Облачные технологии как фактор политического риска информатизации политической системы России

Овчинников Сергей Александрович, проректор Саратовского государственного социально-экономического университета, член «Гильдии Управляющих Документацией», д.и.н., профессор

18 апреля 2012 года в Москве прошла Международная научно-практическая конференция по облачным технологиям. Её участникам был вручен уникальный сувенир – красного цвета мощная рогатка с текстом: «Персональное многофункциональное бизнес-наступательное облакометательное устройство защитника Отечества», что на наш взгляд, довольно симптоматично в условиях распространяющейся, возможно и весьма не безосновательно, эйфории по поводу беспредельно огромных возможностей так называемых «облачных технологий.

Выслушав ряд докладов представителей разработчиков технических устройств, которые заманчиво обещали с помощью «облаков» решить практически все земные проблемы, невольно вспомнились строки из бессмертного произведения И.Ильфа и Е.Петрова «Золотой теленок», когда Остап Бендер «сватал» водителя «Антилопы» Козлевича на авантюрную поездку в славный город Черноморск: «...Бендер не жалел красок. Он развернул перед смущенным шофером удивительные дали и тут же раскрасил их в голубой и розовый цвет».

Когда на материалы этой, безусловно, весьма интересной конференции, смотришь по прошествии некоторого времени, вновь убеждаешься, что бизнес-информатизаторы навязывают органам власти и обществу новые (или несколько забытые) идеи. Но при этом исключительно интересы бизнеса превалируют над другими, не менее важными вопросами, и, прежде всего, проблемами информационных рисков и угроз политической системе, т.е. именно над теми аспектами, которые наиболее чувствительны для личности, общества и государства.

Полагаем, что нельзя двигаться дальше в развитии информационных технологий, не выслушав компетентные мнения специалистов – политологов, документоведов, социологов, юристов, психологов и т.п., с тем, чтобы на научной основе, экспертным путем оценить позитивные и негативные стороны этого процесса. Именно такой подход

поможет минимизировать различные информационные риски для политической системы и граждан, с чем нам уже неоднократно пришлось сталкиваться.

Вхождение в информационную эпоху было столь стремительным, что многие негативные стороны внедрения ИК-технологий своевременно не были замечены и сегодня приходится «расхлебывать» эту кашу, ведь изначально многие негативные аспекты этого процесса не были учтены. И в финале – даже западные исследователи ныне открыто признают: надежды на то, что информационные технологии изменят в лучшую сторону общественно-политические процессы, мягко говоря, не оправдались, а стремительно проникающие информационные технологии несут угрозу демократическим принципам современного общества.

Весьма примечательно, что на состоявшейся г. Москве 14 марта 2013 года научно-практической конференции «ИКТ в госсекторе, один из докладчиков призвал несколько «приостановить» активный процесс информатизации до тех пор, пока не будут надежно обеспечены вопросы информационной безопасности в этой сфере и осуществлена необходимая работа по подготовке кадров.

Кроме того, внедрение технологий электронного правительства требует колоссальных финансовых вложений и по этой причине многие развивающиеся страны остаются «за бортом» процессов информатизации, стремительно развилась и не сокращается политико-конфликтогенная проблема цифрового неравенства, что актуально и для России.

Анархия, творящаяся в Интернете, нанесла огромный ущерб морали, нравственности людей, породила абсолютно новые, ранее неизвестные практике формы киберпреступности, в том числе нарушения в сфере соблюдения прав человека и норм о защите авторских прав.

Тем не менее, в современной России наблюдается активный процесс внедрения в систему государственного управления информационно-коммуникационных технологий, на базе которых формируется новая форма взаимодействия государства с обществом. Так, Президент России В.В.Путин выступая в Новосибирске в прошлом году подчеркнул, что «информатизация государственных органов – это, прежде всего серьёзный ресурс для укрепления национальной экономики, повышения инвестиционной привлекательности, эффективная модернизация социальной сферы, качественных изменений в здравоохранении, образовании, системе социальной защиты, более простое и прозрачное общение граждан с властью, реальная и очень эффективная

антикоррупционная мера. Речь идет о построении эффективного, современного государственного механизма управления, ориентированного на запросы граждан, на интересы общества и национальной экономики».

И действительно, сегодня активно развиваются порталы федеральных, региональных и муниципальных органов власти, получают распространение госуслуги в электронном виде. И, хотя на этом поприще, существует множество проблем, в целом динамика положительная.

Тем не менее, эти процессы ведут к прямой зависимости эффективного государственного управления, а, следовательно, устойчивого политического развития страны, от совместимости, стандартизации и качественного функционирования систем межведомственного электронного взаимодействия и обмена документами, на которых выстраивается система электронного государственного управления.

И в этих условиях вероятность крупного сбоя в работе информационной инфраструктуры госуправления, чего исключать нельзя, несет объективный риск дисфункции системы государственного управления, что может вызвать дестабилизацию социально-политической и экономической ситуации в регионе и, в целом, в стране.

Поэтому в интересах устойчивого политического развития страны, обеспечения информационной безопасности процессов внедрения электронного правительства, необходимо системное проведение прикладных научных исследований для выявления «слабых» звеньев в системе электронного государственного управления, особенно при электронном обмене документами при оказании госуслуг гражданам и бизнесу.

Так, например, сегодня многих настораживает довольно сложная проблема, которую Президент страны обозначил таким образом: «*...нужно предусмотреть защиту от так называемых грязных данных – разного рода неточных или ошибочных сведений. Именно из-за такой искажённой информации в базах данных различных ведомств и возникла мнимая налоговая задолженность у миллионов граждан – практический результат этой «грязной» информации. Ведомствам надо самим наводить порядок в своих электронных архивах, чтобы у людей потом не возникали неудобства, связанные с финансовыми, бюрократическими издержками и пустой тратой времени*».

Таким образом, электронное государственное управление может рассматриваться как высокотехнологичный вид политической коммуникации между системой государственной власти, органами местного самоуправления и общественными субъектами.

При этом важным критерием является наличие оперативной обратной связи «общественные субъекты – власть», ныне все более функционирующей в интерактивном режиме. Однако в случае преднамеренного или случайного перекрытия этого канала, система электронного государственного управления разбалансируется и не сможет успешно функционировать.

В настоящее время ренессанс переживают так называемые «облачные технологии», в том числе внедряемые в госсектор. Это не новое явление. Сервис-ориентированные архитектуры с веб-интерфейсом, лежащие в основе «облаков», были известны и применялись на практике, хотя и весьма ограниченно, еще в 90-е годы прошлого столетия.

Несомненно, что облачные технологии – это модель обеспечения повсеместно доступного, удобного и оперативно предоставляемого по требованию сетевого доступа к разделяемому пулу конфигурируемых вычислительных ресурсов (таких как сети, серверы, хранилища, приложения и услуги). Доступ может быть предоставлен быстро, с минимальными затратами на управление и взаимодействие с сервис-провайдером.

В современном мире единую инфраструктуру «облака» формируют и развивают сотни производителей, но при этом о реализуемой ими системе гарантированной защиты технологического процесса эксплуатации облаков мало что известно, более того, в ряде опубликованных аналитических материалов высказываются серьезные опасения по поводу обеспечения информационной безопасности облачных технологий.

Критичные с точки зрения безопасности информационные объекты в облаке довольно нечетки и аморфны. Безопасность даже идеально проверенного в части исходных кодов приложения может быть разрушена «некодовыми» компонентами. Поэтому пользователи всех «облачных» программных продуктов постоянно подвергают себя информационному риску, и, как правило, неосознанному.

Отсутствие эффективного государственного контроля над облачными технологиями, реализуемыми коммерческими структурами, создает атмосферу настороженности вокруг внедрения этого процесса в электронное государственное управление, стало общей проблемой информационной глобализации и формирования единого мирового информационного пространства.

В настоящее время основу ряда систем электронного государственного управления, разработанных в 2000 годы, составляют так называемые «гибридные облака», соединившие в себе методы внешней и внутренней доставки услуг, что позволяет

объединить в одной системе четыре блока: «государство-граждане», «государство-бизнес», «государство–общественные организации», «государство-государство». И именно это обусловило появление политического риска в процессе функционирования таких систем.

Электронное государственное управление, при котором хранение информационных ресурсов организовано на удаленном сервере, несет, на наш взгляд, следующие информационно-политические риски:

1.Возможность прерывания интерактивного диалогового режима органов власти с населением. При этом возможно прекращение оказания электронных услуг населению, или отчуждение граждан от участия в процессе принятия государственных решений. Все это может вызвать волну протестных проявлений, эскалацию социально-политической напряженности.

Среди возможных причин прерывания интерактивного диалогового режима можно назвать:

-человеческие ошибки в управлении, последствия от которых будут тем катастрофичнее, чем больше размер облака, поскольку «человеческий фактор» порождает ошибки с самой большой вероятностью;

-цифровые атаки на программные модули и целенаправленное внедрение в гибридное облако злонамеренных «хищных» процессов, состоящих из «безобидных» частей, проходящих через все фильтры безопасности гибридного облака. Но «собравшись» в облаке, «хищные» процессы объединяют усилия, наносят удар, причем с максимально возможным ущербом для облака.

2.Возможность блокирования доступа к общественно-значимой информации. Данный риск связан с тем, что на существующих пиках пользования электронными услугами (праздники, катастрофы, социально-экономические потрясения) вероятны невосполнимые дефициты ресурсов, и «облако» может «зависнуть», быть парализовано по аналогии с существующей сотовой связью в праздничные дни. Не исключены и потери данных, находящихся в стадии обработки, из-за дефицита ресурсов облака в таком случае. Это может повлечь снижение уровня доверия населения к власти и дезориентацию основных социальных слоев общества.

3.Возможность утечки персональных данных и иной конфиденциальной информации. В частности, перехват данных при их передаче. Одной из причин может быть недостаточно эффективное удаление данных, когда утечка фрагментов данных происходит через неочищенные динамические пространства памяти. Атака клиппирования пакетов в

маршрутизаторах позволяет процессам, расположившимся в памяти, ранее занятой другими процессами, читать в больших объемах информационный «мусор» и вести эффективную аналитическую разведку. При этом возникает проблема борьбы с инсайдерами, находящимися в структурах облачных технологий, а также хакерами и кибертеррористами.

Утечка информации о персональных данных в системе электронного государственного управления может привести к массовому недовольству пользователей, обуславливает рост недоверия к интерактивной форме взаимодействия с органами власти, может активизировать протестные выступления граждан.

4.Возможность разглашения в системе электронного межведомственного документооборота служебной информации ограниченного доступа, критически важной информации. Риск кроется в реальной возможности компрометации такой информации сервис-провайдером. Особенно критична для электронного государственного управления компрометация ключевых документов пользователей. К сожалению, выбрав в качестве технологии гибридное облако, приходится доверять своему провайдеру, при этом ничем не обосновывая это доверие, поскольку другой альтернативы в данном случае нет.

При использовании в межведомственном электронном обмене данными гибридного облака возможна потеря изоляции пространства индивидуального потребителя, что также может рассматриваться как риск. При этом возникает вопрос, а какие реальные механизмы контроля коммерческой структуры - владельца облака у нас имеются кроме договора и его «честного слова»?

5.Возможная остановка процесса внутриведомственного и межведомственного обмена документированной и недокументированной информацией. Этот риск проявляется в результате использования в гибридном облаке односторонней аутентификации. Любая интерактивная система, допускающая одностороннюю аутентификацию, является крайне уязвимой для внешних угроз. И система электронного государственного управления – не исключение. В результате может произойти временное прекращение работы министерства или ведомства, приостановиться процесс оказания электронных государственных услуг населению по принципу «одного окна», прерывание связи и контроля над объектами критически важной инфраструктуры и т.п.

Особо тяжкие политические последствия могут возникнуть, если остановка процесса внутриведомственного и межведомственного обмена такой информацией произойдет, например, в день голосования или проведения референдума. Тогда могут

возникнуть предпосылки для оспаривания результатов голосования, появится сомнение в легитимности избранных представителей власти.

Таким образом, считаем, необходимо учитывать, что применение облачных технологий в системе электронного государственного управления трансформирует программно-сетевые и технологические риски в политические.

Проецирование выявленных рисков на политическую сферу раскрывает реальную социально-политическую опасность применения облачных технологий в электронном государственном управлении. Все это ставит новую научно-практическую задачу перед отечественной политологией, документоведением, юриспруденцией, теорией государственного управления, информатикой и другими научными дисциплинами по разработке комплекса мер выявления, управления и минимизации информационно-политических рисков, в том числе, гибридного облака, применяемого в рамках электронного государственного управления.

Нашим научным коллективом впервые в стране разработана теория и практика общественной информационной экспертизы, ведется подготовка экспертов-документоведов, способных решать многие из обозначенных выше задач. Кроме того, нами разработано новое научное направление в политологии, обозначенное как информационно-политическая рискология с тем, чтобы на научной основе высказать предложения по минимизации рисков и угроз в этой сфере.

По всем этим вопросам успешно защищены докторская и несколько кандидатских диссертации, опубликованы научные статьи и методические материалы. Ряд конкретных предложений нами внесен в виде проектов законов и нормативных актов в областную Думу и Правительство области. Эта работа, на наш взгляд полностью соответствует политической установке, данной Президентом страны на совещании в Новосибирске в 2012 году: необходимо «***привлечь граждан к разработке и тестированию сайтов и информационных продуктов государственных ведомств. Они должны быть действительно удобны и понятны в обращении, должны быть развёрнуты к человеку».***

Не сомневаемся, что совместные усилия власти, научного сообщества и граждан будут способствовать успешному продвижению России по пути к информационному обществу.