Законодательное обеспечение информационной безопасности

Владимир Лопатин, депутат Государственной Думы РФ

Вопросами информационной безопасности я начал заниматься в союзном парламенте, в комиссии академика Рыжова, где в 1989 году мы впервые ввели в оборот понятие "информационная безопасность". С тех пор многое изменилось. По нашим предложениям был принят Закон о безопасности, создан Совет Безопасности Российской Федерации, межведомственная комиссия Совета Безопасности по информационной безопасности. Созданы, по аналогии с ситуационной комнатой Белого Дома США, ситуационные центры в Администрации Президента, в Правительстве РФ, в Совете Безопасности России, во многих министерствах, ведомствах, спецслужбах.

Но от этого, к сожалению, наша жизнь не стала более безопасной, в том числе в информационной сфере. Это подтверждают как скандалы по сбору и распространению компромата, что является прямым покушением на неприкосновенность частной жизни граждан – на примере ситуации вокруг Скуратова, так и примеры по войне в Югославии или провалившаяся попытка преодолеть вето Президента РФ на Закон "О Высшем Совете по защите нравственности телевещания и радиовещания в Российской Федерации", где под предлогом защиты нравственности стремились протащить некую структуру с функциями цензуры.

Сначала я хотел бы определить, что такое информационная безопасность и какое место она занимает в информационной сфере, а также сказать несколько слов о месте законодательства об информационной безопасности в системе российского информационного законодательства. Речь идет о законодательном регулировании четырех основных сегментов информационной сферы. Первое – это законодательство о средствах массовой информации, второе – законодательство о связи и телекоммуникациях, третье – законодательство об объектах интеллектуальной собственности и четвертое – это законодательство об информационной безопасности. На сегодняшний день эта структура информационного законодательства пока носит неоформленный характер, и, к сожалению, мы не можем сказать, что у нас есть концепция развития законодательства как в целом в информационной сфере, так и по отдельным направлениям.

На мой взгляд, сейчас необходимо решать в приоритетном порядке вопросы, связанные с законодательным обеспечением информационной безопасности.

Сегодня есть два подхода к определению предметной области информационной безопасности. Одни (это, прежде всего, гуманитарии) говорят, что информационная безопасность – это только то, что связано с тайной, и ничего более. Другие (представители ФАПСИ и спецслужб) утверждают, что к информационной безопасности относится все, что происходит в информационной сфере. На мой взгляд, как всегда, истина лежит посередине, и я предлагаю понимать под информационной безопасностью состояние защищенности основных, жизненно важных интересов личности, общества, государства от внутренних и внешних угроз в информационной сфере.

Понятие информационной безопасности включает в себя несколько основных элементов. Во–первых, это основные, жизненно важные интересы личности, общества и государства. В каком соотношении находятся эти интересы? Одни говорят, что на первом место должны стоять интересы личности. Представители ФАПСИ и Минюста утверждают, что на первом месте должны стоят интересы государства.

Скорей всего мы все–таки придем к тому, что должен быть баланс интересов.

Вторая составная часть – угрозы жизненно важным интересам личности, общества, государства. Они подробно перечислены в Концепции национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 17 декабря 1997 года. Этот Указ определил основные жизненно важные интересы и угрозы, как внутренние, так и внешние, этим интересам в информационной сфере, а также принципы и задачи защиты от этих угроз.

Что касается вопроса о том, кто и как должен обеспечивать информационную безопасность, ответ на него нигде не зафиксирован в четко выраженном виде. Это приводит к постоянной борьбе между спецслужбами и информационщиками, к отсутствию четко выраженных приоритетов и, соответственно, к неэффективному решению тех или иных задач, заявленных в Концепции национальной безопасности.

Наш подкомитет по информационной безопасности попытался решить некоторые проблемы,

связанные с отсутствием концепции развития законодательства в информационной сфере.

Первое – проанализировали действующее законодательство: около 20 международных договоров и соглашений, участником которых является Россия, около 100 федеральных законов, 150 подзаконных федеральных нормативных актов (указы, постановления, распоряжения), сейчас приступили к анализу регионального законодательства. Выводы, которые можно сделать из этого анализа, неутешительны: законодательство противоречиво, декларативно и страдает большим количеством белых пятен. То есть общественные отношения, реальная практика и жизнь существенно опережают наше законодательство.

Второе – подготовили проект Концепции развития законодательства в сфере информационной безопасности. Она издана в виде брошюры тиражом 1000 экземпляров на 160 страницах, есть в электронном виде на моей страничке в Интернете и на сервере Госдумы, издана на лазерном диске тиражом 5 тысяч для участников форума–выставки "Технологии безопасности". Мы признательны всем, кто участвует в обсуждении и доработке этой концепции.

В основу этой концепции положены следующие основания. Первое – защита самой информации и прав на нее, второе – защита информационных систем, в которых эта информация циркулирует, третье – защита общества, человека от воздействия "вредной" информации. Все три объекта защиты тесно связаны со средствами массовой информации, связью, телекоммуникациями, в том числе объектами интеллектуальной собственности. Поэтому они в той или иной степени косвенно присутствуют. Когда будет сформулирована общая концепция развития информационного законодательства, я думаю, что будет более четкое разделение этих областей.

Итак, первый объект – это защита самой информации. С точки зрения права, вся информация делится на две больших части. Первая часть – это информация с ограниченным доступом, вторая часть – это общедоступная информация. В общедоступной информации сегодня ученые различают около 20 основных видов информации. Но при этом здесь есть сегмент, который стоит на особом месте – это информация, доступ к которой не может быть ограничен.

Первая часть – в соответствии с Посланием Президента Федеральному Собранию (1998 год), где он определил основное направление развития внутренней государственной политики в этом вопросе как сужение области ведомственных тайн, – должна уменьшаться, зато вторая часть и особенно информация, доступ к которой не может быть ограничен, должна расширяться.

Однако следует иметь в виду, что в секторе общедоступной информации стоят такие виды информации как объекты интеллектуальной собственности. Кроме ноу–хау, которое защищается в режиме коммерческой тайны, все остальные объекты интеллектуальной собственности защищаются особыми институтами – авторского, патентного права и т. п. Это общедоступная информация, но ее использование влечет за собой ряд ограничений, которые установлены законодательством в сфере интеллектуальной собственности. Это надо знать, потому что здесь, к сожалению, нынешнее пиратство и масштабы вседозволенности просто поражают. Мы имеем одно из лучших в мире законодательств в сфере авторского права, в сфере интеллектуальной собственности, но мы сегодня стоим на одном из последних мест по его применению, потому что, к сожалению, авторы не знают своих прав.

Вот почему я предложил уже в ближайшее время ввести во всех вузах страны, независимо от получаемой специализации, обязательную дисциплину "Основы авторского права", чтобы все выпускники: техники, инженеры, гуманитарии – могли бы знать свои права в этой области и могли их защищать.

Какие законы регулируют информационное пространство? В сфере общедоступной информации – это законы "Об информации, информатизации и защите информации" и "О международном информационном обмене". К сожалению, эти законы противоречат не только друг другу, но и другим законам. Поэтому мы предлагаем внести ряд поправок. Также в Государственную Думу внесен и принят в первом чтении Закон "О праве на информацию". Сейчас идет подготовка ко второму чтению, и он будет называться "О праве на доступ к информации".

Кроме того, здесь нужны еще два закона, которые имеют особое значение для компьютерных сетей: Закон "Об электронно–цифровой подписи" и Закон "Об электронном документообороте". Из–за отсутствия этих законов мы не можем пользоваться многими информационными системами Запада. Например, Европейский Союз три года готовил такую унификацию, и сейчас у них создана единая унифицированная система защиты информации в единой компьютерной сети.

Как я уже говорил, в области защиты интеллектуальной собственности мы имеем одно из лучших

в мире законодательств. Здесь не отрегулирован только один вопрос, касающийся прав государства на объекты интеллектуальной собственности, полученные за бюджетный счет. Например, за последние три года в США выдано 800 американских патентов на наши дорогостоящие высокие технологии. Причина – наши авторы не желают использовать наше законодательство в силу его затратности, а государство не может это сделать, так как в законе это не записано. Например, МИГ–31 был продан по частям в Китай, при этом большая часть узлов не была запатентована нашими российскими производителями, и в итоге мы сейчас будем у Китая покупать то, что изобрели сами. Вот почему я внес в Государственную Думу проект закона "О реализации прав государства на объекты интеллектуальной собственности".

Что касается законодательства об информации с ограниченным доступом, то следует сказать, что когда мы начинали делать в 1995 году анализ российского законодательства, было 30 видов тайн, сейчас насчитывается около 40 видов тайн, и перечень постоянно пополняется. Например, в проекте закона "О внесении изменений в Закон "О почтовой связи" предлагают ввести наряду с тайной связи, еще и тайну почтовой связи. Другое министерство готовит проект закона, где фигурирует психологическая тайна. Напомню, что Закон "О средствах массовой информации" запрещает распространять информацию, которая составляет тайну. Соответствующая декларация есть во многих законах, постановлениях, где говорится о том, что за незаконное разглашение тайны наступает уголовная, административная, гражданско–правовая и другая ответственность. Причем, из этих 40 видов тайн в кодексах прописано только 12 видов тайн, т.е. реальная ответственность может наступить только при разглашении 12 видов тайн, остальные просто продекларированы и не более того. Вот почему мы предлагаем эти 40 видов тайн свести к шести основным видам.

Первый – это гостайна. Закон "О государственной тайне" действует, в 1997 году принят мой авторский закон о новой редакции этого закона. Сейчас мы готовим еще одно дополнение к данному закону с тем, чтобы снизить степень ответственности за рассекречивание или за незаконное разглашение информации под грифом "секретно", поскольку здесь достаточно, порой, и административной ответственности.

Второй вид тайны – это коммерческая тайна. Закон "О коммерческой тайне" рассматривался три года в Государственной Думе. Сейчас Президент РФ наложил вето под предлогом, что закон не нужен, у нас и так все хорошо. Но сегодня коммерческой тайной торгуют все, начиная от чиновников, которые получают доступ к коммерческой тайне в силу своих служебных обязанностей, заканчивая журналистами, которые распространяют эту информацию, получив ее от тех или иных лиц. К сожалению, проблема недобросовестной конкуренции и промышленного шпионажа стоит сегодня как никогда остро. Вот почему Закон "О коммерческой тайне" нужен. Совместно с Администрацией Президента создана Комиссия по доработке данного закона, куда я вошел от Государственной Думы. Надеюсь, что он все–таки будет подписан Президентом и вступит в действие.

Третий вид тайны – банковская тайна. Сегодня есть статья 26 Закона "О банках и банковской деятельности". Центробанк России, ФАПСИ говорят, что этого достаточно, давайте мы банковскую тайну будем защищать как коммерческую тайну. Но это полное непонимание правовой природы банковской тайны. Для того, чтобы возникла коммерческая тайна, достаточно, чтобы любое лицо, занимаясь предпринимательской деятельностью, сказало: "Вот эта информация – коммерческая тайна". Ему нигде не надо ее регистрировать. Его права будут реализованы только тогда, когда он будет защищаться в суде, где будет доказывать, что его права нарушены. Для возникновения банковской тайны нужны, как минимум, два субъекта. Это владелец тайны – любой клиент, который доверил тайну банковского вклада, счета, информацию о своей частной жизни, и сам банк как пользователь, как вторая сторона в этом процессе, без которой банковская тайна просто невозможна. Мы надеемся, что этот закон все–таки будет подготовлен в этом году и будет внесен в Государственную Думу.

Четвертый вид тайны – это профессиональная тайна. Пятый – служебная тайна. Чем отличается профессиональная тайна от служебной тайны? Профессиональная тайна – это чужая тайна, которая стала известна лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой. Например, тайна исповеди, тайна нотариуса, адвокатская тайна, тайна страхования и т.д. Служебная тайна – это чужая тайна, которая стала известна чиновнику, т.е. представителю органов государственной власти и местного самоуправления в связи с исполнением им своих служебных обязанностей.

И, наконец, последний, шестой вид тайны – это персональные данные как особый институт охраны права на неприкосновенность частной жизни. В Государственную Думу внесен Закон "Об информации персонального характера", но мы надеемся, что он все–таки будет переименован, как это сделано уже в большинстве стран мире, где есть такие законы. Сегодня есть 25 национальных законов о персональных данных, есть соответствующая конвенция в Европе по этому вопросу с

таким же названием, и мы надеемся, что именно такой закон о персональных данных и будет принят.

Я хотел бы остановиться на некоторых моментах, которые, на мой взгляд, носят достаточно принципиальный характер. Первое, что касается подслушивания, подглядывания и использования этой информации, в том числе через средства массовой информации, поскольку распространение информации о частной жизни лица происходит, как правило, через СМИ.

Я напомню, что есть Закон "Об оперативно–розыскной деятельности", который устанавливает, что только два министерства и ведомства: ФСБ и МВД – имеют право в своем составе иметь спецподразделения и спецсредства для проведения негласного съема информации. Никакие детективные агентства, никакая частная охрана, никакие другие государственные структуры, кроме ФСБ и МВД, не имеют, по закону, права заниматься негласным съемом информации. Это первое основание, которое установлено в данном законе.

Второе основание. Негласное подглядывание, подслушивание возможно только лишь на основе судебного решения. Если судебного решения нет, то даже МВД и ФСБ не могут провести такие оперативно–розыскные мероприятия. Если эти правила не соблюдается, то, соответственно, гражданин имеет три дополнительных механизма защиты своих интересов. Он имеет право: а) обратиться в вышестоящий орган и обжаловать действия конкретного должностного лица, если ему это стало известно; б) он имеет право получить информацию, которая собрана в отношении него негласным способом, если уголовное дело, которое было при этом возбуждено, прекращено и доказана его несостоятельность; в) должностные лица обязаны восстановить права граждан, которые были нарушены в ходе оперативно–розыскных мероприятий.

А как же быть тогда со средствами массовой информации, с редакциями газет, представители которых проводят такого рода операции, располагают такого рода информацией? Как быть гражданину в данной ситуации? Европейский суд по правам человека, на мой взгляд, вынес однозначный вердикт: при коллизии, которая возникает между правом на доступ к информации и правом неприкосновенности частной жизни, приоритет имеет право неприкосновенности частной жизни. Как известно, Россия является участником Совета Европы, а Европейский суд по правам человека – это высшая инстанция на Европейском континенте, и мы обязаны выполнять его решения.

Отсюда напрашивается необходимость соответствующих изменений в законодательстве о средствах массовой информации, чтобы названные выше три механизма, обеспечивающие защиту частной жизни гражданина перед госструктурами и спецслужбами, были записаны в Закон "О средствах массовой информации".

Еще один возникающий в связи с этим вопрос имеет отношение к публичным политикам. Как быть, если граждане хотят знать, что происходит с теми или иными известными лицами, государственными чиновниками и т.д., в том числе в их частной жизни. Опять же, есть соответствующая резолюция Европарламента по этому вопросу, которая утверждает, что при коллизии между правом на доступ к информации и правом на неприкосновенность частной жизни в отношении публичных политиков, общественных деятелей, приоритет имеет право на неприкосновенность частной жизни, за исключением случаев, которые оговорены в законе.

Закон должен установить четко информацию, которая может быть доступна гражданам, если есть такая коллизия, как это было, например, в случае с информацией о здоровье Президента. Государственная Дума должна принять закон, который бы четко прописывал, что информация, которая для обычных граждан составляет врачебную тайну, в данном случае должна предоставляться для всеобщего сведения, поскольку затрагиваются интересы государства и общества, которые находятся в зависимости от состояния здоровья того или иного руководителя.

Приведу еще один пример. Фактически в каждом более или менее крупном банке, на каждом более или менее крупном предприятии установлены так называемые офисные АТС. Они, как правило, импортного производства, и независимо от страны–производителя все они имеют встроенный блок полицейских функций, что позволяет снимать информацию о всех телефонных переговорах. Владельцу или руководителю предприятия, банка ежедневно на стол кладется распечатка всех телефонных переговоров: кто звонил, кому звонил и что говорил. Когда я начинаю спрашивать, почему это происходит, мне говорят: мы защищаем интересы банковской тайны, интересы служебной тайны, коммерческой тайны, промышленные секреты. А как быть в таком случае с неприкосновенностью частной жизни? В Конституции Российской Федерации записана тайна телефонных переговоров, телеграфных, почтовых и иных сообщений. Я был вынужден на специальном совещании с участием представителей Верховного Суда, Генпрокуратуры, ФСБ,

Госкомсвязи поставить вопрос о том, кто будет все–таки отвечать за обеспечение тайны связи, за неприкосновенность частной жизни. Оказывается, за это никто не отвечает и не хочет отвечать. Вот почему было предложено провести инвентаризацию всех таких телефонных станций и установить режим, обеспечивающий запрет на использование блока полицейских функций без соответствующих санкций, решения суда и т.д.

Проблемой является и переход в ряде регионов России на поминутную оплату телефонных переговоров. Практика показывает, что распечатка телефонных переговоров и хранение соответствующих сведений на магнитных носителях либо в бумажном виде непосредственно затрагивает тайну частной жизни. Режим защиты этой информации, к сожалению, на местах сегодня не обеспечен.

Европейский суд по правам человека рассматривал этот вопрос и пришел к выводу, что распространение данной информации без санкции лица, в отношении которого имеется такая информация, будет вмешательством в частную жизнь.

Эти примеры нарушения законодательства о неприкосновенности частной жизни наиболее типичны. Я специально заострил на них внимание, потому что, к сожалению, правовая некомпетентность большинства граждан приводит к манипулированию их правами.

До сих пор речь шла об информации и праве на нее как предмете системы информационной безопасности.

Второй объект защиты в системе информационной безопасности – это информационные системы и права на них. Все информационные системы с точки зрения права можно классифицировать по трем критериям: "государственные–негосударственные", "российские–международные", "открытые–закрытые". Представители ФАПСИ предлагают возложить на государство обязанность защищать как все виды информации, так и все виды информационных систем. Дай Бог, чтобы у государства хватило сил и средств защитить государственную и служебную тайну, защитить государственные, российские, закрытые информационные системы. Остальные виды тайн и другие виды инфосистем должны защищаться самими владельцами тайн и собственниками этих систем.

Государство должно установить только четкие правила функционирования и не более того, т.е установить правовые запреты. И здесь возникает ряд вопросов, на которых я коротко остановлюсь.

Что касается закрытых государственных информационных систем. Есть соответствующее решение Гостехкомиссии при Президенте РФ которая отвечает за защиту государственной тайны Российской Федерации, четкая рекомендация и обязательное для исполнения всеми органами государственной власти решение – не подключать государственные закрытые информационные системы к открытым информационным системам.

Приведу пример, подтверждающий правильность этого решения. В конце прошлого года Пентагон и Великобритания провели специальные учения, в ходе которых были предприняты электронные атаки на электронную сеть Пентагона. По завершении учений Служба безопасности информационных сетей Пентагона заявила, что лишь 30 процентов зафиксированных электронных атак были учебными. Остальные 70 процентов были вполне реальными нападениями на секреты Пентагона. По оценке экспертов, ежегодно в сетях Интернета происходит около 900 миллионов атак. И многие из них успешны.

Беда в том, что хакеры подвизаются не только на частной ниве, они работают сегодня и в интересах государств. Вот почему США, которые стоят на первом месте по развитию открытых информационных систем, Интернет–технологий и их применения, были вынуждены в феврале 1998 года принять решение о разработке нового проекта "Next generation Internet" (я его называю "Internet–2"). Они выделили полмиллиарда долларов на разработку этого проекта, который будет иметь не только большие возможности и большие скорости, но и будет более закрытым для доступа. Они сейчас пытаются отсоединить от открытых информационных систем свои системы управления оружием, органы государственной власти, а мы еще не присоединяли, поэтому нам не нужно повторять этих ошибок, мы должны использовать этот 30–летний мировой опыт и идти дальше.

Еще одна проблема. На сегодняшний день программный продукт на территорию СНГ поставляет в основном Америка, информационные технологии – Европа, персональные компьютеры поставляет для нас в основном Юго–Восточная Азия по японским и американским технологиям. Мы же в основном потребители, наше производство составляет ничтожную долю по всем трем составляющим. К чему это приводит? Приведу только один пример. На территории Российской Федерации за 90–е годы число междугородных цифровых телефонных станций импортного

производства увеличилось с двух до 80. Мы провели специальное исследование и выяснили, что на каждой станции есть "черный ящик" с программным продуктом, к которому наши пользователи не имеют доступа. А у нас сегодня большинство открытых информационных сетей построено на модемной связи через эти самые междугородные телефонные станции. И вот ситуация: в определенное время "Ч" через спутник проходит соответствующий сигнал, активизируется закладка обратной связи в АТС и либо идет съем информации, либо, что хуже во много раз, идет вывод из строя, уничтожение, модификация системы управления органов государственной власти, производствами, банковскими потоками и т.д.

Достаточно сказать, что сегодня весь федеральный бюджет переведен на казначейское исполнение. Принято решение в регионах России также перевести всю систему бюджета на казначейское исполнение бюджета. Это очень хорошо – сокращаются финансовые службы, бюджет становится более прозрачным и т.д. Но при проверке выяснилось, что связь казначейства с казначейством строится на открытой модемной связи. Влезть туда, модифицировать, похитить, исказить информацию – ничего не стоит. Вот почему сегодня возникает условие – не строить эти системы на основе модемной связи.

Недавно на сервере Министерства юстиции Российской Федерации, где выставлено все законодательство Российской Федерации для Совета Европы, систематически исчезала вся информация.

Так что вопросы информационной безопасности, защиты информационных систем выходят на одно из первых мест в системе национальной безопасности.

Что касается открытых информационных систем, и в частности Интернета, то сейчас идет большая дискуссия о том, насколько законным является применение СОРМ. Сегодня ни у кого не вызывает сомнения возможность проведения операций подслушивания на основании закона, судебного решения через телефонную сеть. Но Интернет как открытая информационная система используется и как вид связи, с помощью которого, через который и на основе которого разрабатываются, готовятся и осуществляются преступления. Вот почему мы сегодня должны быть готовы к тому, чтобы эту информацию, при наличии опять же судебного решения, использовать в интересах общественности, в интересах государства, в интересах добропорядочных граждан. Раньше таких технических возможностей не было.

Сейчас, благодаря усилиям специалистов из ФСБ, Госкомсвязи и т.д., такая техническая возможность есть. С точки зрения права, нет никаких оснований для паники, потому что продолжает действовать статья Закона "Об оперативно–розыскной деятельности", которая четко устанавливает обязательность двух названных выше условий: наличие судебного решения и право использовать спецсредства только МВД и ФСБ – без соблюдения которых невозможно проводить съем информации.

И, наконец, третий объект – защита личности и общества от воздействия так называемой "вредной" информации. Сегодня в законодательстве можно условно выделить следующие виды вредной информации: – информация, возбуждающая социальную, расовую, национальную, религиозную ненависть и вражду; – призывы к войне; – распространение порнографии; – недобросовестная, недостоверная, неэтичная, заведомо ложная, скрытая реклама; – информация, оказывающая деструктивное воздействие на психику людей.

По отдельным видам ограничения в законах уже определены, так, например, в Законе "О рекламе" установлено ограничение на скрытую рекламу. Есть и статья в УК РФ, но, к сожалению, механизма проверки, экспертизы реализации правового запрета до сих пор нет.

Особого внимания требует в законодательстве защита от информации, оказывающей деструктивное воздействие на психику людей.

Приведу только один пример. Секретарь Совета Безопасности Олег Лобов лично помогал распространению идей и взглядов запрещенной во многих странах мира и в Японии секты "Аум Синрике". Асахара чуть ли не ежедневно вещал по радио "Маяк", по телевидению.

Результат – на территории России во многих регионах секта существует и работает. По данным, которые были обнародованы на специальных парламентских слушаниях, сегодня в таких новокультовых образованиях на территории России участвуют около пяти миллионов человек. 70 процентов из них – молодежь, около одного миллиона – студенты. Четверть миллиона семей разрушены в такого рода сектах – "Белое братство", "Аум Синрике" и т.д. Это цифры, которые заставляют бить тревогу.

Средства массовой информации энергично пропагандируют колдунов, магов, экстрасенсов и т.д. Во многих газетах можно прочитать объявления о том, что патентованный колдун или колдунья снимет или наведет сглаз, порчу. Так называемые пси–технологии открыто используются во многих избирательных кампаниях. В штабах многих кандидатов в депутаты, в губернаторы, в президенты и т.д. сегодня обязательно присутствует один или несколько экстрасенсов, которые обеспечивают "наведение хорошей ауры", получая за это большие деньги.

И, наконец, компьютерные сети. Известен случай, когда 700 японцев попали в больницу с признаками эпилепсии после просмотра компьютерного мультика. Это опять же не случайность. Много лет во многих странах мира, в США в том числе, ведутся разработки типа МК–ультра, МК–дельта, программы ультрамозгового контроля, программы дистанционного управления поведением человека и т.д. По данным наших спецслужб, на подготовку информационных войн и разработку информационного оружия за 15 лет затраты увеличились в 4 раза. В США эти затраты сопоставимы с затратами на ракетно–ядерные космические программы. По сути дела, нас пытаются втянуть в новый этап гонки вооружений. Когда–то мы создали химическое оружие, потом средства защиты от него, теперь не знаем, что нам делать с 40 тысячами тонн отравляющих веществ – у нас нет денег на то, чтобы их уничтожить. Потом мы создали ядерное оружие, средства защиты от него, теперь не знаем, что делать со 100 подводными лодками с невыгруженными ядерными реакторами, каждая из которых – Чернобыль; не знаем, что делать с теми огромными запасами ядерных вооружений, у которых уже истекли физические сроки. Нам их нужно уничтожать, но у нас нет средств.

Сегодня нас пытаются втянуть в новый, не менее дорогостоящий этап гонки вооружений, необходимых для широкомасштабного ведения информационных войн. Вот почему, наряду с Законом " Об информационно–психологической безопасности" я был вынужден в 1997 году инициировать разработку международной Конвенции о запрещении информационных войн и ограничении оборота информационного оружия.

В декабре 1997 года эта инициатива была поддержана девятью парламентами стран СНГ, участвовавшими в работе межпарламентской ассамблеи СНГ, на которой я был докладчиком по этому вопросу. В марте 1998 года на встрече в Государственной Думе с Генеральным Секретарем ООН Кофи Аннаном я вновь изложил эту инициативу и просил его поддержки. В 1998 году МИД России внес эту инициативу от имени Российской Федерации в Организацию Объединенных Наций, и сейчас идет подготовка с целью заключения международной Конвенции о предотвращении информационных войн, ограничении оборота информационного оружия и создания международной системы информационной безопасности.

И последнее. Если Российское государство, как и любое другое государство, имело в начале XX века такие обязательные государствообразующие признаки, как территория, язык, единое население, то в конце XX века новым государствообразующим признаком является единое информационное пространство. Это новое понятие, это новый признак государства и отсюда – новые последствия для пересмотра системы международного права, для пересмотра систем наших взаимоотношений, для пересмотра систем не только науки, но и практики.

Что сегодня происходит? Мы являемся одной из немногих стран мира, на территории которой зарубежные информационные агентства распространяют для нас информацию о нас самих. Такого нет ни в одной стране мира, имеющей сколько–нибудь развитую информационную базу. Мы рискуем здесь попасть в информационную зависимость, когда в определенное время просто будет вброшена информация, которая не будет объективной, но которая будет положена в основу важных для судеб страны или регионов решений.

Вот почему сегодня, по всей видимости, настало время говорить о двух угрозах разрушения единого информационного пространства: со стороны иностранного вмешательства и со стороны регионального сепаратизма, когда наше единое информационное пространство раздергивается в клочья.

Таковы основные направления развития законодательства в сфере обеспечения информационной безопасности и некоторые проблемы его практического применения