документа личной ЭЦП служащего и ЭЦП электронного нотариуса предприятия

Одной из наиболее острых проблем формирования ЭЦП служащих является надежная авторизация подписывающего. К сожалению, служащие не редко передают друг другу свои полномочия. Например, служащий может доверить формирование его ЭЦП своему подчиненному, набиравшему ранее документ на ПЭВМ. Привлечение менее квалифицированного служащего для выполнение неквалифицированной работы следует приветствовать, но доверять кому либо формирование своей ЭЦП категорически нельзя. Надежная технология должна исключать такую возможность.

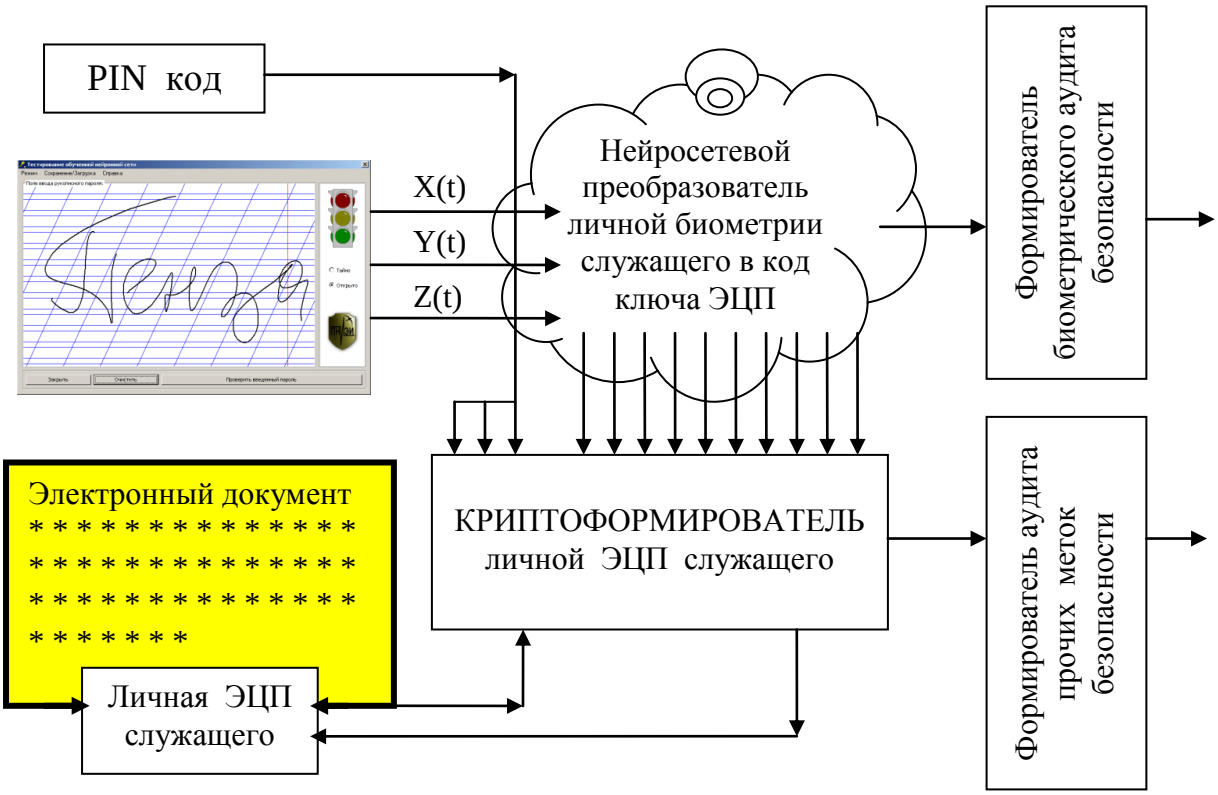


Рис. 2. Биометрико-нейросетевой криптоформирователь личной ЭЦП служащего с высокой степенью авторизации

Для того, что бы существенно повысить уровень авторизации управления личными формирователями ЭЦП необходимо привлечение современных биометрических технологий высоконадежной аутентификации [2, 3]. Одна из таких технологий, построенная на анализе динамики рукописного почерка отражена на рисунке 2. Каждый из нас имеет уникальный рукописный почерк. На этом построена процедура подписывания автографом обычных бумажных документов. Исследования, проведенные в России и за рубежом показали, что наиболее удобен для автоматической идентификации человека анализ динамики «живой» рукописной надписи. При воспроизведении надписи осуществляется оцифровка колебаний пера X(t), Y(t) и давления пера на подложку Z(t). Эти оцифрованные данные являются биометрическим образом пользователя, используя несколько биометрических образов удается автоматически обучить искусственную нейронную сеть преобразовывать образ «Свой» в ключ формирования ЭЦП пользователя.

Преимуществом новой нейросетевой технологии [2, 3] является прежде всего то, что отпадает необходимость хранения ключа формирования ЭЦП в программе. В программе храниться только сеть искусственных нейронов, на выходах этой нейросети ключ может появиться только как отклик на биометрический образ «Свой». Если на входы нейросети подать случайный биометрический образ «Чужой», то на выходах нейросети появится случайный выходной код. При сохранении в тайне биометрического рукописно пароля подобная система биометрической защиты обеспечивает стойкость к атакам подбора на уровне 100 000 000 000 попыток до первой удачи. Если же рукописный пароль скомпрометирован (один служащий показал свой рукописный пароль другому служащему), то «Чужому» потребуется от 100 до 10 000 попыток воспроизведения «Чужого» рукописного пароля.

Для исключения служебных злоупотреблений биометрико-нейросетевой криптоформирователь личной ЭЦП служащего должен иметь блок формирования биометрического аудита. Очевидно, что многократные попытки сформировать «Чужую» ЭЦП другим человеком могут быть достаточно легко обнаружены [4], разбором биометрического аудита. В связи с этим личный формирователь ЭЦП служащего должен иметь блок формирования биометрического аудита (см. рисунок 2), а «электронный нотариус предприятия» перед

подтверждением внешней легитимности внутреннего электронного документа должен проконсультироваться с автоматическим аудитором биометрических данных (см. рисунок 1).

Кроме формирования биометрического аудита личный формирователь ЭЦП служащего должен дополнительно формировать аудит прочих меток безопасности. Например, к прочим меткам безопасности могут быть отнесены время формирования ЭЦП документа, текущее состояние вычислительной среды (портрет параллельных вычислительных процессов на ПЭВМ), данные о предшествующей клавиатурной активности и иной активности по предшествующим операциям. Сделать систему надежной, удается только совместив личные формирователи ЭЦП служащих с надсистемой обеспечения информационной безопасности. Правильно выполненная система обеспечения информационной безопасности должна иметь свой удостоверяющий центр личных открытых ключей служащих предприятия, свой генератор пар ключей (открытых и тайных), свой депозитарий ключей, используемых и использовавшихся ранее на предприятии разными служащими.

Как уже было выше отмечено, объем ключевой информации внутренней системы электронного документооборота предприятия должен быть примерно в 100 раз выше, чем объем аналогичной информации, проходящей через удостоверяющие региональные центры. Все это делает задачу разработки системы внутреннего документооборота достаточно сложной, видимо с ней могут справится только организации, имеющие лицензии ФСТЭК России, ядро программного обеспечения в виде «формирователя ЭЦП электронного нотариуса» должно строиться на основе только сертифицированного в установленном порядке программного обеспечения. Множество криптоформирователей личных ЭЦП служащих для внутреннего использования не формируют юридически значимых документов и не подлежат сертификации как независимые программные продукты в соответствии с «Постановлением Правительства РФ» от 23.09.2002 № 691. Вполне возможно, что «электронный нотариус предприятия» (электронный секретарь предприятия) окажутся единственными программами, нуждающимися в полноценной сертификации и регистрации их открытых ключей вне предприятия. Последнее позволяет существенно снизить издержки предприятия и упростить работу по формированию внутреннего электронного документооборота.

ЛИТЕРАТУРА:

1. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
3. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
4. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во Пензенского гос. ун-та, 2000. – 188 с.

Идентификация человека по рисунку отпечатка пальца с размещением личных биометрических данных в нейросетевом контейнере

Статья журнала «Нейрокомпьютеры»
Д. А. Фунтиков

В настоящее время активно используются биометрические средства аутентификации при доступе к информации находящейся на ПЭВМ, ноутбуках, USB-flash, при удаленной идентификации и при доступе к ключу формирования ЭЦП. Подобные средства могут иметь разные биометрические датчики ввода информации, однако на данный момент наибольший объем рынка (от 50 до 80% по разным оценкам) составляют средства, использующие ввод данных о рисунке отпечатка пальца человека. Этот сектор рынка биометрических устройств сегодня поддерживается практически всеми фирмами, профессионально занимающимися средствами биометрического ограничения доступа. Применяются на практике три типа сканеров отпечатков пальцев, построенных на разных физических принципах: оптические, емкостные сканеры, сканеры с радиочастотным считыванием.

Как правило, представленные на рынке продукты биометрической защиты построены с использованием метода «разблокировки ключа». Ключ и биометрический образ хранятся раздельно в системе. Для получения доступа к ключу необходимо пройти биометрическую идентификацию, при этом решение о разблокировки ключа принимается на основе классического решающего правила, имеющего «последний бит» (да/нет).

В случае реализации программным способом процедуры обработки данных, возникает две основных проблемы:

биометрический шаблон не защищен, может быть скомпрометирован или подменен;

программная биометрическая защита оказывается крайне слабой из-за подмены «последнего бита». «Последний бит» обнаруживается подбором, после его обнаружения хакер для тиражирования успеха выпускает вирус, который позволяет взламывать действующую защиту и получать доступ к конфиденциальной информации.

Одновременно решить обе проблемы удается, если перейти от классической обработки [18, 19] к использованию высоконадежного нейросетевого преобразователя биометрия-код, выполненного по требованиям нашего национального стандарта ГОСТ Р 52633-2006 [2].

При реализации нейросетвого преобразователя возникает проблема недостаточного объема данных, извлекаемых из рисунка отпечатка пальца. Обычно анализируются:

контрольные точки, находящиеся в окончаниях или разветвлениях папиллярных линий, так называемые минуции (ГОСТ Р ИСО/МЭК 19794-2-2005 [2]);

ширина папиллярных линий, впадин в районе контрольной точки;

плотность пор в области контрольной точки;

направление папиллярных линий.

Все перечисленные выше параметры обычно измеряются в окрестностях особых точек (минуции), а биометрический шаблон [20] рисунка отпечатка пальца обычно формируется в виде списка наиболее часто встречающихся особых точек (минуций) с описанием их окрестностей. Список особых точек отпечатка пальца нуждается в обязательной защите [20], так как по нему легко может быть найден владелец отпечатка пальца.

Реализация нейросетевого преобразователя биометрия-код показала, что объем обрабатываемой информации должен быть многократно увеличен путем введения дополнительных областей, не содержащих минуций. Производится контроль перечисленных выше параметров, как в областях, содержащих реальные минуций, так и в пустых областях, без особых точек. При этом внешний наблюдатель не знает, с какой контрольной областью он имеет дело: реальной минуций или пустой областью контроля параметров рисунка отпечатка пальца.

Объем обрабатываемой информации, при этом подходе к решению задачи, увеличивается в 3...4 раза, что позволяет улучшить стойкость нейросетевого преобразователя биометрия - код к атакам подбора за счет увеличения информативности биометрического образа. В качестве безопасного, действительно биометрического шаблона, нейросетевой преобразователь хранит расширенный список контролируемых областей. Добавления «пустых» областей в расширенный список

осуществляется с использованием генератора случайных чисел, что позволяет скрыть расположение реальных контрольных точек (минуций) и, тем самым, обеспечить анонимность пользователя.

Пример создания безопасного биометрического шаблона показан на рисунке 1.

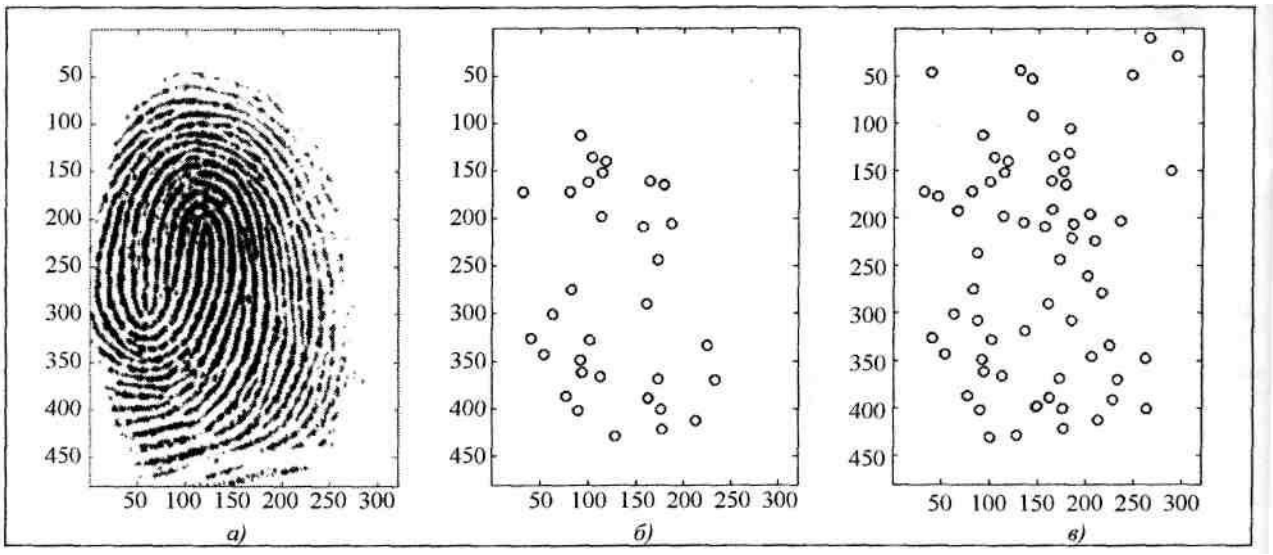


Рис. 1. Пример создания безопасного биометрического шаблона: *а* - изображение отпечатка пальца; *б* - места расположения реальных минуций, запоминаемых в обычном биометрическом шаблоне; *в* - безопасный биометрический шаблон, расширенный за счет дополнительных областей не содержащих минуций

Нейросетевой преобразователь биометрия-код обучают на выдачу заданного личного кода пользователя с использованием безопасного биометрического шаблона и нескольких отпечатков пальца пользователя. Используется алгоритм быстрого обучения [4], обеспечивающий обучение нейросети, содержащей от 240 до 360 входов и 256 выходов (каждый выход соответствует одному разряду 256 битного личного ключа).

Так, на рисунке 1,б отображены порядка 30 реальных минуций найденных в реальном отпечатке пальца, показанном на рисунке 1,а. Эти 30 реальных особых точки дополнены 30 мнимыми особыми точками, что дает 60 контрольных точек, отображенных на рисунке 1,е. При контроле всего 4 параметров каждой из 60 контрольных точек мы получаем нейросеть с 240 входами. Учет 6 параметров рисунка отпечатка пальца по каждой из 60 контрольных точек позволяет использовать нейронную сеть с 360 входами.

После обучения сети искусственных нейронов, данные о том, какая из контрольных точек содержит реальную минуцию, а какая ее не содержит, уничтожают, уничтожают также информацию о личном коде пользователя. Информация об обученной нейронной сети сохраняется в виде таблицы связей и весов нейронов этой сети, в виде так называемого «нейросетевого контейнера» [21].

Обучение нейросети происходит следующим образом:

Шаг 1. Пользователь предъявляет несколько отпечатков регистрируемого пальца, обычно от 10 до 15.

Шаг 2. В каждом отпечатке выполняется поиск минуций.

Шаг 3. Затем отпечатки выравниваются относительно найденных минуций. Создается множество *M(n),* в котором запоминаются координаты областей содержащих найденные минуции, где n общее количество таких областей.

Шаг 4. С помощью генератора случайных чисел задается множество *D(r),* в котором запоминаются координаты дополнительных контрольных областей, не пересекающихся с областями в множестве *M.* Для обеспечения стойкости безопасного биометрического шаблона необходимо чтобы *r>3n.*

Шаг 5. Далее создается безопасный биометрический шаблон путем объединения множеств *M* и D в множество *B(к),* где *к=n+r.* При этом задается определенный порядок следования областей множества B в соответствии с их координатами, например, слева направо и сверху вниз.

Шаг 6. Для каждого отпечатка пальца, участвующего в обучающей выборке, в каждой области из множества *B(к)* вычисляется вектор контролируемых биометрических параметров $I_к$, включающий:

наличие/отсутствие минуций в данной области;

среднюю ширину папиллярных линий и впадин;

плотность пор;

направление папиллярных линий;

Шаг 7. Набор, полученных векторов, используется для обучения двухслойной нейронной сети с 256 выходами, каждый выход соответствует определенному биту извлекаемого криптографического ключа пользователя или его длинного пароля доступа. После этого, автомат обучения должен добиться появления нужного кода на выходах нейронных сетей при предъявлении на их входы любого из набора векторов биометрических параметров из обучающей выборки «Свой». При предъявлении нейросети любого набора векторов биометрических параметров из выборки «Чужие», на выходах нейронной сети должны появляться случайные коды. На каждом из выходов должен появляться независимый «белый шум» двух равновероятных состояний «О» и «1». По требованиям ГОСТ Р 52633-2006 [2] допустимо появление корреляции между парами различных разрядов выходного кода, однако среднее значение модулей коэффициентов корреляции не должно превышать 0,15.

При аутентификации проверяемого рисунка отпечатка пальца сканируют этот рисунок, выравнивают рисунок относительно безопасного биометрического шаблона с использованием предварительно сохраненной в шаблоне вспомогательной информации. В качестве вспомогательной информации могут быть использованы координаты точек наибольшей кривизны папиллярных линий, данные о структуре поля направлений отпечатка или координаты трех-четырех минуций. Открытая часть шаблона не превышает 3% от объема полного безопасного биометрического шаблона. Далее, используя сам безопасный биометрический шаблон, выделяют на нем контролируемые области, вычисляют параметры контролируемых областей и подают их на соответствующий вход нейронной сети, а нейронная сеть преобразует входные данные в некоторый выходной код.

За счет того, что исчезает «последний бит» (появляется 256 «последних бит») снимется проблема тиражирования успеха хакерами при взломе одной программы. Если каждая программа имеет свой ключ, подбор ключа является задачей с гарантированно высокой вычислительной сложностью. После взлома биометрической защиты одной программы, создать на основе полученного опыта универсальную программу для автоматического взлома программ других пользователей нельзя.

Так как параметры отпечатка пальца своего пользователя связаны с его личным ключом с помощью безопасного биометрического шаблона, таблицы связей и весов нейронов нейросетевого преобразователя, обеспечивается высокий уровень конфиденциальности, анонимности, обезличенное™ персональных биометрических данных пользователя. Это позволяет выполнять требования закона «О персональных данных», РД ФСТЭК России и ГОСТ Р 52633-2006 [2].

ЛИТЕРАТУРА

1. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.

2. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации /Пенза-2006 г., Издательство Пензенского государственного университета., 161 с.

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

4. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

5. ГОСТ Р 52633.1 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

6. ГОСТ Р 52633.2 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

7. Иванов А.И. Эволюция паспортов и удостоверений личности: замена биометрической органолептики на биометрическую автоматику. /Защита информации. INSIDE. 2006 г. №2, с. 22-26.
8. Иванов А.И. ГОСТ Р 52633-2006: Россия достроила фундамент мировой цифровой демократии, сделав его устойчивым! //«Защита информации ИНСАЙД» № 3 2007
9. Фунтиков В.А., Ефимов О.В., Иванов А.И. Биометрико-нейросетевое управление криптографическими механизмами защиты информации. «Нейрокомпьютеры: разработка, применение» №12 2007, с.6-8.

Перспективы использования флешпроцессора с биометрико-криптографическими механизмами аутентификации сотрудников МВД РФ для хранения служебной информации

Статья журнала «Специальная техника средств связи»
А.В. Колючкин, С.Е. Трифонов, И.Г. Монахова

В настоящее время в нашей стране идет бурный процесс информатизации практически всех сфер общественной деятельности, в том числе и в МВД России. Хотя бумажный документооборот все еще преобладает над электронным документооборотом в силу довольно слабой распространенности последнего, объем корпоративных электронных документов удваивается каждые три года. В связи с этим все более актуальной становится задача разработки индивидуальных малогабаритных (портативных) защищенных от НСД устройств пользователя для выполнения криптографических преобразований информации в процессе информационного обмена, а также для хранения служебной информации сотрудников МВД России, в том числе в оперативной обстановке.

В настоящее время предприятие ФГУП "ПНИЭИ" (г. Пенза) проводит ряд разработок, направленных на создание изолированной программно-аппаратной среды для выполнения функций криптографической обработки информации на базе отечественных алгоритмов. В том числе защищенные от НСД индивидуальные малогабаритные (портативные) устройства пользователя - флешпроцессоры.

Малогабаритные портативные устройства представляют собой вычислительную программно-аппаратную среду на базе встроенных микроконтроллера и Flash-памяти большого объема (до 1024 Мбайт), имеют последовательный стык ввода/вывода USB 1.1 или 2.0. С целью защиты от НСД конструкция выполнена в виде неразборного малогабаритного корпуса с внешним разъемом USB-A.

Кроме того, в устройствах применяется ряд дополнительных технических решений, позволяющих обеспечить защиту от НСД даже в случае взлома корпуса и доступа к программно-аппаратным ресурсам устройства.

Внешний вид устройства и его габаритные размеры приведен на рисунке 1. Технические характеристики данной программно-аппаратной среды приведены в таблице 1.

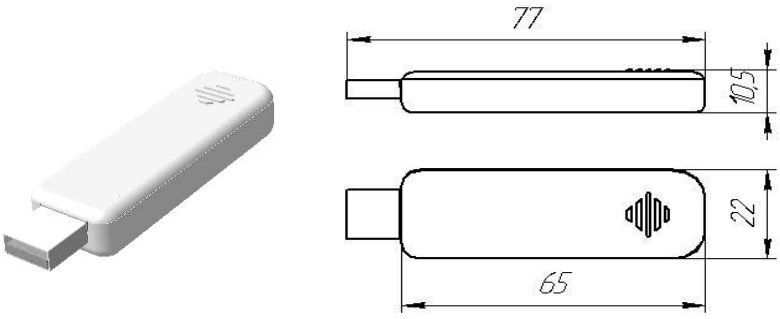


Рис. 1. Внешний вид устройства и его габаритные размеры

Таблица №1

Архитектура	Накопитель на базе Flash-памяти, работающий под управлением микроконтроллера
Исполнение	Малогабаритный корпус с USB-разъемом типа А
Емкость памяти	64, 128,256, 512, 1024 Мбайт

Материал корпуса	Пластмасса, металл (в зависимости от желания заказчика)
Тип микроконтроллера	1886ВЕ3У (отечественный микроконтроллер со встроенным ядром криптографической обработки информации)
Тактовая частота микроконтроллера	48 МГц
Протокол обмена с устройствами	USB 1.1, интерфейс точка-точка
Скорость обмена	12 Мбит/с
Логические уровни обмена	Логические уровни USB-интерфейса
Вес, не более	20 г
Напряжение питания	5 В
Потребляемый ток, не более	100 мА
Рабочая температура	От –40 до +50 °С
Температура хранения	От –55 до +65 °С
Питание	От интерфейса USB
Количество перезаписей в одну ячейку памяти	Не менее 100 000
Срок хранения данных, не менее	10 лет

Данные устройства – малогабаритные вычислитель-носители (МВН) – имеют следующие функциональные характеристики:

- защита от НСД криптографическими, алгоритмическими и физическими способами;
- возможность гарантированного стирания записанной информации (как выборочно, так и в полном объеме (аварийно));
- большой объем встроенной памяти (до 1 Гбайт), позволяющий хранить не только большой объем электронной информации, но и ключевой информации пользователя (ключи (открытые и закрытые) электронной цифровой подписи (ЭЦП) [1], сертификаты открытых ключей ЭЦП).

Созданный и рассмотренный задел может быть значительно расширен как функционально, так и по назначению.

Проработаны технологии встраивания в защищенную программно-аппаратную среду МВН (без увеличения его массогабаритных характеристик) средств криптографического преобразования информации с аппаратной поддержкой, для достижения высоких показателей производительности, включая алгоритм вычисления хэш-функций от сообщений произвольной длины согласно ГОСТ Р 34.11-94 [3] и алгоритм ЭЦП согласно ГОСТ Р 34.10-2001 [1].

Примерный перечень основных функциональных характеристик, которые могут быть обеспечены МВН [5]:

- обеспечение криптографической защиты информации пользователя (группы пользователей) в виде файлов или данных, а также защиты от несанкционированного доступа (НСД) к ресурсам и записанной информации с помощью пароля;
- вычисление хеш-функции согласно ГОСТ Р 34.11-94 [3];
- вычисление электронной цифровой подписи согласно ГОСТ Р 34.10-2001 [1];
- обеспечение криптографических преобразований по алгоритму шифрования согласно ГОСТ 28147-89 [2];
- поддерживаемые платформы: Windows 9x/2000/XP, Linux, МСВС 3.0, DOS 6.22;
- наличие встроенной системы организации файлов;
- возможность внутреннего 100% резервирования программно-аппаратной среды.
- Благодаря этому возможны следующие модификации МВН по назначению:
- МВН аутентификации пользователя по паролю и определения выделенных каждому пользователю полномочий;
- МВН хранения ключей пользователя в защищенной среде с доступом по паролю;

- МВН индивидуальной криптографической защиты информации пользователя с возможностью шифрования/дешифрования файлов и данных пользователя в режимах, как «на проходе» (ПЭВМ⇒Носитель⇒ПЭВМ), так и в режимах с сохранением информации в физически защищенной от НСД среде МВН в зашифрованном виде.

Показатели производительности МВН:

- производительность шифрования информации – не менее 500-600 кбайт/с;
- производительность хэширования информации – не менее 300 кбайт/с;
- время вычисления ЭЦП – не более 1,2 сек;
- время проверки ЭЦП – не более 2,4 сек;
- ресурс формирования ключевых пар (ключ ЭЦП и ключ проверки ЭЦП) – 2 млн. пар.

Начиная с 2001 г. на предприятии ведутся исследования по биометрической идентификации личности с применением технологий искусственных нейросетей. При этом проблемы биометрии на предприятии рассматриваются в непосредственной взаимосвязи с методами криптографической защиты на базе отечественных алгоритмов.

В этой сфере ФГУП "ПНИЭИ" принимал непосредственное участие в разработке государственного стандарта [4] ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

В настоящее время ФГУП "ПНИЭИ" прорабатывает варианты встраивания нейронных сетей в изолированную программно-аппаратную среду МВН в целях внедрения передовых биометрико-криптографических технологий высоконадежной аутентификации и авторизации пользователей в соответствии с их биометрическими параметрами, включающими тайный образ [5]. При этом сам пользователь является носителем криптографического ключа, а доступ его к ресурсам МВН может быть осуществлен только после предъявления биометрических параметров (речь, отпечатки пальцев).

Это направление ФГУП «ПНИЭИ» рассматривает в качестве перспективного, и в настоящее время изготовлен действующий макетный образец. На рисунке 2 приведены эскизы трех возможных модификаций данных устройств.

Рис. 2. Эскизы трех модификаций флэшпроцессоров

Применение выше описанных МВН в системах управления обменом электронной информацией с юридически значимой ЭЦП [1], к которым предъявляются требования информационной безопасности, позволяет достигнуть качественно новых тактико-технических показателей [5].

С помощью инфраструктуры УЦ [6] ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Однако собственноручная подпись является индивидуальным биометрическим показателем человека, содержащим его тайный образ, а ЭЦП – результат совместной деятельности УЦ, выдающего сертификат на основе данных центра регистрации, и технических средств пользователя, осуществляющих работу с закрытым или открытым ключом ЭЦП [1]. В последнем случае имеет место «опосредованность» пользователя, чьи биометрические параметры анализируются только однократно в процессе первоначальной регистрации, как правило, на основе его регистрационных, учетных, паспортных и т.п.

В этой связи большую актуальность имеет задача внедрения биометрических параметров пользователя при формировании каждого электронного документа, а также их контроля при обращении или взаимодействии с УЦ, включая внедрение в сертификаты ключа подписи.

В этом случае может быть достигнута практически полная персонализация как всех действий при обращении к ресурсам ЭДО, так и электронных документов через индивидуальные биометрические параметры пользователей.

Рассмотрим подробнее вопрос применения МВН в системах управления электронным документооборотом и проблемы обеспечения безопасности в ЭДО с применением подобных изделий.

Под управлением электронным документооборотом в общем случае понимают весь комплекс процедур по организации составления, использования, хранения и обмена электронными документами.

Для создания и поддержания инфраструктуры электронного документооборота с ЭЦП, имеющей юридическую значимость, федеральный закон (ФЗ) [6] «Об электронной цифровой подписи» требует наличия третьей «арбитражной» доверенной для всех участников стороны – Удостоверяющего Центра (УЦ).

Основными функциями УЦ должны явиться:

- автоматизированное управление политикой безопасности, включая управление ключами и сертификатами участников;
- управление индивидуальной (персональной) информацией участников;
- удостоверение подлинности ЭЦП [1];
- юридически значимый разбор конфликтных ситуаций.

При этом компоненты УЦ могут носить территориально-распределенный характер, а инфраструктура УЦ может иметь иерархическую, многоуровневую структуру, отражающую особенности организации связи и управления в том или ином ведомстве.

Исходя из определения основных функций УЦ, следует, что инфраструктура открытых ключей, управляемая со стороны УЦ, есть набор служб безопасности, позволяющий использовать и управлять техникой криптографии с открытыми ключами, включая, в том числе, собственно ключи, сертификаты участников и политику администрирования.

Другими словами, инфраструктура открытых ключей есть система цифровых сертификатов, центров сертификации и других регистрационных центров, которые проверяют и идентифицируют каждую из сторон, вовлеченных в электронный информационный обмен, реализуя "иерархию доверия”.

Естественным требованием является то, что технология использования открытых ключей, применяемых в ЭЦП, должна интегрировать все функциональные области системы безопасности информации, соответствующей заданному уровню доверия.

Применительно к задачам организации сбора и обмена информацией в инфраструктурах открытых ключей следует обратить внимание, что большое значение должно иметь выполнение двух условий. С одной стороны, система безопасности должна обеспечивать необходимый уровень защищенности электронного информационного обмена, гарантирующего безопасность при всех видах атак как со стороны внешнего, так и внутреннего нарушителя. В то же время, наличие интегрированной подсистемы безопасности в системе электронного информационного обмена не должно приводить к усложнению работы пользователя, когда на него возлагается значительная часть управления безопасностью. Это создает большой ряд угроз информационной безопасности, но может также привести и к сбоям (системным отказам) в процессе электронного информационного обмена по вине пользователя.

Таким образом, имея в виду информационные системы с ЭДО с применением ЭЦП, в современной трактовке требование обеспечения защиты соответствующего уровня предполагает наличие подсистемы автоматизированного управления безопасностью, включая дистанционное управление шифрключами, ключами ЭЦП и сертификатами по каналам связи, в режимах «прозрачных» для пользователей. Поэтому на УЦ в системе ЭДО должны быть возложены дополнительные функции автоматизированного управления безопасностью. Только при выполнении этого требования могут быть созданы условия «погружения» технологий ЭЦП и функций УЦ в безопасную среду, стойкую к атакам квалифицированного нарушителя. При этом

следует иметь в виду, что особый класс нарушителя в системе ЭДО, имеющий значительный перечень существующих угроз безопасности, составляют внутренние нарушители, являющиеся пользователями системы и образовавшиеся вследствие явных и неявных компрометаций.

Указывая на интегрированный характер подсистемы обеспечения безопасности информации, необходимо обратить внимание также на следующий факт: подсистема безопасности, опираясь на единое ядро криптографической защиты, должна охватывать несколько уровней сетевого взаимодействия. Как показывает практика, минимально необходимыми в этом отношении являются прикладной (пользовательский) уровень и уровень сетевого управления (сетевой).

Для решения задачи НСД к информационным ресурсам и службам УЦ, а также в целях автоматизации процесса учета событий и организации аудита безопасности на заданную глубину во времени, в защищенной среде ЭДО должны быть выполнены три условия.

Во-первых, должна быть обеспечена доверенная и защищенная от НСД программно-аппаратная среда для каждой компоненты УЦ;

Вторым условием является персонализация всех действий обслуживающего персонала и администраторов по управлению УЦ на всех территориально-распределенных объектах с введением автоматизированного учета событий, защищенного от модификаций и несанкционированного уничтожения;

В-третьих, особую проблему составляет задача создания подсистемы управления ключами в защищенной системе электронного документооборота с применением ЭЦП. В целях обеспечения оперативности функционирования и живучести в системе должны быть предусмотрены технические решения, обеспечивающие как клиентские рабочие места ЭДО, так и компоненты УЦ возможностями децентрализованной генерации ключей ЭЦП (пар ключей ЭЦП: открытый ключ/закрытый ключ).

Таким образом, в целях эффективного решения рассмотренных вопросов и обозначенных проблем безопасности как внутри инфраструктуры УЦ, так и на клиентских рабочих местах ЭДО целесообразно применять СКЗИ, выполненные на базе изолированной, малогабаритной, многофункциональной, защищенной от НСД среды. Созданный ФГУП "ПНИЭИ" задел может быть также эффективно использован в целях создания УЦ и оснащения клиентских рабочих мест.

Большую актуальность при внедрении юридически значимой ЭЦП с электронным документооборотом имеет задача сопряжения с действующими системами электронного документооборота. Эта проблема может быть эффективно решена опять же с помощью клиентских МВН, реализующих функции криптопровайдера и выполненных в виде выделенной от абонентских станций, изолированной программно-аппаратной среды.

Отличительной особенностью действующей системы юридически значимого ЭДО с применением МВН-криптопровайдера является то, что все процессы криптографической обработки электронных документов осуществляются в изолированной и защищенной от НСД программно-аппаратной среде криптопровайдера, отделенной от общесистемной и операционной среды ПЭВМ или сопрягаемых изделий. Кроме того, шифрключи, включая ключи шифрования и ключи ЭЦП, никогда не покидают и не выводятся за пределы программно-аппаратной среды криптопровайдера в течение всего жизненного цикла и неизвестны даже пользователю СКЗИ.

Второй отличительной особенностью данного технического решения является то, что каждый абонент электронной почты или электронного документооборота может на рабочем месте произвольно во времени генерировать и менять ключи ЭЦП и может быть при этом уверен, что секретные ключи вычисления ЭЦП неизвестны никому, включая УЦ. Парадокс заключается в том, что секретный ключ вычисления ЭЦП остается неизвестным даже самому пользователю – ключ формируется и функционирует только в изолированной среде криптопровайдера, недоступной пользователю для непосредственного обращения.

В-третьих, принципиально важной тактико-технической характеристикой рассматриваемых технических решений, опять-таки в силу изолированности среды, отделенной от общесистемной среды ПЭВМ, является возможность достижения высоких уровней защищенности при минимальных затратах средств и времени на разработку. При этом практически не затрагивается операционная среда ПЭВМ и выполняемых в ней приложений. Например, ФГУП «ПНИЭИ» прорабатывает вопрос использования криптопровайдера в среде приложений электронного документооборота Lotus Notes или MS Docs Vision [5] для вычисления юридически значимой ЭЦП

согласно отечественному криптографическому алгоритму. При этом предполагается, что вся криптографическая обработка данных должна проходить в режимах «прозрачных» для пользователей.

В комплексе, по мнению ФГУП «ПНИЭИ», описанные технические решения на базе изолированной, малогабаритной, многофункциональной, защищенной от НСД среды позволят внедрить в интегрированной сети с электронным документооборотом новые принципы реализации политики безопасности с юридически значимой ЭЦП с максимальным использованием автоматизированных процессов управления и дистанционного мониторинга.

ЛИТЕРАТУРА:

1. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Формирование и проверка электронной цифровой подписи».
2. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
3. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования».
4. Первая редакция проекта ГОСТ Р (ТК 362) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005. 32 с. Публичное обсуждение начато с 9.09.05.
5. Отчеты НИР, ОКР.
6. Федеральный Закон «Об электронной цифровой подписи» от 10.01.2002 года №1-ФЗ

Сандарты высоконадежной биометрической аутентификации, разрабатываемые в рамках ГОСТ Р ТК 362 «Защита информации»

Национальные стандарты: ГОСТ Р 52633-2006, ГОСТ Р 52633.1, ГОСТ Р 52633.2, ГОСТ Р 52633.3, ГОСТ Р 52633.4, ГОСТ Р 52633.5 образуют фундамент для цифровой демократии

1. ГОСТ Р 52633-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. (принят)
2. ГОСТ Р 52633.1. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. (проект, окончательная редакция)
3. ГОСТ Р 52633.2. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. (проект, окончательная редакция)
4. ГОСТ Р 52633.3. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. (проект)
5. ГОСТ Р 52633.4. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код. (план-проспект)
6. ГОСТ Р 52633.5. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код. (план-проспект)

ПРОДУКТЫ И РЕШЕНИЯ

Био-ЭЦП

Новая инновационная технология, обеспечивающая вовлечение биометрических параметров человека в процесс формирования ЭЦП в системах электронного документооборота. Одним из примеров применения данной технологии является обеспечение возможности пользователя формировать ЭЦП под электронными документами с помощью своей собственноручной индивидуальной подписи, содержащей его уникальный биометрический параметр – динамику рукописной подписи

Описание:

В настоящее время идет развитие цифровых технологий, в том числе в области услуг и сервисов, предоставляемых населению по обеспечению безопасности персональных данных.

В традиционных системах (бумажном ЭДО) имеется материальный носитель информации – бумага, на которую накладывается личная подпись и печать, которая объединяет в единый документ содержащуюся на ней информацию и биометрические признаки человека, утверждающего этот документ.

В современных автоматизированных системах, использующих цифровые технологии, заверение документов, осуществляется с помощью электронной цифровой подписи (ЭЦП), применяемой в составе инфраструктуры открытых ключей. Во взаимодействии человека с автоматизированной системой его аутентификация производится опосредованно и является условной. Гарантами подлинности и достоверности идентификации являются только условия корректности политики безопасности и соблюдения организационно-технических и регламентных мероприятий. Причина тому – отсутствие биометрических параметров и индивидуальных признаков в сертификатах ключей ЭЦП, а также в отсутствии современных высоконадёжных электронных технологий биометрической идентификации личности

Суть 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. Для снятия других биометрических данных используются другие первичные преобразователи. В качестве двоичного числа в рассматриваемых приложениях целесообразно использовать электронный формат ключевого контейнера ЭЦП (в имеющихся системах инфраструктуры открытых ключей ключевой контейнер ЭЦП обычно хранится на каком-либо электронном носителе, например, USB-flash, при этом на пользователя возлагаются дополнительные обязанности, связанные с безопасным хранением и использованием персонального носителя ключевой информации).

Принципиальное отличие, в случае применения новой технологии, это отсутствие ключевого контейнера ЭЦП пользователя на каком-либо материальном носителе. Формат ключевого контейнера будет формироваться каждый раз для использования его в целях вычисления ЭЦП под электронным документом. Но это будет возможно только в случае корректного исполнения пользователем рукописной подписи, или предъявлением им данных, содержащих его биопараметры.

Область применения:

- обеспечение криптографической защищенности, достоверной идентификации и аутентификации человека при электронных банковских платежах, при автоматизированном оформлении кредитов, электронном документообороте
- обеспечение персонализации и криптографической защищенности конфиденциальной информации пользователя
- обеспечение персонализации в системах голосования со сбором голосов
- высоконадежная аутентификация пользователя без раскрытия персональных данных

УЦ

Системообразующая компонента инфраструктуры открытых ключей, обеспечивающая нормативно-правовые, юридически значимые условия использования ЭЦП в электронных документах

Описание:

Среди факторов, которые способствуют развитию системы электронного документооборота (СЭД), следует отметить общую потребность в создании систем хранения и управления данными. В дальнейшем СЭД имеют значительные перспективы внедрения в органах власти, и спрос на них будет устойчиво расти, поскольку эффективная организация работы с документами является для властных структур одной из неотъемлемых и жизненно важных задач.

Действующие в настоящий момент широко распространенные СЭД, такие как Lotus Notes и Docs Vision, обладают большой функциональностью и удобством пользовательского интерфейса. Они нашли широкое применение в различных Ведомствах и Госструктурах России.

Однако, в противоположность удобству и функциональности, обозначенные СЭД не отвечают современным требованиям по обеспечению необходимого уровня безопасности. Это обусловлено следующими особенностями архитектуры их программного обеспечения:

- отсутствием поддержки отечественных алгоритмов криптографического преобразования информации (для зарубежных СЭД);
- оторванностью подсистемы обеспечения информационной безопасности от процесса создания и обработки электронного документа, например, ЭЦП под документом появляется только в момент передачи документа по каналу связи, а в фазах создания, копирования и хранения (в том числе архивного хранения) документ может быть не подписан. В составе документа отсутствуют метки безопасности.

В данных условиях необходимо использовать технологию, которая позволила бы обеспечить, с одной стороны, совместимость с действующими широко применяемыми на практике продуктами в области ЭДО, с другой стороны, позволила бы создавать новые продукты на базе новых принципов организации с архитектурой, отвечающей как современным требованиям автоматизации делопроизводства, так и жестким требованиям информационной безопасности.

Данным требованиям удовлетворяет разрабатываемый продукт, который предназначен для такого сегмента рынка информационных технологий как обеспечение информационной безопасности ЭДО. Удостоверяющий центр (УЦ) удовлетворяет международным рекомендациям X.509 и обеспечивает совместимость с абонентскими рабочими местами системы электронной почты и электронного документооборота на базе криптопровайдеров «Верба-ДМ» и «CryptoPro CSP» (версия 3.0).

Отличительные особенности:

- многокомпонентная структура с возможностью территориального распределения, предоставляющая пользователям широкий спектр сервисов инфраструктуры открытых ключей
- взаимодействие с зарегистрированными пользователями по каналам связи общего пользования

Область применения:

- обеспечение нормативно-правовых условий использования ЭЦП в электронных документах
- для внедрения систем ЭДО в органах государственной власти, коммерческих структурах

Нотариус

Автоматическая проверка подписи человека в документах

Описание:

При принятии документов строгой учетности, накладных, товарных чеков, ведомости получения денежной суммы, у получающего документ подотчетного лица, возникает проблема проверки подлинности подписи на документе. Особенно остро эта проблема стоит, когда поток документов строгой учетности велик и заполняются они множеством людей. Если людей много, то проверка соответствия очередной подписи человека на очередном документе становится очень сложной.

Товарный чек
Наименование товара и его цена для списания с кредитной карты NN№ xxxxxxxx 20 ноября 2009 г. Кассовый аппарат NN№ xxxxxxxx ИНН магазина
1. Рубашка мужская – 600 руб. ***2. Куртка замшевая – 3000 руб.*** ***3. Щетка зубная – 30 руб.*** ***Итого к списанию с кредитной карты NN№ xxxxxxx – 3630 рублей***
Со списанием с моей кредитной карты согласен: ***Подпись-1***
Подпись-2
Подпись-3
Подпись-4

Рис.1

Предложена новая технология, которая автоматически контролирует «подлинность» подписи на документе при ее воспроизведении человеком, ранее зарегистрированным в системе контроля. Проверка осуществляется в режиме контроля динамики воспроизведения «живой» подписи на документе. Предусмотрена возможность многократного воспроизведения подписи под документом (это отображено на рисунке 1).

По старой технологии оформления документов строгой отчетности возможен сговор кассира с посторонним лицом, которое расписывается в ведомости или ином документе строгой отчетности, а кассир закрывает глаза на расхождение почерков. Предлагаемая система исключает эту возможность и делает поток документов строгой отчетности на много более достоверным. По данным наших исследований кассир-человек может выявить попытку подделки подписи с вероятностью 0.9 (ошибочно принимая 10% подделок за подлинные подписи). Предлагаемая система работает в 100 раз надежнее человека и позволяет выявлять попытки обмана с вероятностью 0.999 (пропуск одной подделки на 1000 обнаруженных подделок).

Фактически новая система является «электронным нотариусом» контролирующим процесс воспроизведения в документе электронной подписи. Крайне важным моментом новой технологии является то, что принимающий отчетный документ человек может вообще не знать лично другого человека оформляющего документ и не иметь образца его автографа для сравнения. При этом достоверность документа строгой отчетности, оформленного в присутствии проверяющего, оказывается высокой. Еще одной важной особенностью работы системы является то, что она может быть распределенной и контролировать оформление документов в разных местах, что является необходимым для крупных предприятий занимающихся логистикой и имеющих склады в разных регионах.

По новой технологии в присутствии кассира проверяемый человек расписывается специальной ручкой на документе строгой отчетности. Далее кассир вставляет кредитную карту в считыватель или набирает персональные данные человека (фамилию, имя, отчество, домашний адрес). После этого по сети связи из базы данных извлекается защищенный нейросетевой контейнер с биометрическими параметрами автографа человека и доставляется в терминал проверки автографа.

Запускается эмулятор искусственной нейронной сети, который проверяет подлинность введенного при подписании документа автографа. Если автограф признается подлинным, нейронная сеть выдает сигнал о положительной авторизации человека. Если происходит отказ в признании автографа подлинным, проверяемый человек повторно расписывается на отчетном документе ниже своего первого автографа. Процедура повторяется до момента, пока последний

введенный автограф на документе не будет признан системой подлинным. Количество попыток - до 7.

Перед применением системы проверяемый человек должен в ней зарегистрироваться. Регистрация осуществляется путем воспроизведения регистрируемым его 12 автографов на специальном бланке регистрации. При этом все 12 образцов подписи проверяемого параллельно с нанесением на бланк регистрации вводятся в систему. Далее на них обучается нейросетевой преобразователь биометрия-код и электронные образцы автографов в системе уничтожаются. В электронной форме хранятся только параметры искусственной нейронной сети, обученной узнавать автограф проверяемого человек

Область применения:

- предприятия, занимающиеся логистикой и имеющие обширное складское хозяйство
- банки, работающие с частными лицами и предоставляющие по требованиям Закона №152 «О персональных данных» услугу по анонимной выдаче наличных с биометрической проверкой личности получателя по его автографу на документе о получении денег
- системы телебанкинга
- крупные магазины, работающие с кредитными картами покупателей
- интернет-системы информирования граждан о состоянии их счетов по оплате коммунальных услуг, оплате штрафов
- корпоративные системы электронного документооборота

БиоЗамок

Устройство хранения цифровых ключей
с биометрической технологией доступа по отпечаткам пальцев

Описание:

Распознавание по отпечаткам пальцев-самый распространенный статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свертку) и сравнивается с ранее введенным шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Отпечатки пальцев, сканирование лица или радужной оболочки глаз - в любом случае при использовании биометрических методов речь идет о повышении уровня безопасности и комфорта. Прежде всего, с помощью этих средств предприятия стремятся защитить данные, здания и системы.

Примерно 44% всех биометрических решений составляют системы распознавания отпечатков пальцев, есть логичное объяснение. Согласно результатам многочисленных проектов, население охотнее всего принимает методы распознавания отпечатков пальцев: они сканируются быстро и удобно, проверка не требует много времени и больших затрат. Простые системы пользователи принимают более лояльно, в отличие от длительных и сложных, трудно воспроизводимых процедур

Отличительные особенности программного продукта БиоЗамок от существующих сегодня состоят в том, что в соответствии с ГОСТ Р 52633-2006 ключи в памяти процессора не хранятся. Хранятся только параметры высоконадежного преобразователя биометрия - ключ. Ключ появляется в доверенной вычислительной среде только, если пользователь, предъявляющий свой биометрический образ, является санкционированным лицом.

В существующих сегодня на рынке продуктах хранятся образы биометрии. Это дает возможность несанкционированному лицу при взломе данного средства извлечь образ и скомпрометировать истинного владельца биометрического образа. т.е. получить доступ к защищаемому объекту.

В данной разработке сами образы не хранятся. Извлечь или восстановить биометрический образ по признакам, распределенным в нейросети, невозможно. Таким образом, исключается вероятность компрометации и доступа несанкционированного пользователя к охраняемому объекту.

Область применения:

- использование в электронном документообороте в качестве ключа шифрования, ЭЦП
- разграничение доступа к ПЭВМ, сетевым ресурсам
- ограничение доступа в помещения (подъезды жилых домов, офисные помещения и т.п.)
- использование на предприятиях для контроля и учета рабочего времени персонала
- использование в составе охранных систем в качестве оконечного устройства захвата образов отпечатков пальцев

Устройство может быть использовано в высоконадёжных биометрических системах, отвечающим требованиям ГОСТ Р52633-2006.

Цифровой ключ и биометрический образ связаны между собой преобразователем биометрия-код. Невозможно извлечь ключ из преобразователя, не владея биометрическим образом законного пользователя. Для каждого пользователя в устройстве хранится свой преобразователь биометрия-код.