

ПАКЕТ РОССИЙСКИХ БИОМЕТРИЧЕСКИХ СТАНДАРТОВ КАК ОДНА ИЗ ПРЕДПОСЫЛОК УСТОЙЧИВОГО РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Ворона Ю.В. (г. Москва), Иванов А.И., (г. Пенза)

В настоящее время все развитые страны объявили о создании «электронного правительства» и своего стремления активно двигаться в направлении создания информационного общества или общества «знаний». При этом инициаторами, а так же идеологами всех этих процессов являются США и страны НАТО, а абсолютное большинство менее активных в создании новой идеологии стран занимают пассивную позицию молчаливой поддержки всех инициатив лидеров информатизации.

К сожалению, пассивная позиция большинства присоединяющихся стран делает страны лидеры информатизации абсолютно защищенными от критики. Пользуясь своим доминирующим положением ИТ-элиты (олигархия) США и стран НАТО стремятся разрушить существующие нормы международного права и международной морали и навязать всем решения суда штата «Калифорния», как образец для подражания. Происходит открытое вмешательство США и стран НАТО во внутренние дела суверенных государств с помощью «гуманитарных бомбардировок» и отключения банкоматов в момент «цветных революций». С этим нельзя мириться, у США и стран НАТО нет монополии на истину.

При изучении истории мы видим чередующиеся циклы нестабильности (хаоса) и стабильности, причем выход из хаоса, как правило, осуществляется через диктатуру как наиболее простую форму общественной организации. На рисунке 1 приведена иллюстрация основных исторических этапов развития человечества: матриархат, рабовладение, феодализм, капитализм, «информатизм» с наложением на них чередующихся циклов стабильности в форме демократии или диктатуры и хаоса.

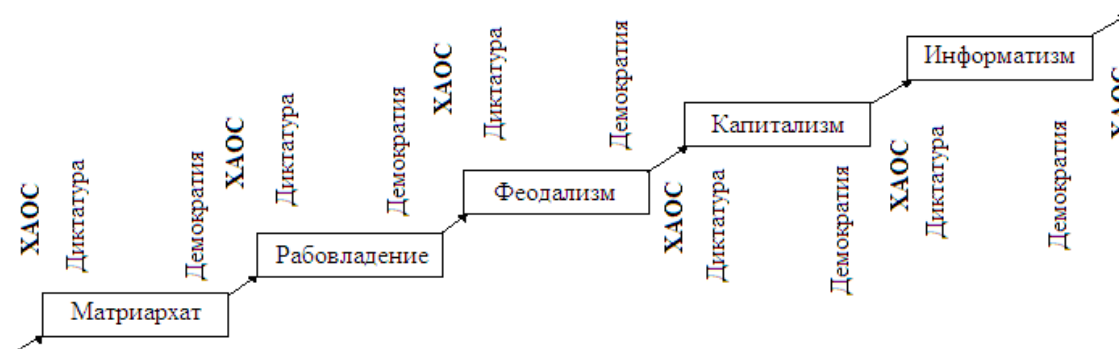


Рис. 1. Этапы развития общественно-экономических формаций, связанные со сменой общественных укладов, морали и права

Очевидно, что выделенные на рисунке 1 исторические эпохи являются достаточно стабильными образованиями со сходными в рамках одной эпохи нормами: морали, права личности, межгосударственного права. То, что в эпоху рабовладения отвечало нормам морали и права сегодня уже не является

моральным и не соответствует нормам современного права, как гражданского, так и международного.

Очевидно, что между стабильными эпохами развития цивилизации с похожими нормами морали и права возникают переходные периоды нестабильности, войн, хаоса. Обычно этот период наступает после эпохи демократии (рабовладельческой, феодальной, капиталистической). Сегодня мы находимся на этапе свертывания капиталистической демократии и скатывания в эпоху хаоса эпохи перехода в информационное общество (информатизм). Все современные политики говорят нам об угрозе «терроризма», однако «терроризм» это синоним неустойчивости перехода в информационное общество. Если бы общество продолжало бы быть устойчивым, то никто не стал бы его раскачивать. Терроризм создают две стороны: СМИ и террористы. Если бы СМИ в погоне за сенсациями не освещали бы подробно террористические акты, террор был бы полностью бесполезен с точки зрения его организаторов. Если нет соответствующего подробного массового освещения в СМИ террористических актов, то они оказываются абсолютно неэффективными и не могут повлиять на общественное сознание.

Наши естественные языки являются некоторыми коллективными системами МЕТО оцифровывания окружающей нас действительности. Люди отличаются от других млекопитающих только тем, что коллективно создали (получили от всевышнего) развитую систему языкового общения. Пользуясь этой системой каждый из нас способен передать другим (обобществить) свои личные знания или получить от других необходимые ему общественные знания.

Если исходить из предпосылки, что язык и сформулированные на нем знания являются некоторой технологической основой обработки информации, то удастся связать общепринятые исторические этапы общественного развития с определенными совершенствованиями технологий обработки информации.

«Матриархат» следует рассматривать как период нехватки людей или период тиражирования общественных знаний (тиражирования людей как носителей общественных знаний). Окончание «матриархата» наступает, когда людей становится больше, чем могут прокормить легко доступные природные ресурсы. Начинается конкуренция между людьми за природные ресурсы, самая жестокая форма конкуренции это война. Уважение к матерям сменяется на уважение общественного сознания к ярким воинам (боярам). Оценка успехов того или иного военного похода осуществляется по числу пленных (рабов), наступает эпоха рабовладения.

При рабовладельческом строе происходит важнейшее технологическое нововведение – появляется письменность. Фактически происходит отрыв личных и общественных знаний от человека – их носителя. Человек, как носитель информации не может жить вечно и одновременно находиться в разных местах (знания, сформулированные на языке людей, являются информацией). Излагая, свои знания в рукописной форме, человек создает новые носители информации, которые могут существовать вечно и распространяться в пространстве (тиражироваться) без участия первоисточника знаний. Письменность – это последовательность оцифрованных звуков языка, зафиксированных на твердом носителе в виде последовательности букв некоторого алфавита (в западной традиции) или последовательность иероглифов, каждый из которых соответствует тому или иному понятию (восточная традиция).

Во времена феодализма совершенствуется технология тиражирования знаний в виде книг, параллельно происходит рост числа грамотных людей, способных писать и читать. В наиболее информационно развитых странах, например таких Русь наблюдается феномен всеобщей грамотности в сочетании с

очень высоким уровнем демократии (новгородское вече полностью грамотного населения). В этот момент Россия оказывается информационным центром развития цивилизации, именно тогда зарождается идея третьего Рима.

При феодализме активно идет торговля, развиваются товарно-денежные отношения, ведется цифровая учетность гражданского и государственного имущества в денежном эквиваленте. Появляется класс буржуазии (капиталистов), который во время хаоса буржуазных революций захватывает власть и устанавливает свою диктатуру. Пользуясь неограниченной властью диктатуры, капиталисты активно разрушают мораль и право предшествующего феодального строя. При этом диктатура «дикого» капитализма создает невыносимые условия для абсолютного большинства других «угнетенных» классов (сословий) и закрепляет свою победу в виде новых норм морали и права.

В эпоху капитализма происходит ряд технологических изменений, связанных оперативностью доставки новой общественно значимой информации потребителям. В 19 веке появляются СМИ в виде газет, сокращается время транспорта информации по телеграфу. В середине 20 века получают активное распространение: кино, телефон, радио, телевидение, создаются ЭВМ коллективного пользования. Все это способствует обузданию алчности «дикого» капитализма, который после его приручения превратился в капиталистическую демократию последней четверти 20 века.

Капиталистическая демократия на наших с Вами глазах превращается в информационное общество. Толчком к этому является тотальная персонализация ЭВМ и снятие проблемы вычислительных ресурсов. Мы являемся свидетелями тотального использования персональных телефонов (персональных ЭВМ, предназначенных для оцифровывания и обработки голоса при его передаче по радиоканалу связи). Появление Интернета делает доступными огромные массивы оцифрованных знаний, видимо, в ближайшее время мы станем свидетелями появления персональных СМИ, ориентированных на личные интересы и пристрастия каждого из нас. В свою очередь огромные объемы цифровой информации, размещенные в сети Интернет, порождает необходимость в появлении специальных поисковых машин, осуществляющих сортировку и ранжирование знаний.

Главным признаком информационного общества является тотальная приватизация вновь полученных знаний и приватизация старых знаний, конвертированных в форму программных продуктов для типовых ЭВМ. Если в эпоху классического капитализма авторское право распространялось на литературные произведения и патенты, то в эпоху раннего информатизма ИТ олигархия стремится распространить авторские права на любой цифровой контент. То, что недавно было бесплатным, сегодня кем-то приватизировано и за каждую цифровую копию нужно платить. Рушится старая мораль и право, а на их месте новая информационная олигархия пытается навязать всем нам новые правила игры, выгодные, прежде всего, наиболее развитым в информационном отношении странам. Наш мир стремительно движется к «дикой» стадии информационного общества в форме цифровой диктатуры информационной олигархии.

Еще одной тенденцией информационного общества является персонализация аппаратно-программных средств обработки цифровой информации. Персональные ЭЦВМ превратились в персональные цифровые телефоны, далее появятся персональные программы, ориентированные на удовлетворение и защиту информационных интересов только одной личности. Все мы разные, наши интересы различны и рано или поздно мы придем к ситуации, когда нам будут предлагать строго индивидуальные лекарства

(синтезированные с учетом личного генотипа), а электронное правительство должно будет подходить к каждому из нас ИНДИВИДУАЛЬНО. Мы перестанем быть безликой массой, соответственно, наши личные программы и автоматы (наше личное железо) должны уметь безошибочно нас узнавать.

Для решения этой задачи в США и России активно развиваются биометрические технологии. Пока только эти две страны имеют собственные (независимые) национальные политики по развитию средств биометрической идентификации и аутентификации личности. Отличительной особенностью национальной политики США является упор на развитие полицейской биометрии автоматизированного паспортно-визового контроля иностранных граждан, пересекающих границу страны. Для этой цели национальные институты стандартизации США (NIST и ANSI), разработали более 100 национальных биометрических стандартов. Часть из этих национальных стандартов США с 2002 года преобразуются в международные биометрические стандарты международной организацией по стандартизации ISO/IEC через подкомитет JTC1 SC37 (Биометрия).

Россия, так же как и все иные страны, заинтересована в развитии средств полицейского биометрического контроля иностранных граждан, пребывающих на ее территорию. В связи с этим, международные стандарты ISO/IEC JTC1 SC37 гармонизируются и комитетом № 355 (Автоматическая идентификация) подкомитетом №7 (Биометрическая идентификация) ГОСТ Р. Сложившаяся ситуация по разработке биометрических стандартов отображена на рисунке 2.

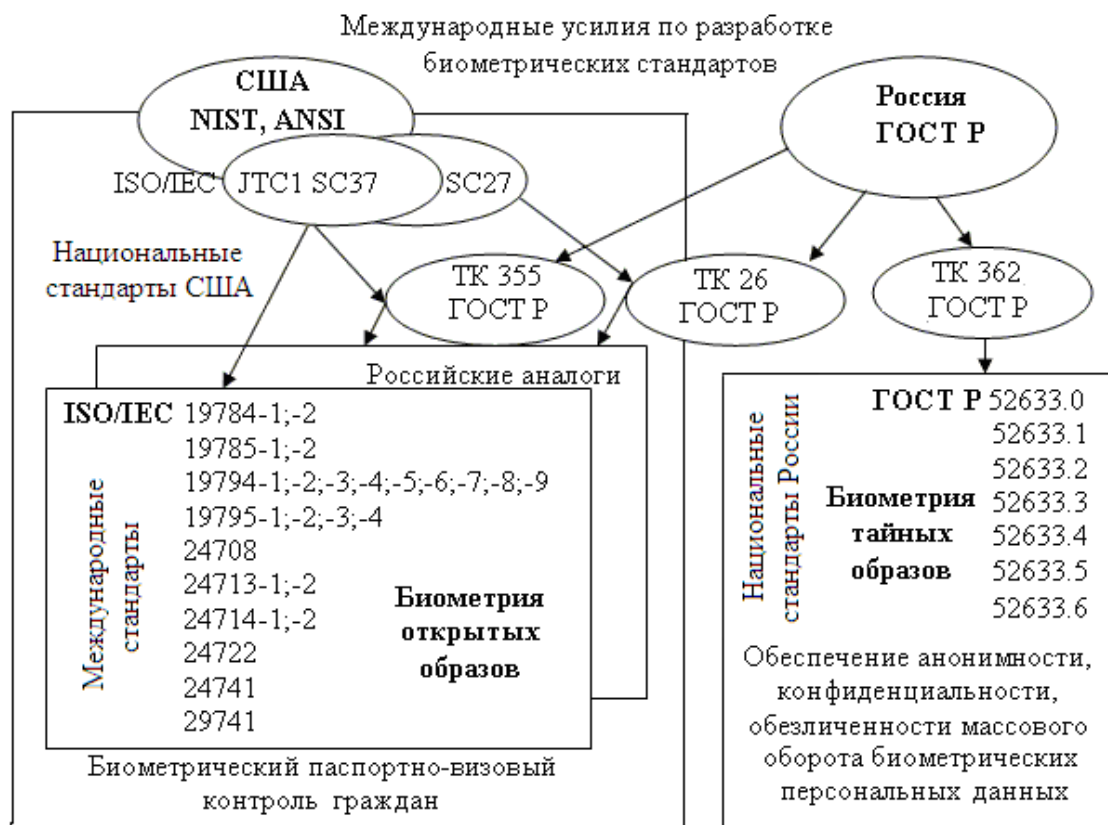


Рис. 2. Усилия США и России по созданию двух ветвей биометрических стандартов.

Принципиальным отличием усилий России является то, что наша страна начала создавать национальные стандарты формирующие требования к гражданской биометрии, способной безопасно работать с гражданской

асимметричной криптографией. Эти усилия России отображены в правой части рисунка 2 и осуществляются техническим комитетом по стандартизации № 362 «Защита информации» (ТК 362).

Безопасность личности в открытом информационном пространстве может быть обеспечена только через применение средств асимметричной криптографии. При этом открытый ключ должен быть общедоступен, а личный ключ человека должен надежно храниться в секрете и быть доступным только своему хозяину. У обычных людей сегодня нет надежных средств для хранения своего личного ключа и именно по этой причине у обычных людей нет особого желание регистрировать свой открытый ключ в удостоверяющем центре и получать сертификат открытого ключа. Подобный шаг приводит к появлению дополнительных рисков возможной компрометации личного ключа гражданина.

Риски компрометации могут быть минимизированы, если хранить личный ключ в параметрах большой нейронной сети преобразователя биометрия-код по базовому стандарту [1]. При этом проблема автоматического обучения больших нейронных сетей должна быть решена по стандарту [2]. Тестировать надежность биометрико-нейросетевой защиты личного ключа следует по стандарту [3]. Особенности формирования баз тестовых биометрических данных описываются стандартами ГОСТ Р 52633.1-2009 и ГОСТ Р 52633.2-2010. Унификация интерфейсов средств биометрико-нейросетевой защиты информации должна выполняться по стандарту ГОСТ Р 52633.4-2011. Только при выполнении требований всего пакета стандартов может появиться гарантия безопасного хранения и применения личного ключа гражданина.

Принципиально важным является то, что Россия имеет собственную независимую политику применения биометрии для решения задач информационной безопасности. Именно это и позволило России создать свои национальные стандарты формирующие требования к средствам защите личности в открытом информационном пространстве, которых нет у США и стран НАТО. Наметилось очевидное международное разделение труда США - это очевидный лидер по созданию стандартов «полицейской» биометрии, а Россия - это очевидный лидер по разработки стандартов для личной «гражданской» биометрии. Устойчивое (бескризисное) развитие информационного общества возможно только при сбалансированном применении средств «полицейской» биометрии общественного контроля за личностью и средств биометрической самозащиты гражданских прав личности в Интернет и иных открытых информационных пространствах.

Литература:

1. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
2. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
3. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».