
Э. М. БРАНДМАН

ЦИВИЛИЗАЦИОННЫЕ ИМПЕРАТИВЫ И ПРИОРИТЕТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Проблема императивов информационной безопасности – это проблема реально действующих факторов ее воздействия, в значительной степени определяющих ее стратегию и принципы, а также направления реализации на международном, региональном и национально-государственном уровнях организации и функционирования. Содержание их вытекает из анализа условий и проблем цивилизационного развития в наступившем XXI веке, из характера и приоритетных путей разрешения противоречий, сложившихся в информационной сфере, из реальных возможностей современных государств разрешить или не разрешить эти противоречия.

Всемерное развитие информационной сферы – это то, что реально может дать человечеству возможность продвигаться вперед к идеалам мира, свободы и социальной справедливости. При этом функционирование информационной сферы выводит на первый план гармоничное и подлинное развитие человека, фиксируя недостаточное внимание к личности со стороны индустриальных и постиндустриальных государств, приносивших личность в жертву технико-экономическому прогрессу.

Переход к постиндустриальной цивилизации сопровождается сменой всей системы ценностей во всемирном масштабе. В таких условиях информационная среда приобретает качественно новый смысл в том плане, что именно она должна помочь человечеству выжить в условиях воздействия глобальных опасностей – военных, экологических, демографических и других. В таком контексте есть прямой смысл говорить о новых парадигмах информатизации и информационной политики государства с позиций вызовов и опасностей XXI века, что, в свою очередь, предполагает подчинение вполне определенным императивам – реальностям объективного порядка, которые диктуют стратегическую линию развития информационной

сферы на всех уровнях ее организации – международном, региональном (межгосударственном) и национально-государственном.

В настоящее время крайне необходим такой реформационный сдвиг, который бы повлек за собой существенное обновление жизненного смысла людей, в значительной степени обесценившегося под воздействием индустриальной эпохи общественного развития. Эта эпоха, сыгравшая свою роль в развитии общественного, а в основном научно-технического и материального прогресса, отодвинула на второй план саму личность с ее культурными, ментальными, духовными и нравственными характеристиками и запросами. Индустриальный век втянул личность в орбиту рационального прагматизма, деформировавшего саму естественную природу личности, ее ценностные жизненные установки и качества, противопоставил личность обществу и государству, одну личность – другой личности и коллективу. Соответствующая индустриальной эпохе информационная среда оказалась не личностно-ориентированной, а производственно-ориентированной. Налицо разрыв с интересами и природой самой личности. Ориентировать информационную среду на самого человека – одна из основных задач российского государства в XXI веке.

Современные требования к информационной безопасности определяются не только противоречиями в информационной сфере, но и сложившимися реальностями как условиями современного бытия и существования людей. Эти реальности выступают непосредственными причинами вполне конкретного содержания информационной безопасности современных государств.

Возврат к личности, ее интересам и потребностям, достоинству и идеалам, благополучию и духовности – стратегическая линия современной политики государства в информационной сфере. Эта стратегическая линия лежит в основе формирования и формулирования императивов государственной информационной политики, реализует конкретные для российского государства задачи в информационной сфере на данном этапе его развития.

Автор полагает, что основными объективными требованиями информационной безопасности российского государства являются:

- защита институтов публичной власти от негативного информационного воздействия;

- формирование информационных потоков, направленных на обеспечение незыблемости конституционного строя, суверенитета и территориальной целостности России;
- блокирование манипуляций общественным сознанием;
- обеспечение открытости общества и информированности населения о деятельности институтов публичной власти;
- обеспечение благоприятных условий для реализации конституционных прав и свобод граждан в области получения и использования информации в целях их гармоничного развития.

Почему именно эти требования становятся во главу угла информационной безопасности российского государства? И почему именно государство обязано гарантировать реализацию названных требований информационной безопасности? Наконец, какими способами государство осуществляет их реализацию?

Источники возникновения объективных требований информационной безопасности российского государства находятся в тех условиях, которые породил минувший XX век и в которых формировалась информационная среда. К основным из этих условий можно отнести:

- истощенность и слабость информационных факторов социализации личности в условиях индустриального общества, необходимость органичного единства между рациональной стороной информационной деятельности государства и сохранением целостности личности, ее индивидуальной природы;
- необходимость преодоления посттоталитарных, переходных условий развития России, связанных с деформированностью внутренних и внешних информационных потоков в соответствии с интересами политического режима;
- низкий уровень информатизации, не позволяющий без внешней помощи и поддержки реализовать переход российского общества в информационную стадию развития;
- воздействие процессов информатизации и компьютеризации всех сфер общественной жизни, современной коммуникативной системы на деятельность институтов публичной власти (государства).

Определив основные источники требований, перейдем к характеристике состояния информационной безопасности российского государства, чтобы объективно осмыслить необходимые приоритеты. Исключительно важным является здесь ее правовое обеспечение.

Сразу следует отметить, что *формирование базы правового обеспечения информационной безопасности* приходится в основном на последнее десятилетие XX века. В этот период были приняты Закон Российской Федерации «О государственной тайне», Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», ряд других законов и, наконец, Доктрина информационной безопасности Российской Федерации. Но главное, разумеется, состояло в том, чтобы создать действенные механизмы их реализации и подготовить законопроекты, регламентирующие общественные отношения в информационной сфере. В этой работе, к сожалению, далеко не все соответствует потребностям общества и государства.

В свое время «Новая газета» опубликовала статью о лотерейном игорном бизнесе иностранных компаний в России и его «безобидном» влиянии на проблемы информационной безопасности¹. Речь в ней шла о корпорации «Джитек», являющейся мировым лидером в лотерейной отрасли. Ее лотерейные системы работают в 27 из 30 штатов США, проводящих лотерейные игры, и более чем в 30 странах мира. В настоящее время «Джитек» принадлежит около 70 % мирового рынка лотерей и тотализаторов, а ежегодный оборот корпорации составляет около 100 млн долларов.

Огромное геополитическое пространство России не могло не заинтересовать дельцов игорного бизнеса. Линий проникновения в интересующие страны «Джитек» выработала более чем достаточно. Например, через установление хороших контактов в высших эшелонах власти или посредством лоббирования нормативных актов высшей юридической силы о государственной монополии на данный вид бизнеса. Можно, наконец, попытаться перекрыть национальный бизнес в этой отрасли, навязав ему свои правила игры.

¹ См.: Зубова, Т. Лотерея как угроза национальной безопасности // Новая газета. – 2003. – № 7. – Февраль. – С. 4.

Здесь следует пояснить, что игорный бизнес приносит баснословные прибыли, поэтому не случайно до 90 % (!) прибыли от него облагается налогами. Помимо денег из кошельков наивных граждан такая компания может выуживать у государства бесценную, в том числе, и совершенно секретную информацию. Каким образом? Для реализации лотерейно-тотализаторского проекта такой территории, как Россия, «Джитек» потребуется осуществить «спутниковое» покрытие основной части территории Российской Федерации. Для проведения лотерей и тотализаторов будет использоваться диапазон частот двойного назначения, то есть тех самых частот, которые в случае чрезвычайной ситуации будут использоваться нашими военными, правоохранительными органами и МЧС. Нет необходимости пояснять, что при этом через спутники можно будет считывать всю информацию, передаваемую по специальным каналам. (Попытки проникновения на российский рынок корпорация предприняла еще в середине 90-х годов и продолжает их до настоящего времени.) Приведенный пример лишний раз подчеркивает актуальность установления ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности.

Другая важная сторона этой проблемы – реальная *правовая, организационная и техническая необеспеченность* закрепленных в Конституции Российской Федерации прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, сочетаемая с неудовлетворительной организацией защиты собираемых федеральными органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Эта опасность еще не осознана в российском обществе. Суть же ее состоит в неограниченной возможности влияния на человека. Новейшая информационная технология позволяет не только «подключиться» к каждому, но и «выключить» каждого из активного процесса социальной деятельности, личной жизни – любое обращение к средствам связи и средствам передачи информации фиксируется в памяти вычислительных машин, что позволяет просле-

доть за работой, коммерческими операциями, покупками и т. п. каждого человека. И это не гипотетические предположения, а уже существующая реальность. Так, в Швеции еще в конце 80-х – начале 90-х годов создан государственный банк данных «Фобальт», который содержит самые разнообразные данные о каждом гражданине, включающие демографические сведения, сведения о здоровье, месте жительства, профессии, образовании, партийности, политических убеждениях и т. д. Кроме того, банк содержит данные о работодателях, потребностях в рабочей силе, перемещении населения и др., что позволяет контролировать жизнедеятельность любого человека. Американская компания IBM еще в конце восьмидесятых годов XX века установила на своих предприятиях систему INTER-PERS, позволяющую любому предпринимателю или начальнику полностью контролировать каждого сотрудника, определять меру его профессиональной пригодности, техническую подготовленность, количество производимой продукции, простои, уровень заработной платы, отсутствие по болезни, наличие свободного времени, склонности, хобби и т. д. С помощью особых программ компьютеры могут сравнивать работников, подготавливать списки для увольнения или поощрения, следить практически за каждым шагом своих сотрудников. Преимущества предпринимателя здесь очевидны, но они заставляют каждого работника быть в постоянном напряжении, что делает производство в определенной степени антигуманным. Досуг, личная жизнь, мышление, поведение, настроения и иные человеческие проявления оказываются жестко и принудительно нормированными, а сам человек находится как бы под «стеклянным колпаком», сквозь который можно наблюдать всю его жизнь.

Исключительно важным в характеристике состояния информационной сферы является *отставание отечественной информационной инфраструктуры, информационных технологий* от западных. Как правопреемница СССР, Россия унаследовала от него достаточно обширную, но не менее отсталую информационную базу. Как известно, доступ к современной информации обеспечивается персональными компьютерами, интегрированными сетями связи и общедоступными базами данных и знаний. Напомним, что информационным является лишь то общество, которое гарантирует

наличными техническими средствами, возможностями и законодательными актами доступ любому своему гражданину к любой информации (кроме содержащей государственные и военные тайны, определенные законом). В США еще в 90-х гг. XX века практически каждая вторая семья имела персональный компьютер, а некоторые – несколько. В СССР они были практически недоступны для населения (прежде всего, по цене).

Процесс информатизации немислим без *медиатизации* – современной технологии связи. Компьютеры и базы данных, не подключенные в единую систему связи, подобны водопроводным кранам без водопровода. Информационно-компьютерная революция вообще невозможна без создания единой интегрированной системы связи, объединяющей все виды коммуникаций (радио, телефон, телевидение, видеовещание, телекс, телефакс, телеграф, спутниковую связь), а также все общедоступные ведомственные, вневедомственные, бытовые, научные, здравоохранительные и т. д. базы данных и знаний с подключением систем «электронной почты» и персональных компьютеров, находящихся в личном пользовании граждан, не говоря уже о персональных ЭВМ служебного пользования. В США, Японии и Западной Европе такие системы интегрированной связи уже созданы и находятся в состоянии перманентного развития и совершенствования. В России к ее созданию не приступали, в то время как отсутствие такой системы делает информатизацию и медиатизацию вообще невозможными.

Справедливости ради следует отметить, что отдельные передовые научные «площадки» от СССР нам все же достались. Приведем конкретный пример. Так, средства массовой информации (с соответствующей подачи идеологических работников) давно внушили населению страны, что против нас в «подвалах ЦРУ» куется психотропное оружие. Такие работы велись и у нас, только под колпаком «оборонщиков и комитетчиков». Группа ученых, в свое время «выплывшая» из чисто научного интереса на психодиагностику и психокоррекцию, которую возглавлял заведующий лабораторией психокоррекции ныне Московской медицинской академии И. Смирнов, достигла в этом научном направлении весьма значительных результатов. В то время как американцы в 1987 году только начали публиковать свои идеи по неосознанной психодиагностике, группа

Смирнова уже имела 17 изобретений в этой области, из них 4 – «пионерских», то есть не имеющих аналогов в мире. И способ семантической психокоррекции изобретен не в «подвалах ЦРУ», а в подвалах Московской медицинской академии (здесь следует понимать в буквальном смысле, поскольку уникальные научные исследования проводились в цоколе «дурдома» в трех помещениях размером четыре на полтора квадратных метра с битым кафелем на стенах и протекающими потолками)². А еще космонавтика, а еще ракетостроение и самолетостроение, а еще лучшие в мире образцы военной техники и оружия... Иными словами, было бы совершенно неверно считать, что у нас не происходили и не происходят сейчас какие-либо позитивные изменения в сфере развития и наращивания информационных технологий. Но общая ситуация в России выглядит примерно как подъем лифта в углубляющейся шахте: лифт поднимается вверх, но края шахты надстраиваются гораздо быстрее, так что расстояние между лифтом и краем шахты постоянно растет.

Безрадостное состояние информационной сферы жизнедеятельности общества настоятельно требует выделения основных приоритетов информационной безопасности российского государства как обязательных элементов, определяющих стратегию и тактику деятельности государства в данной сфере жизнедеятельности.

Под приоритетами информационной безопасности государства автор понимает первенство по времени в осуществлении мероприятий в информационной сфере, специально выделенных в качестве основных. Определение приоритетов в обеспечении информационной безопасности России основывается на выявлении соответствующих угроз в информационной этой сфере. Сегодня среди таковых руководство государства выделяет стремление со стороны ряда развитых стран к доминированию в мировом информационном пространстве, разработка ими концепции «информационных войн», предусматривающей создание средств опасного воздействия на информационные сферы других стран мира. Объектами таких воздействий могут быть как духовные средства общества, так и информационные ресурсы, автоматизированные системы управления и передачи данных. Противодействие этим угрозам должно осуществ-

² Подробнее см.: Наука управлять толпой? // Правда. – 1994. – 6 марта.

ляться комплексно: с одной стороны, государство обязано создать условия для развития отечественной индустрии современных информационных технологий, обеспечить возможность доведения до граждан полной и достоверной информации о тех или иных событиях, а с другой стороны, защитить общество от негативных информационно-психологических воздействий, обеспечить безопасность охраняемой законом информации и информационной инфраструктуры страны. Автор и не ставит перед собой непосильную задачу охарактеризовать всю совокупность угроз информационной безопасности российского государства; задача его более скромна – показать безусловное наличие и необходимость их блокирования.

Значительные негативные последствия для информационной безопасности могут иметь усиление экономической зависимости средств массовой информации от коммерческих структур и определенная асимметрия в сторону преобладания иностранной составляющей в информационной инфраструктуре российского общества. Речь идет о том, что отдельные граждане и общество в целом не получают в достаточном объеме необходимую им правдивую информацию о деятельности государственной власти, ее планах и намерениях. Данная информация доходит до людей в различной, иногда даже полярной трактовке. Разобраться в этой пестрой картине, отделить правду от вымысла бывает очень трудно.

Нельзя не сказать и о том, что существующее положение на информационном рынке России порождает угрозы, связанные с размыванием духовной базы российского общества, экспансией со стороны других стран в области культуры. Информационная безопасность предполагает защиту культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, введение запрета на использование эфирного времени в электронных СМИ для проката программ, пропагандирующих насилие, низменные человеческие проявления.

В настоящее время на территории России зарегистрированы 38 электронных и 66 печатных СМИ, созданных с привлечением иностранных инвестиций или в числе учредителей которых состоят иностранные юридические лица. 1157 иностранных изданий получили разрешение на распространение своей продукции в нашей стране. Но при этом необходимо, чтобы «правила игры» были оди-

наковы для отечественных и зарубежных СМИ. Почему, скажем, радио «Свобода» имеет право *неограниченного вещания* на территории России, а, к примеру, радиостанция «Маяк» не имеет аналогичных прав на территории США? Оказывается, законом о средствах связи США установлены строгие ограничения на выдачу лицензий на иностранное радиовещание на территории страны. Так, не разрешается выдавать или владеть лицензией на ведение вещания любой корпорации, где более одной пятой капитала принадлежит непосредственно либо через право распоряжаться им иностранным гражданам или их представителям³.

Существуют угрозы и в области индустрии информатизации, которые обусловлены, прежде всего, значительной деградацией отечественной электронной промышленности и недостаточно эффективной деятельностью государства по ее возрождению. Это приводит к консервации существующего положения, превращению России в экспортера сырьевых и интеллектуальных ресурсов, невозможности достойного участия в мировом разделении труда в одной из наиболее интенсивно развивающихся отраслей мировой экономики и торговли.

По мнению автора, наиболее важными и нерешенными до настоящего времени являются следующие проблемы:

1. Разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации.
2. Совершенствование нормативной правовой базы обеспечения информационной безопасности РФ, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации.
3. Установление ответственности должностных лиц федеральных органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности.
4. Разработка и создание механизмов формирования и реализации государственной информационной политики России.

³ См.: Емельянов, Г. В. Информационная безопасность: ключевые вопросы // Бизнес и безопасность в России. – 2000. – № 6. – С. 9.

5. Обеспечение технологической независимости в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, в первую очередь, в области создания специализированной вычислительной техники для образцов вооружения и военной техники.

б. Создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

Нормальной основой для реализации приоритетов информационной безопасности является устойчивое и бесконфликтное развитие государства, развитое гражданское общество, способное контролировать и корректировать государственные позиции в информационной сфере, гарантированная безопасность общества и личности. Поскольку устойчивое общественное развитие менее всего характерно для современной России, постольку в содержании информационной безопасности нет той степени единства, которая гарантирует соблюдение приоритетов.