УДК 316.324:004

СУДОРГИН О.А.

Информационные вызовы современной России: в поисках управленческой парадигмы

В статье рассматриваются понятие и социальная сущность информационного пространства общества. Анализируются особенности и трудности формирования информационного общества с точки зрения безопасности управленческой информации. Отмечено, что развитие информационной цивилизации сопровождается появлением новых вызовов, порожденных стремительным развитием киберпространства, возможностями информационного влияния и управления человеческим сознанием. Обозначена необходимость создания общей системы информационной безопасности.

Ключевые слова: информация, управление, информационное общество, информационное пространство, информационные вызовы и угрозы, информационная безопасность.

Опыт развития передовых стран мира показывает возрастающую роль информации, информационной сферы в общественной жизни. Стремительно развиваясь, она оказывает активное влияние на состояние политических, экономических, социальных, военных и других процессов. Бесспорен ее положительный результат, несущий людям возможность невиданного до селе обмена информацией; ускоряющий возможность быстрого и масштабного установления контактов; обеспечивающий социально-экономический прогресс и разрешение различных противоречий, проблем современности.

С середины двадцатого века западные страны в поиске новых укладов общественной жизни начали разрабатывать теоретические основы постиндустриального общества. Следует отметить, что еще в начале 70-х гг. выделилось его информационное направление. Такие ученые, как И. Масуда, Д. Белла, Э. Тоффлер, С. Нора, А. Минка, Э. Паркера, Дж. Нейсбита, Э. Брэнскома, Дж. Вакка и др., выдвинули ряд концепций информационного общества – общества, где главенствующую роль будет играть информация. Эти изыскания не остались только теоретическими, они нашли и находят свое воплощение в практике. Так, США, Япония, Франция, ФРГ, Великобритания и др. приступили к формированию информационного общества. Более того, с развитием Интернета стали говорить о становлении информационной цивилизации.

Россия, по вполне понятным причинам, из этого русла общественного прогресса «выпала». Неразвитость информационной инфраструктуры, отсутствие разработок новых образцов информационной техники, слабые производственные мощности в совокупности с отсутствием политической воли ограничили информационное развитие российского общества.

Несмотря на то, что в последнее время государством принят ряд важных документов по информационной проблематике, формирование информационного общества в России пока затруднительно. В этом смысле для нашего Отечества в качестве вызовов стали:

* проблемы формирования информационного общества;

* создание условий для сопряжения информационного пространства России с мировым информационным пространством. Речь идет о возможностях нашей страны к вступлению в мировое информационное сообщество (информационную цивилизацию).

Современный анализ социальных процессов в ведущих странах Европы и США убедительно показывает, что формирование нового вида социальной организации – информационного общества – является результатом развития информационных процессов и имеет информационную и

сетевую природу, основу которой составляют знание и свободное распространение связанной с ним информации через сетевую информационно-коммуникационную инфраструктуру.

Информация и знания, понимаемые не как субстанция, воплощенная в производственных процессах или средствах производства, а уже как непосредственная производительная сила, становятся важнейшим фактором современного хозяйства. При этом отрасли, производящие знания и информационные продукты, становятся первичным сектором экономики, «снабжающим наиболее существенным и важным ресурсом производства»[1].

Говоря о важности этого ресурса, специалисты имели в виду не столько качественную характеристику, то есть речь не шла об избытке или недостатке сырьевых ресурсов, труда или капитала. Имелось в виду нечто другое, а именно: информационные издержки, как ранее затраты труда или капитала, становятся основными и в чисто количественном аспекте. Так, в 1991 году в США впервые расходы на приобретение информации и информационных технологий, составившие на тот момент 112 млрд. долл., стали больше затрат на приобретение производственных технологий и основных фондов (не превысивших 107 млрд. долл.[2]).

Рост значения информации, например, в США оказался настолько стремителен, что уже к началу 1995 года в американской экономике «при помощи информации производилось около трех четвертей добавленной стоимости, создаваемой в промышленности»[3]. Именно развитие информационных технологий стало в значительной степени определять экономический потенциал государства в современных условиях и существенным образом влиять на его положение в мировом разделении труда и международной торговле. Очевидно, что в таких условиях перспектива формирования концепции «информационного общества» становилась объективно закономерной. Политическими элитами осознана приоритетность информационного развития как основного фактора, определяющего место страны в мировом сообществе.

В развитых странах Европейского союза, Японии, США, большинстве развивающихся стран (Индия, Бразилия, Россия и т.д.) разработаны и находятся на различной стадии реализации собственные стратегические программы информационного развития (электронный бизнес, электронное правительство и т. д.), основная цель которых – удержание/достижение лидерства в экономике и стабильное социальное развитие. Применяемые в этих программах сетевые технологии рассматриваются как единый комплекс, социально-технологическая база современной информационной среды, основа формирования информационного общества.

Отметим главенствующую роль государства в процессе становления информационного общества, в организации и координации совместных усилий государства, бизнеса, общественных институтов и граждан для достижения поставленной цели.

Развитие информационной цивилизации сопровождается появлением новых вызовов, порожденных стремительным развитием киберпространства, возможностями информационного влияния и управления человеческим сознанием. Эти вызовы присущи информационно развитым странам и, можно полагать, приобретают устойчивый характер.

Особую опасность представляют несанкционированные доступы к информационным сетям и системам, особенно военным. Дело в том, что современные средства вооруженной борьбы в подавляющем большинстве управляются с помощью информационных систем, в которых вырабатываются и передаются необходимые для эффективного использования вооружения, сведения и данные. Прецеденты несанкционированного проникновения в военные компьютерные системы имеются.

В последние годы проблема хакерства приобретает достаточно серьезное значение. Достаточно сказать, что она становится предметом изучения и исследования. Так, среди хакеров выделяют представителей «старой» и «новой» школ. К старой школе принадлежат люди, для которых интересны сам дух виртуальных приключений, жажда знаний и борьба за справедливость[4]. Считается, что хакеры старой школы почти не наносят никому вреда, они могут даже исправить систему, работающую плохо. К своим достоин-

ствам они добавляют преобразование компьютерной сети военного ведомства США – Арпанет в современный Интернет.

Иное дело – представители новой школы. Это люди, девизом которых стал лозунг: «Дайте мне инструмент, и я взломаю систему». Действия новичков куда менее предсказуемы и более разрушительны. Они взламывают системы, уничтожают программное обеспечение, охотятся за секретной информацией по чьим-либо заказам[5].

Вместе с тем привычным делом в общественной жизни становится информационная борьба, информационная разведка. Не случайно в поиск и добычу информации, обеспечивающей высокую степень осведомленности о социально-политических и экономических процессах в других странах, вкладываются огромные финансовые средства.

Таким образом, с одной стороны, угрозы информационного характера имеют достаточно разнообразные формы проявления, а с другой – способны наносить колоссальный урон. Эти вызовы могут спровоцировать информационный коллапс цивилизации[6].

Большую опасность представляют всевозможные схемные решения, выполненные на этапе проектирования и производства. Они оказывают существенное воздействие на компьютерные системы и строящиеся на их базе сети. Речь идет о несанкционированном проникновении в информационные компьютерные системы, базы данных, банки информации и т. д. с целью получения ценной информации, изменения (подмены) ее на фиктивную, внедрения «программ-вирусов», которые не только нарушают работу компьютеров, но и превращают их в распространителей этих вирусов; «логических бомб», представляющих собой вставки в программное обеспечение, срабатывающих при определенных условиях или по специальной команде и дезорганизующих работу информационных систем; «троянских коней», при помощи которых можно скрытно снимать информацию конкурента.

Новым вызовом становятся информационные операции и информационные войны[7]. Их особенностью является то, что информационным воздействиям подвергаются и сознание людей, и коммуникационные системы. Причем по последствиям эти действия сравнимы с крупномасштабной или ядерной войной, но с той лишь разницей, что они не оставляют разрушений материальных объектов.

Можно отметить, что для России новыми информационными вызовами являются:

· установление монополий на создание, получение и распространение информации, ущемление прав граждан в области информационной деятельности, а также слабая разработанность нормативно-правовой базы, регулирующей отношения в информационной сфере;

· применение информационного воздействия на массовое сознание и психику граждан с целью манипуляции, незаконного подчинения, а также дезинформирование, сокрытие или искажение информации;

· нарушения технологии обработки информации, разработка и распространение программ, нарушающих функционирование программных и аппаратных средств;

· уничтожение, повреждение и радиоэлектронное подавление средств и систем обработки информации, телекоммуникации и связи, а также перехват информации в технических системах и иных объектах;

· несанкционированный доступ к закрытым информационным системам (телекоммуникационным и связи), а также информационным ресурсам и их хищение;

· деятельность иностранных разведывательных служб (агентурным и техническим путем) и нарушение порядка подготовки конфиденциальных (служебных, секретных) сведений к открытому опубликованию[8].

Таким образом, следует сделать важный вывод о том, что новые информационные вызовы уже объективно существуют и не могут не учитываться в деятельности государств. Даже если государство полностью откажется от развития информационной сферы, это еще не говорит о том, что оно избавилось от негативных информационных влияний.

Одновременно мировой опыт свидетельствует не только о появлении нового комплекса угроз внутреннего и внешнего характера для отдельных государств, но и негативных тенденций глобального характера, что явилось следствием «взрывного» информационного развития при переходе к новому цивилизационному феномену – информационному обществу. В качестве одного из основных негативных критериев следует выделить так называемое «цифровое не-

равенство», т.е. возможности в доступе к информационным ресурсам стран и социальных групп существенно разнятся, что приводит к увеличению разрыва как между государствами, так и между богатыми и бедными. Технологически передовые страны завоевывают не только финансово-экономические рынки, но и активно вторгаются в информационное пространство менее развитых государств, создавая своими действиями новые источники нестабильности.

Направленная на социум информация не только дает представление о происходящих событиях, ориентирует человека в современном мире, но в целом оказывает сильнейшее воздействие на общество – его ментальность, морально-этические взгляды, самооценку, психологическое пространство и т.д. То есть определенная информация, поданная соответствующим образом, способна существенно корректировать формирование личности и цивилизации.

Развитие информационно-коммуникативной среды также является существенным фактором информатизации социально-политической сферы, где информационные технологии выступают как система информационных сред (властных структур, политических институтов, граждан), связанная с общественными процессами через информационные потоки. Возможности «сети» уже активно используются политическими акторами, осознавшими важность и необходимость развития новых политических практик, продуцируемых технологическими инновациями. Причем происходит количественное и качественное изменение самих субъектов политического процесса – акторами становятся физические лица, ранее не имевшие возможности оказывать влияние на сферу политики. Свободное распространение информации, в том числе политического характера, облегчает формирование надгосударственных и наднациональных политических организаций, деятельность которых может выходить за правовые рамки конкретных государств. В настоящее время можно с уверенностью говорить о появлении глобального политического рынка, где «учредителями» будут передовые в техническом и технологическом плане страны, активно использующие информационную составляющую в продвижении своих идей и защите своих национальных интересов. Существующие индивидуальные и комплексные системы и методы безопасности государств не успевают за быстро развивающимся мировым информационно-коммуникативным пространством. И в ближайшей перспективе единый информационный рынок потребует создания общей системы информационной безопасности. Россия должна занять самую активную позицию в данном вопросе, так как это отвечает и нашим национально-государственным интересам, и интересам мирового сообщества.

---

[1] См.: Drucker P.F. The Age of Discontinuiti. Guidelines to Our Changing Society. New Brunswick (US)-London, 1994. P. 264.

[2] См.: Stewart T.A. Intellectual Capital. The New Wealth of Organization. N.-Y.-L.: Doubleday/ Currency, 1997. P. 20–21.

[3] См.: Stewart T.A. Intellectual Capital. The New Wealth of Organization. N.-Y.-L.: Doubleday/ Currency, 1997. P. 14.

[4] Один из некриминальных хакеров Стивен Леви, написавший книгу «Хакеры: герои компьютерной революции», сформулировал принципы хакерской этики: доступ к компьютерам должен быть неограниченным и полным; вся информация должна быть бесплатной; не верь властям и борись за децентрализацию; ты можешь творить на компьютере искусство и красоту; компьютеры могут изменить твою жизнь к лучшему (См.: Мутасов Г. Романтики виртуальных сетей //Новый век. 2001. № 3. С. 33).

[5] См.: там же. С. 33.

[6] См.: Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. М.: СИНТЕГ, 1999. С. 41.

[7] Информационные операции, как правило, ведутся в период военных действий, в вооруженных конфликтах. Информационные войны все устойчивее приобретают самостоятельную форму войны. Их главная цель – достижение информационного превосходства. Информационные операции и информационные войны становятся предметами научных исследований, им уделено много внимания в научной и публицистической литературе. См., например: Почепцов Г.Г. Информационные войны. М.: «Рефл-бук», К.: «Ваклер», 2000; Мухин А.А. Информационная война в России. М.: «Гном и Д», 2000; Панарин И.Н. Информационная война и Россия. М.: Мир безопасности, 2000; Шаравов И. К вопросу об информационной войне и информационном оружии //Зарубежное военное обозрение. 2000. № 10 и др.

[8] См.: Концепция национальной безопасности /Указ Президента РФ от 10.01.2000.