МУЛЬТИСТЕЙКХОЛДЕРНЫЙ ПОДХОД В УПРАВЛЕНИИ ИНФОРМАТИЗАЦИЕЙ

ЧЛЕН КОМИТЕТА СОВЕТА ФЕДЕРАЦИИ ПО НАУКЕ, ОБРАЗОВАНИЮ, КУЛЬТУРЕ И ИНФОРМАЦИОННОЙ ПОЛИТИКЕ, ПРЕДСЕДАТЕЛЬ КОМИССИИ СОВЕТА ЗАКОНОДАТЕЛЕЙ СОВЕТА ФЕДЕРАЦИИ ПО РАЗВИТИЮ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Руслан Усманович Гаттаров

Сегодня инфокоммуникационные технологии обеспечивают все большее сокращение дистанции между органами государственного управления и институтами гражданского общества. Однонаправленная модель управляющей коммуникации, когда решения принимаются «наверху» и спускаются «вниз» для исполнения, недостаточно эффективна в сложных мультистейкхолдерных системах. В архитектуре частно-государственных отношений «вертикаль» во многих их аспектах заменяется «горизонталью».

Горизонтально ориентированная коммуникация основана на сетевом принципе. В обсуждении вопросов и принятии решений по ним должен участвовать широкий круг заинтересованных лиц и групп. Государственное управление может быть поднято на качественно новый уровень через мобилизацию социального капитала общества. Для этого перспективно использование мультистейхолдерного подхода, представляющего собой один из видов сетевого метода принятия решений. Его суть заключается в совместном обсуждении проблемной ситуации всеми ключевыми ее участниками и поиске оптимального пути нормализации с учетом интересов всех сторон. В вопросах государственного управления ключевыми участниками, как правило, являются ответственные госорганы, бизнес-структуры, представители гражданского общества. В ходе дискуссии достигается синхронизация мнений о том, что именно следует регулировать, с помощью каких норм и как эти нормы будут применяться на практике. Так создается общая стратегия, внутренняя логика которой уравновешена системой сдержек и противовесов.

Однако, несмотря на все необходимые технологические возможности, конструктивное взаимодействие в сетевом формате не возникает само собой. Во-первых, мультистейкхолдерный

подход пока мало освоен государственными органами, которые еще испытают воздействие инерции прежней закрытости. Во-вторых, готовность бизнеса идти на компромисс с государством не всегда достаточна, поскольку ориентация государственной политики на создание прозрачных правил игры может вызывать рост конкуренции. В-третьих, представители гражданского общества пока еще не научились формулировать субъектную и ответственную позицию, которая согласовалась бы с законом и правоприменительной практикой. Тем не менее прилагать усилия в этом направлении необходимо, поскольку опыт должен нарабатываться, и в целом готовность каждого из элементов триады «государство – общество – бизнес» это позволяет.

Опираясь на описанное выше понимание, мы занялись институционализацией данного подхода в рамках Совета Федерации. При Совете законодателей Совета Федерации была создана комиссия по развитию информационного общества. В настоящий момент она преобразуется в орган уже при объединенном Совете законодателей Федерального Собрания Российской Федерации. Свою задачу мы видим в преодолении разрыва между федеральными органами власти, региональными ведомствами, разработчиками и поставщиками ИКТ-продуктов, потребителями, организации между ними конструктивного диалога и последующей выработке правил игры, рекомендаций, проектов нормативных актов. В заседаниях комиссии участвуют также представители федеральных ведомств, крупных ИТ-компаний, приглашенных в соответствии с повесткой дня экспертов.

Первым ключевым направлением, регулярно обсуждаемым в рамках комиссии, является электронное правительство. Для России электронное правительство – не просто технология, а инструмент модернизации. Система предоставления государственных услуг в нашей стране излишне зарегулирована и при этом слабо управляема. Нередки факты коррупции. Поэтому мы не можем просто описать работающую систему в «программных кодах». Наша задача – внедряя электронные технологии, проводить административную реформу, через электронное правительство менять государство. Вопрос внедрения электронного правительства имеет политический характер. От того, насколько успешно будет реализован проект, зависит будущее нашей системы государственного управления, уровень доверия общества к власти и, наконец, ее эффективность в решении конкретных задач.

С 1 июля 2012 года по всей стране была запущена в эксплуатацию так называемая региональная система межведомственного электронного взаимодействия (РСМЭВ). РСМЭВ является ключевым элементом электронного правительства и призвана обеспечить юридически значимый обмен данными между органами власти в электронном виде. Она должна заменить бумажный документооборот на электронный и избавить граждан от сбора большого количества разнообразных справок.

Анализ первых месяцев работы системы показывает, что разработка и запуск произведены с недостаточным качеством. Региональные правительства посылают бумажные письма курьерами, переписываются по электронной почте, используют информационные системы собственного производства. И лишь в незначительном объеме пользуются СМЭВ. Технологические причины – отсутствие в системе целого ряда необходимых электронных сервисов, неработоспособность или лишь частичная работоспособность других, постоянное изменение параметров, крайне недружественный интерфейс. Однако все это – лишь следствие системных ошибок. Выбранная монопольная модель реализации электронного правительства сама по себе порочна. При этом ответственность за результат оказалась размыта. Не работают федеральные сервисы – виновен ФОИВ, региональные – регион. Но проблема в том, что низкий уровень качества компонент общего пользования не позволяет объективно сравнить регионы между собой.

Опыт большинства успешных проектов запуска электронного правительства в других странах говорит о том, что они реализуются только при наличии единого центра, определяющего стратегию, подотчетного непосредственно первым лицам государства и обладающего полномочиями ставить задачи ведомствам. В России наличия такого центра пока не ощущается.

Опросы регионов, а также получателей госуслуг показывают, что региональные органы власти в основном добросовестно выполняют ФЗ-210 и не требуют с граждан лишние документы. Однако для обмена информацией СМЭВ используется в незначительном объеме. Информационная система, широко потребовавшая для своего создания немалого количества бюджетных средств – как федеральных, так и региональных – пока не выполняет поставленных задач.

По данным официальной статистики обращения субъектов РФ к электронным сервисам федеральных органов власти, размещенной по адресу http://www.interfax.ru/spravkinet/regstatobr.asp, налицо крайняя неравномерность распределения обращений. Более 90% запросов обеспечивают 10% субъектов РФ. Почти в 60% регионов количество запросов находится на уровне статистической погрешности, то есть больше чем в половине регионов страны взаимодействие через СМЭВ практически не осуществляется.

Примерно по 50% федеральных сервисов, необходимых регионам (программы, обеспечивающие доступ к базам данных федеральных органов власти), нужная информация на технологическом портале СМЭВ отсутствует. Из нескольких десятков федеральных сервисов, зарегистрированных в СМЭВ, стабильно работают лишь два: доступ к сведениям ФНС и Росреестра. Но и эти сервисы функционируют небыстро – налажено лишь предоставление информации по ЕГРЮЛ/ЕГРИП и СНИЛС. Срок получения электронных ответов от Росреестра достигает трех-четырех недель. Нередко ответы вообще не приходят, при этом работающих механизмов воздействия на орган власти, не предоставляющий данные, нет. При возникновении сбоев система не позволяет оперативно выяснить, на каком уровне и по какой причине сбой произошел. Доступ к целому набору данных федеральных органов власти нестабилен (данные недоступны от 15 до 75% времени суток) – статистика представлена на http://smev.iac.spb.ru/monitor/federal.jsp.

Нестабильность работы системы связана с постоянной доработкой стандартов отображения данных в СМЭВ. Вслед за изменением стандартов федеральные органы власти вносят изменения в свои сервисы, следом изменения должны вносить регионы, иначе данные не будут стыковаться и обмен информацией будет невозможен. Эта работа происходит несогласованно и долго. В СМЭВ отсутствует автоматизация процессов управления изменениями и управления эксплуатацией (в том числе разрешения конфликтов), что критично для такой сложной системы. Ошибки в программном обеспечении исправляются очень медленно, пожелания по доработке не учитываются, система отличается крайне недружественным интерфейсом. Текущий прогноз по вводу оставшихся сервисов СМЭВ – конец 2012 года. Этот срок вызывает у экспертов большие сомнения ввиду отсутствия соответствующих кадровых ресурсов, а также общего состояния готовности федеральных сервисов.

В связи с вышесказанным мы считаем принципиально важным создание единой системы управления изменениями (разработка методологии и техническая реализация). В противном случае через непродолжительное время функционирование СМЭВ станет невозможным из-за критического количества накопившихся изменений и ошибок. Второй необходимый инструмент обеспечения надежности СМЭВ – система управления инцидентами на базе Минкомсвязи России. Без создания такой системы существует серьезная угроза массовых случаев нарушения сроков оказания услуг и судебных исков. И, наконец, в обозримые сроки должно быть обеспечено безвозмездное для субъектов РФ функционирование СМЭВ и всех региональных систем межведомственного электронного взаимодействия с применением облачных технологий с последующим возможным выводом из эксплуатации субъектами РФ РСМЭВ. В противном случае будет крайне сложно реализовать включение в РСМЭВ всех участников межведомственного взаимодействия, что регулярно приводит к задержкам при оказании государственных/муниципальных услуг и неоправданным финансовым издержкам во всех субъектах РФ.

Вторым важным направлением, к разработке которого мы только приступаем, является кибербезопасность. Интернет стремительно развивается и начинает оказывать все большее влияние на реальность. Стремительно растут объемы неструктурированных, в том числе персональных данных. Использование облачных технологий вошло в норму на всех уровнях бизнеса и сейчас все глубже проникает в государство и гражданское общество. Это в корне меняет взгляд на принципы работы с информацией. Суперсовременное оборудование и новейшее программное обеспечение начинают предоставляться как сервис, уравнивая в возможностях транснациональные корпорации, малый бизнес и отдельных пользователей.

Все это делает вопросы информационной безопасности чрезвычайно актуальными для государства, бизнеса и гражданского общества. А как обеспечить всестороннюю безопасность в Се-

ти? Ею в принципе невозможно управлять из одного центра. Таким образом, мы приходим к модели коллективного или распределенного управления.

В Сети должны быть обеспечены:

– конфиденциальность – обеспечение доступа к информации только тех субъектов, которые имеют на нее право;
– целостность – исключение несанкционированной модификации информации;
– доступность – исключение временного или постоянного ограничения доступа к информации пользователям, имеющим на нее право;
– неотказуемость – удостоверение имевшего места действия или события таким образом, чтобы эти события или действия не могли быть позже отвергнуты;
– подотчетность – обеспечение идентификации субъекта доступа и регистрации его действий;
– достоверность – соответствие предусмотренному поведению или результату;
– подлинность – гарантия того, что субъект или ресурс идентичны заявленным.

Сегодня эти принципы далеко не всегда реализуются. Примеры – взломы сайтов госорганов, утечки персональных данных, фишинг, спам и т.д. В России действует ряд нормативных документов, так или иначе имеющих отношение к кибербезопасности. Однако они либо устарели, либо касаются узкого круга вопросов, таких как защита критической инфраструктуры. В то же время государству и обществу необходима выработка целостного документа, определяющего системный подход к обеспечению кибербезопасности.

Мы должны определить ключевые направления реализации стратегии. В рамках каждого направления должны быть описаны политика, необходимые шаги, ответственные лица. Такими направлениями могут быть:

– обеспечение безопасности ведения бизнеса как непосредственно в Интернете, так и с использованием ИКТ-инфраструктуры;
– обеспечение гарантий прав граждан (защита частной жизни, персональных данных и т.д.);
– защита национальной ИКТ-инфраструктуры;
– реализация современных систем управления с использованием ИКТ (электронное правительство и т.д.);
– построение эффективных механизмов борьбы с киберпреступлениями;
– противодействие массированным кибератакам.

Безусловно, следует работать с моделями угроз. Например:

– давление на личность (посредством сбора персональной информации и манипуляции ею);
– экономическая блокада (отключение платежных систем, систем бронирования и т.д.);
– аппаратная атака на персональные компьютеры граждан и организаций;
– атака на бытовые объекты;
– атака на критически важную инфраструктуру (кибервойна);
– киберпреступления (хищения, мошенничество, спам, фишинг и т.д.);
– распространение опасного контента (детская порнография и т.д.).

Нам необходимо обсуждать инфраструктуру кибербезопасности: национальные аппаратную и программную платформы, электронные системы управления, корневую инфраструктуру и медиаструктуру Интернета – национальные стандарты кибербезопасности, кадровое обеспечение данной сферы и др. Проблематику такого масштаба не охватит не только отдельное ведомство, но и государство в целом. Для эффективной работы в таких сложных областях возможен только мультистейкхолдерный подход.

Третьим направлением работы комиссии, тесно связанным с кибербезопасностью, является создание национальной программной платформы на базе свободного ПО. Комиссия констатировала недостаточное внимание ответственных ведомств к вопросу продвижения свободного программного обеспечения, разработанного отечественными компаниями. Между тем этот вопрос стратегически важен для государства. Использование свободного ПО дает целый ряд преимуществ:

1. Снижается зависимость страны от зарубежных разработчиков ПО, которая может оказаться критической в случае конфликта.

2. Бюджет перестанет платить миллиарды за лицензии, которые нужно обновлять раз в три-четыре года (средний срок жизни программного продукта). Переход от покупки лицензий к покупке технического сопровождения программ, которые сами по себе распространяются бесплатно, в несколько раз снижает расходы на информатизацию.
3. Будут сужены каналы утечек стратегической информации и персональных данных. Открытый машинный код дает возможность проверить приобретаемое программное обеспечение на отсутствие скрытых закладок, шпионских программ и т.д.
4. Исчезает зависимость потребителя от конкретного поставщика программного продукта. Становятся возможными смены недобросовестных подрядчиков, поскольку ПО с открытым кодом может сопровождать любая квалифицированная компания.
5. Бюджетные средства останутся в стране и пойдут на зарплаты российским специалистам, создание российских инновационных технологий. Реализуется поддержка отечественных производителей ПО и создания тем самым конкурентоспособных российских программных продуктов.

Отечественные программные продукты с открытым кодом должны быть систематизированы в рамках национальной программной платформы. Распоряжением Правительства Российской Федерации №2299-р определен целый ряд мероприятий по ее созданию. По значительной их части сроки уже не соблюдены, перспективы туманны. Комиссия рекомендовала Минкомсвязи России ускорить создание национальной программной платформы и заявила о своем намерении возвращаться к этому вопросу до тех пор, пока все необходимые мероприятия не будут выполнены.

Наконец, *четвертое важное направление* деятельности Комиссии – защита прав субъектов персональных данных при их автоматизированной обработке. Руководством Совета Федерации принято решение о создании постоянно действующего Совета по защите прав субъектов персональных данных под руководством Председателя Совета Федерации. Проблема защиты прав субъектов персональных данных становится все более актуальной. Количество разнообразных персональных данных постоянно увеличивается (данные о движении средств, покупках товаров, личные предпочтения, результаты анализов и показатели здоровья и т.д.) наряду с ростом числа каналов коммуникации, по которым возможна их утечка. В этой связи необходима организация системной работы по защите прав субъектов персональных данных. В соответствии с Конвенцией о защите физических лиц при автоматизированной обработке персональных данных, в каждой стране-участнице должен существовать как минимум один независимый орган, занимающийся данной проблематикой.

В действующем законодательстве по персональным данным масса нестыковок и белых пятен.

1. Действующий Федеральный закон №152-ФЗ «О персональных данных» направлен в большей степени не на защиту граждан, а на установление технологических требований к обработке персональных данных, по своей сложности сравнимых с защитой информации, составляющей государственную тайну. По оценкам экспертов, буквальное исполнение закона потребует суммарных затрат порядка 5% ВВП. Именно поэтому он исполняется некорректно.
2. В действующей редакции закона Роскомнадзор проверяет несоответствие операторов персональных данных требованиям, а не фактические утечки. Наказывает за нарушение буквы закона, а не за нанесение ущерба гражданину. Меры ответственности также недостаточны.
3. Отсутствует единый регулятор в области персональных данных, подчиняющийся непосредственно правительству.
4. Не приняты изменения в целый ряд нормативных актов, регулирующих отрасли, оперирующие огромными объемами персональных данных (банки, страховые компании, здравоохранение и т.д.). В результате ряд отраслевых законов фактически противоречит Федеральному закону №152-ФЗ.
5. Недостаточно проработаны ведомственные технические регламенты обработки персональных данных.

Требуется определить минимальный перечень информации, которую необходимо запрашивать у граждан в различных ситуациях (при трудоустройстве, приеме в учебное заведение и т.д.) и запретить запрашивать больше. Персональные данные должны быть четко отделены законодательством от личных данных. Пора, наконец, ратифицировать Конвенцию о защите физических лиц при автоматизированной обработке персональных данных. Возможно, актуальным является отделение общих данных от данных, обрабатываемых спецслужбами, и установление различных режимов для этих категорий данных. Вот далеко не полный фронт работы на этом направлении, и мы намерены последовательно приступить к ней.

Подводя итог вышесказанному, можно заключить, что мультистейкхолдерный подход, который реализован в деятельности комиссии, на наш взгляд является продуктивным. Результатами становятся идеи и конкретные документы, которые содержат последовательные рекомендации по их воплощению. Принципиально важным мы считаем наработку практики участия заинтересованных сторон во взаимодействии по сетевому принципу. Многостороннее представительство позволяет сделать вырабатываемые предложения сбалансированными и обоснованными.