ГОСТ Р 52633-2006:

Россия достроила фундамент мировой цифровой демократии, сделав его устойчивым!

А. И. Иванов, *д. т. н., начальник лаборатории биометрических и нейросетевых технологий ФГУП «ПНИЭИ»*

Благодаря программам типа «Электронная Европа» и ее аналог «Электронная Россия» для всех нас стали привычными такие термины как «цифровой гражданин», «цифровое правительство», «цифровое государство». Более того, с этого года самая «передовая» и самая «демократическая» Эстония голосует через Интернет, что существенно упорядочивает рынок купли-продажи (дарения, переуступки) голосов избирателей. Если раньше заинтересованный покупатель голоса мог быть обманут недобросовестным гражданином Эстонии, имевшим возможность пообещать проголосовать определенным образом неограниченному количеству кандидатов, то теперь это исключено. Отныне в Эстонии появилась ультрасовременная технология, по которой при желании можно заранее продавать свои «цифровые права» на голосование, что является очевидной победой «цифровой демократии» европейского образца и демонстрацией поистине неограниченных возможностей свободного рынка.

Появление в свободной массовой прессе приведенных выше рассуждений возможно, только если они воспроизведены на русском языке. Англоязычная и, тем более, эстонская пресса не стремятся поднимать подобные проблемы – так исторически сложилось. Это у нас с вами демократия все-таки «суверенная», и мы пока еще можем позволить себе не повторять вслух на русском один в один все «цифровые» глупости заокеанского Большого брата. Для сохранения этой привилегии, как минимум, необходимы публичное обсуждение истоков аналого-цифровых проблем и попытка выхода на хорошо понятную большинству населения терминологию. В конечном итоге при демократии решает все большинство, а делает оно это в соответствии с тем, как понимает ситуацию.

Если попытаться «заземлить» проблему, то будущее «цифровое государство» создается для противодействия аналого-цифровому хаосу реальной жизни (рис. 1) и проведения в жизнь более эффективной политики «цифровой» учетности.

Любое государство (аналоговое или цифровое) стремиться реализовать эффективную политику учетности людей, ресурсов, а также их взаимодействия. В качестве наглядного примера приведем самый обыкновенный сельхозрынок в каком-нибудь городке России. На этом аналоговом рынке все продавцы обязаны использовать аналоговые весы

конкретного рынка (пользоваться своими весами запрещено), весы периодически поверяются и имеют погрешность 1 %. Говоря другими словами, технический предел реализуемости государственной политики учетности на этом сельхозрынке составляет 1 %. Все, что менее 1 % – это технически ненаблюдаемая неучтенка, и потому там всегда будет господствовать невидимый государеву оку хаос.

Если мы мысленно перенесемся в светлое цифровое будущее этого маленького сельхозрынка, то увидим у всех продавцов более совершенные и более точные цифровые весы, принадлежащие тому же самому сельхозрынку. Цифровые весы позволяют снизить погрешность до 0,01 %, что существенно уменьшит технический предел реализуемости политики учетности. Если грядущее цифровое государство сочтет нужным, оно ужесточит будущие допустимые нормы утруски, усушки, обвеса на своих рынках. Нормы допустимого хаоса всегда были и всегда будут, они возникают на границе «аналог – цифра». После перехода в цифру такие нормы цифровой наблюдаемости по-прежнему продолжают существовать, просто они часто не формализованы в явной форме.

Очевидно, что для любого государства задача организации политики учетности проживающих на его территории людей (его граждан) гораздо более актуальна в сравнении с учетом движения материальных ценностей. Традиционно эта задача решается через паспортный учет населения. Обычная аналоговая система современных бумажных паспортов имеет свой технический предел учетности. Каков он – я не знаю, но он будет повышаться в больших системах и он будет повышаться по мере совершенствования средств копирования бланков на бумажном носителе. То есть надежность аналогового паспортно-визового учета людей все время падает из-за процессов глобализации (увеличиваются размеры системы) и совершенствования копировально-множительной техники. В связи с этим (а также в связи с трагедией 11 сентября

Рис. 1. ***Противостояние цифрового государства хаосу безучетности и неавторизованности***

2001 года, произошедшей в том числе из-за относительно слабой политики учетности иностранцев в США) современные государства предпринимают попытку ввести паспортно-визовые документы нового поколения с элементами автоматизированного цифрового биометрического контроля. Этот фрагмент цифрового государства отображен на рис. 1 в виде левого эллипса «Цифровой биометрический контроль граждан».

Сочетание слов «цифровой биометрический контроль» является принципиальным. Дело в том, что просто «цифровой контроль» граждан не является привилегией «цифрового государства». Цифровой контроль существовал всегда (все государства как аналоговые, так и цифровые в цифре считают наши доходы, расходы, налоги, пенсии, льготы и т. д.). Отличие любого сегодняшнего государства от будущего цифрового в области цифрового контроля граждан заключается лишь в техническом пороге реализуемости политик учетности. В будущем цифровом государстве точность цифрового контроля цифровых граждан должна увеличиться на порядок или два: в 100 раз труднее будет воспользоваться чужим паспортом и ненаблюдаемая оком государя сумма в цифровом кошельке цифрового гражданина также должна уменьшиться в 100 раз.

Интересно отметить, что государства, преимущественно развивающие средства цифрового контроля граждан, следует называть государствами «цифровой диктатуры». И наоборот, те из них, что активно занимаются поддержкой развития цифровых прав граждан стоит причислить к государствам «цифровой демократии». Исходя из этого примитива «цифровая Эстония» много демократичнее «цифровой России» по критерию наличия голосования через Интернет. Сегодня столь простая логика выгодна Большому брату и его друзьям из НАТО. Необходимо привыкать к тому, что нам будут про это постоянно и нудно петь, для них это очень складная и красивая песня, другой у них нет.

Если же уйти из области поэзии, политики, журналистики в технику, выяснится совершенно иная картина – 99,99 % усилий Европы и США направлены на создание «цифровой диктатуры». Про это они не поют, про это они вводят национальные и международные «биометрические стандарты».

Все биометрические стандарты, принятые за рубежами России после 11 сентября 2001 года, – это исключительно однонаправленные полицейские стандарты, предназначенные для полицейского цифрового биометрического наблюдения за людьми. Россия вводит у себя эти стандарты (нам они тоже нужны), но не мы выступаем в роли их инициаторов, мы просто вынуждены идти на внедрение у себя дорогих

Рис. 2. ***Три базовых технологии, образующие устойчивую опору для «цифровой демократии»***

и неэффективных международных технических решений, которые рассчитаны только на контроль населения со стороны государства. При разработке идеологии паспортно-визовых документов нового поколения технологические лидеры конца прошлого века даже не попытались заложить в новые биометрические технологии потенциальную возможность их гражданского применения. Для них цифровые права граждан и биометрия – совершенно разные вещи.

По факту, единственной страной, которая в этом веке прилагает серьезные усилия по развитию технологического фундамента цифровой демократии, является Россия. В итоге именно Россия первой ввела с 01.04.2007 национальный биометрический стандарт [1], завершающий формирование устойчивого фундамента «цифровой демократии». Эта ситуация отображена на рис. 2.

Поддержка «цифровой демократии» осуществляется через привлечение технологий асимметричной криптографии, электронной цифровой подписи и высоконадежной биометрической аутентификации человека. Эти три технологии (три слона) должны постоянно поддерживаться цифровым государством (цифровое государство на рис. 2 отображено в виде кита). Цифровая демократия отображена в виде земного шара, устойчиво лежащего на трех технологических опорах. Если одну из них убрать, цифровая демократия становится технологически неустойчивой.

В частности, эстонский вариант интернет-голосования технологически неустойчив из-за того, что в нем голосуют не люди, а ключи. Государевы люди «цифровой эстонской демократии» теперь технологически могут обойтись и без некоторой части избирателей. Подавляющее большинство последних не способно надлежащим образом создать и хранить свои личные ключи голосования. Все они вынуждены будут излишне доверять государству, которое может не только помочь своим гражданам, но и проголосовать за них в нужный момент, естественно, по очень важному для всей Эстонии вопросу. Технологических гарантий от подобных злоупотреблений у цифровой Эстонии нет. Безопасность «цифровой эстонской демократии» опирается на совесть исполнителей без соответствующей технологической поддержки и политики учетности их действий.

Для того чтобы исключить любые злоупотребления с ключами голосующих, необходимо безопасно связать эти ключи с биометрией человека [1], а также исключить возможность компрометации ключа голосующего, даже если сам голосующий захочет этого (захочет заранее продать свое право «цифрового голосования»). Еще одним принципиально важным свойством средств защиты «цифровых прав» людей в больших системах является свойство обеспечивать их анонимность. Для поддержки «цифровых прав» граждан просто биометрии недостаточно, нужна анонимная биометрия.

Обычная биометрия принципиально не может обеспечить людям анонимности: на рис. 3 приведена блок-схема процедур классической биометрической аутентификации. Из нее видно, что все устройства и программы классической биометрии должны иметь биометрический шаблон, извлечение которого эквивалентно компрометации анонимности пользователя. Необходимо как-то защитить шаблон, однако это оказывается не простой задачей. Если его шифровать, возникает проблема безопасного хранения ключа шифрования. Хранить ключ шифрования шаблонов в биометрической программе или в биометрическом «железе» нельзя.

Одним из путей обеспечение анонимности является использование искусственных нейронных сетей. На рис. 4 приведена блок-схема нейросетевой реализации процедуры биометрической аутентификации. Преимуществом такой реализации биометрии является следующее: при ней биометрический шаблон исчезает – он растворяется в параметрах и связях искусственной нейронной сети.

Для этого технического решения атака компрометации анонимности

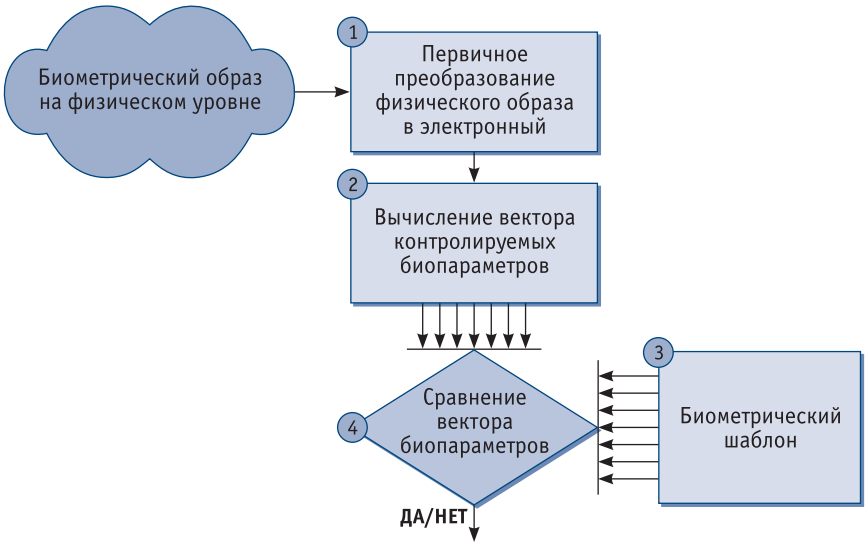

Рис. 3. ***Блок-схема процедур биометрической аутентификации, выполненных с классическим решающим правилом***

биометрии усложняется, однако она все же может быть реализована. Всех людей можно разбить примерно на 100–1000 групп, и поочередно подавать на вход единственной нейросети среднестатистические по каждой группе биометрические образы. Нейросеть сама даст ответ, на кого похож ее хозяин. Таким образом, простыми нейросетевыми решениями нельзя надежно обеспечить анонимность биометрии «цифрового гражданина». Подобная защита легко преодолима и только создает иллюзию безопасности.

Положение меняется только в том случае, когда используются нейросетевые преобразователи «биометрия – код» с большим числом выходов [1]. Обобщенная блок-схема подобных устройств и программ приведена на рис. 5. Новая биометрическая технология, выполненная в соответствии с требованиями национального стандарта [1], обеспечивает надежную защиту анонимности пользователя и ее уже можно применять для биометрического голосования. Высокая надежность защиты биометрических данных в ней обусловлена тем, что атакующий не знает выходного кода ключа нейросетевого преобразователя. Он вынужден наугад подавать множество входных биометрических образов, пытаясь добиться запуска криптопротокола 4, например, реализованного в виде формирования ЭЦП под некоторым текстом.

Высокая надежность нейросетевого многомерного преобразователя «биометрия – код» обеспечивается наличием экспоненциальной связи между размерами искусственного интеллекта и качеством принимаемых им решений. Увеличение искусственных «мозгов» в 100 раз приводит к повышению качества решений в 1 000 000 000 раз. В нашем случае искусственные «мозги» блок-схем на рис. 4 и 5 должны отличаться по размерам в 256 раз, однако это не совсем так. Технически нет смысла строить 256 независимых нейросетей, выгоднее все их объединить в одну. Именно такое техническое решение и дает рост размеров искусственного интеллекта примерно на два порядка, приводящий к «миллиардному» росту надежности биометрической защиты.

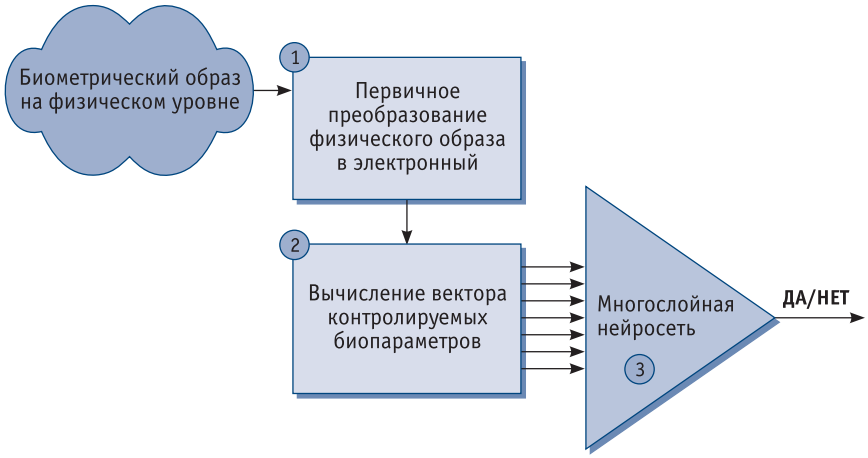

Рис. 4. ***Блок-схема процедур биометрической аутентификации, выполненных с классическим нейросетевым решением с одним выходом***

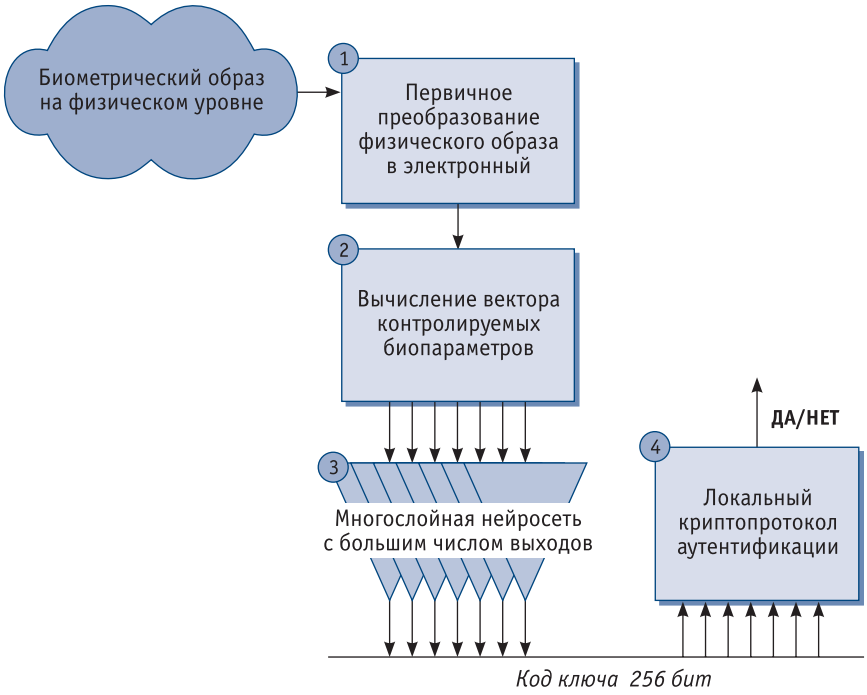

Рис. 5. ***Блок-схема процедур биометрической аутентификации, выполненных с нейросетевым решением «вектор высокой размерности»***

Анонимность цифрового биометрического голосования и его фантастические возможности по реализации политик учетности становятся возможными только при использовании всей тройки базовых технологий: ЭЦП голосующего, некоторого дополнительного асимметричного криптопротокола и анонимной высоконадежной биометрии (см. рис. 2).

То, что кажется сегодня фантастикой, может быть сформулировано в виде соответствующих протоколов или свойств. Перечислим эти свойства.

1. Практически невозможно передать кому-либо свое «цифровое право» голоса (только хозяин права может им воспользоваться заданное число раз или в рамках иной заданной заранее метрики учетности).

2. Обеспечение анонимности высоконадежной биометрии (невозможно установить хозяина нейросетевого преобразователя «биометрия – код»: в разных системах один и тот же хозяин выглядит совершенно иначе).

3. Хозяин цифрового права может анонимно доказать свои полномочия локально или дистанционно неограниченное число раз.

НОВОСТИ

4. Технически выполнима сквозная учетность реализации цифровых прав как со стороны анонимного хозяина, так и со стороны государства (можно проверить, как учтен ваш личный голос Центризбиркомом без компрометации вашей анонимности, можно самостоятельно произвести подсчет голосов, контролируя избиркомы любого уровня, все избиркомы, в свою очередь, контролируют число и верность действий своих анонимных голосующих).

5. Любой обнаруживший ошибку при реализации его «цифрового права» голоса может найти виновного и в судебном порядке наказать его, раскрыв перед судом свою анонимность.

6. Снята проблема безопасного хранения криптографических ключей, используемых при реализации того или иного «цифрового права» гражданина: даже сам пользователь без специальных средств не может увидеть свой ключ, пользователь может только его применить.

В целом, разница между новой высоконадежной анонимной биометрией [1], созданной для частных гражданских приложений, и классической биометрией полицейского контроля паспортно-визовых документов – огромна. Фактически в этих двух биометриях заложены совершенно разные принципы и подходы. Уже сейчас очевидно, что массовое безопасное использование криптографии [2] для защиты общества в целом и каждого гражданина в отдельности невозможно на принципах классической биометрии.

Потратив много государевых денег на реализацию навязанной нам системы паспортно-визовых документов нового поколения, сделанной по международному образцу, мы отстаем от своих же передовых технологий. Нам придется все переделывать в ближайшем будущем. Мы вынуждены будем вносить изменения, позволяющие безопасно использовать электронные паспорта при голосовании, покупках, при взаимной аутентификации граждан.

Проигрываем не только мы, но и третьи страны. От такого развития ситуации выигрывают только фирмы-производители Большого брата: они уже согласны продавать всем морально устаревшее оборудование со своих действующих заводов. Большой брат добился того, чего хотел, «впарив» окружающим свои биометрические наработки прошлого века, и теперь за наш с вами счет обновит свое технологическое оборудование на собственных заводах. Такой политической ловкости всем следовало бы поучиться.

Впрочем, плюс из всего этого Россия все-таки может извлечь, оставаясь лидером разработки гражданских применений высоконадежной биометрии. По крайней мере, наше формальное лидерство с принятием [1] становится неоспоримым, более того, необходимо развивать успех и пытаться разрабатывать всю серию сопутствующих стандартов по биометрической защите «цифровых прав» граждан. Пока мы вынуждены в одиночку работать и за Большого брата, и за его друзей по Северо-Атлантическому альянсу, но это рано или поздно вернется России уважением третьих стран. Рано или поздно проблемы «цифровой демократии» будут осознаны всеми, и все будут использовать наши высоконадежные, высокобезопасные, высокоанонимные технологии.

Нет смысла догонять Эстонию по интернет-голосованию. Нет смысла суетиться, подстраиваясь под текущую конъюнктуру, как это делают многочисленные младшие братья. Мы должны работать глубже, более фундаментально, у России для этого есть и люди, и ресурсы, и технологии. Необходимо активно проводить свою, выгодную России, техническую политику в рамках соответствующего подкомитета международной организации по стандартизации ISO/IEC JTC1 CS27. ■

ЛИТЕРАТУРА

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

2. Гезенко И. И., Иванов А. И. Обеспечение устойчивости будущего информационного общества: массовая гражданская криптография // Защита информации. Инсайд. 2005, № 1, с. 71–73.