
Э. М. БРАНДМАН

ГЛОБАЛИЗАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЩЕСТВА

Глобальная информатизация и новые информационные технологии открывают небывалые возможности во всех сферах человеческой деятельности, порождают новые проблемы, связанные с информационной безопасностью личности, общества и государства. Становится все более очевидным, что и общественный прогресс, и развитие каждого человека сопровождаются и даже в значительной степени определяются развитием их информационной сферы.

Это связано с тем, что в настоящее время информация становится одним из главных рычагов в противостоянии на международной арене за новый передел мира в целях установления господства ведущих государств в глобальном информационном пространстве. В научном мире информация вполне обоснованно считается *стратегическим национальным ресурсом*. Политический вес страны, ее возможности влиять на мировые события зависят не только от вещественно-силовых факторов, но во все возрастающей мере от факторов информационных (возможности эксплуатировать интеллектуальный потенциал других стран, распространять и внедрять свои духовные ценности, культуру, язык, а также тормозить духовно-культурную экспансию других народов, трансформировать и даже подрывать их духовно-нравственные устои). В соперничестве и противоборстве государств, в реализации их политических планов происходит явное смещение центра тяжести с открытых силовых методов и средств к скрытым и более «тонким» информационным методам и средствам, подаваемым как следствия процессов глобализации.

В этих условиях роль информационной безопасности все более возрастает. Информация и информационная инфраструктура для многих развитых стран уже стали критическими компонентами,

воздействие на которые способно вызвать крупномасштабные последствия, дезорганизовать государственное управление, вызвать новые конфликты. Чем выше уровни интеллектуализации и информатизации общества, тем более значимой становится его информационная безопасность, поскольку реализация интересов, целей государств и народов все больше осуществляется посредством информационных, а не вещественно-энергетических воздействий.

Что же представляет собой информационная безопасность как один из новых, но чрезвычайно важных видов общей безопасности?

Безопасность в буквальном смысле слова означает отсутствие опасности. Применительно к личности, обществу и государству это благоприятные (мирные) внешние и внутренние условия их развития. Что касается целей и назначения безопасности, то наиболее распространенным является взгляд на безопасность как на условие сохранения объекта и надежности его функционирования¹. С учетом этих предварительных замечаний перейдем к рассмотрению собственно понятия «информационная безопасность».

На сегодняшний день устоявшегося определения его еще нет. В наиболее общем плане под информационной безопасностью понимают такое состояние защищенности потребностей личности, общества и государства, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз². Иными словами, речь идет о систематизированной совокупности сведений об информационной безопасности и путях ее обеспечения.

Видимо, такой подход слишком общ и не позволяет разобраться в существенных аспектах информационной безопасности, поскольку различная степень зрелости социально-экономических, политических, социокультурных и иных отношений в каждом конкретном государстве характеризуется и различным состоянием информационной безопасности. Последняя же в решающей степени зависит от степени информированности (удовлетворения в какой-либо мере

¹ См.: Философский энциклопедический словарь. – М.: ИНФРА-М, 1998. – С. 36.

² См.: Общая теория национальной безопасности / под общ. ред. А. А. Прохожева. – М.: РАГС, 2002. – 320 с.; Панарин, И., Панарина, Л. Информационная война и мир. – М.: ОЛМА-ПРЕСС, 2003. – 384 с.; Швец, Д. Ю. Информационная безопасность России и современные международные отношения. – М.: Мир безопасности, 2001. – 176 с.

потребностей в информации как отдельной личности, так и государства и всего общества) субъектов политико-экономической жизни, определяющей степень адекватности восприятия ими окружающей действительности и, как следствие, обоснованность принимаемых решений и действий. С этой точки зрения информационная безопасность, например, США не может быть тождественной информационной безопасности России, поскольку структурные составляющие их будут разными.

На наш взгляд, под информационной безопасностью следует понимать способность государства защитить все сферы общественной жизни, сознание и психику граждан от негативного информационного воздействия, обеспечить субъекты политического и военного руководства данными для успешной модернизации общества и армии, не допустить утечки закрытой, общественно ценной информации и сохранить постоянную готовность к информационному противоборству внутри страны и на мировой арене, способствовать достижению социальной стабильности и согласия в обществе.

Каковы источники современных информационных угроз личности, обществу и государству? Раскрывая их, следует учитывать следующее.

1. *Информация – не только мощный двигатель общественного прогресса, фактор многократного усиления совокупного потенциала государства, но и действенный инструмент манипулирования общественным сознанием.* Речь идет о том, что не только сами государства, но и отдельные социально-политические силы внутри них, используя монополию на средства массовой информации, не зная государственных границ и многих ограничений по расстоянию, способны формировать у широких масс определенные идеологические установки, оценки, настроения, ценностные ориентиры поведения. С другой стороны, от развития информации в наше время в значительной степени зависят и другие слагаемые безопасности. Во многих странах для обеспечения информационной безопасности созданы специальные службы, которым выделяются значительные финансовые средства, развернута подготовка соответствующих специалистов. Так, в США и ряде других государств образованы специальные органы для нейтрализации послед-

ствий информационных воздействий. Вашингтон только на разработку методов и средств информационной безопасности ежегодно расходует около 5 млрд долларов.

2. Глубокую озабоченность у многих развитых стран вызывает *информационное вторжение США в мировые информационные ресурсы*. В «мировой паутине» Интернета уже сегодня находятся более 150 млн пользователей, число которых растет по экспоненте, и по прогнозам к 2010 г. их численность превысит 1 млрд человек. Таким образом, подавляющая часть мирового информационного ресурса становится частью Интернета. Соответственно через эту мировую информационную супермагистраль возможны негативные вторжения в информационные ресурсы других стран.

3. Достижения в области информатизации постоянно совершенствуются. Сегодня уже создано так называемое «информационное оружие», под которым понимаются устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона путем опасных информационных воздействий. Существует два типа такого оружия – информационно-техническое и информационно-психологическое. При использовании оружия первого типа (компьютерные вирусы, логические бомбы, программные закладки и т. п.) главными объектами воздействия являются информационно-технические системы (системы связи, телекоммуникационные системы, банки и т. д.). Примеров разрушения информационных ресурсов и телекоммуникаций, несанкционированного доступа к ним, попыток хищения конфиденциальной информации или ее уничтожения в хорошо защищенных компьютерах – множество. С полным основанием можно говорить, что сегодня террористы и шпионы, мафия и хакеры полностью освоились в глобальных компьютерных сетях, шантаж и угрозы информационных диверсий стали привычным делом.

При воздействии информационно-психологического оружия главными объектами являются индивидуальная психика и общественное сознание. Цель такого воздействия – подрыв духовного, морально-психологического потенциала страны-конкурента и подготовка почвы для политико-экономического проникновения. Разрушительные последствия применения этого оружия, подкрепленного всей мощью современных средств массовой информации, ста-

ли очевидны в период «холодной войны» и краха тоталитарных систем в Восточной Европе и СССР.

4. Обострение конфликтов между субъектами международных отношений в регионах, находящихся вблизи границ сопредельных государств, сочетающееся с политической дезинформацией населения. В этом отношении характерны попытки Запада проводить политику «ползучей» информационной экспансии на всем постсоветском пространстве. Под идеологической ширмой религиозной свободы спецслужбами США, Пакистана и других стран проводится стратегическая установка на проникновение вглубь территории Содружества независимых государств с использованием тюркского и исламского факторов. Главная цель Запада и, в первую очередь, США состоит в установлении контроля над нефтяными ресурсами Каспийского моря и создании «санитарного кордона», призванного изолировать Россию как прикаспийское государство от стран Европы, Ближнего и Среднего Востока.

5. На протяжении длительного времени считалось, что для обеспечения прогрессивного развития страны достаточно гарантировать предотвращение или локализацию угроз извне, вследствие чего проблемы безопасности государства и общества рассматривались в жестких рамках идеологических и политических установок. Поэтому традиционно проблема информационной безопасности у нас сводилась к соблюдению режима секретности и ограничивалась сферой защиты секретов и обеспечению безопасности информационных потоков. Зачастую неоправданная секретность наносила серьезный ущерб экономическим, политическим и даже военным интересам страны. По этой же причине и сегодня в значительной степени остаются не вовлеченными в экономический оборот накопленные, например, в оборонном секторе информационные ресурсы. При сохраняющейся архаичной системе у нас потерян реальный контроль за распространением опасных технологий (на что уже указывают не только отечественные специалисты, но и эксперты ООН).

6. Внутренние информационные угрозы. Нет необходимости говорить о том, что западные государства не заинтересованы в стабилизации положения в странах с переходной экономикой. При проведении своей линии, например, в России они опираются на

компрадорский бизнес, укрепившийся в ряде российских банковских структур и экспортно ориентированных сырьевых отраслей. Основная цель – не допустить внутренних накоплений, которые могут составить основу «бюджета развития», пойти на модернизацию обрабатывающей промышленности и сельского хозяйства, конверсию и спасение высоких технологий военно-промышленного комплекса. Поэтому все крупные операции по перекачке ресурсов и средств за пределы России осуществляются при участии иностранных структур. Нельзя не учитывать и того факта, что западные фирмы имеют практически неограниченный доступ к бухгалтерии российских экспортеров, прекрасно информированы относительно движения товарных и финансовых потоков, владеют данными о банковских счетах, сделках с недвижимостью и ценными бумагами. Они имеют на руках криминальный компромат на многих российских участников внешнеэкономической деятельности и связанных с ними политиков и чиновников. В итоге эти представители деловой и политической элиты крайне не самостоятельны, уязвимы, подвержены давлению обладателей компромата и не в состоянии проводить политику в интересах России.

Изменение политической обстановки в России, экономические преобразования, ориентированные на переход к рыночным отношениям, заставляют переосмыслить подходы к обеспечению информационной безопасности в военной сфере. В новых условиях, когда монополизм государства в области информации разрушен, оказались нерешенными многие проблемы охраны и защиты конфиденциальной информации, интеллектуальной собственности, коммерческой тайны (это, так сказать, вторая крайность), без чего невозможно эффективное управление, предотвращение негативного внешнего воздействия, решение всего комплекса проблем информационной безопасности.

Что принципиально важно учитывать сегодня при разработке адекватных мер информационной безопасности России? Каковы основные направления информационного обеспечения безопасности личности, общества и российского государства в условиях глобализации?

1. Прежде всего, необходимо изначально определить, что в деле информационной безопасности (как в никакой другой области) ме-

нее всего нужно ориентироваться на партнерские отношения передовых индустриально развитых государств, уже вошедших в стадию информационных обществ. В каждом конкретном случае у администрации этих государств имеется своя иерархия приоритетов, связанных с собственной концепцией национальных интересов, в соответствии с которой выбираются и тактические приемы «партнерских» отношений. Не случайно в период развала СССР наличие общих целевых установок и определенного выбора способов их реализации заставило США и их западноевропейских союзников по НАТО вычлнить «конфликтную политику» как самостоятельное направление внешнеполитического курса по отношению к СССР.

В этих условиях можно спрогнозировать, что высокий уровень теоретической и практической разработки вопросов, связанных с поисками оптимальных моделей поведения политического руководства России в условиях кризисных и конфликтных ситуаций, должен позволить создать новые прикладные концепции уже в ближайшее время. Иными словами, на повестку дня с особой остротой встает вопрос не столько об информационном партнерстве с США, западноевропейскими и даже восточноевропейскими странами, сколько об информационной защите от такого партнерства.

2. Крайне необходимо выявить дестабилизирующие факторы информационной безопасности. Источниками дестабилизирующих факторов в различных ситуациях могут быть как отдельные личности, так и организации, объединения. Но наиболее сильными из них являются скрыто или открыто враждебные государства или коалиции – в них для формирования информационных угроз создаются и функционируют специальные органы и службы. Особую группу составляют современные информационные системы и средства, поскольку они одновременно являются орудием приведения в действие информационных угроз, каналом проникновения их в сознание личности или общественное сознание и генератором спонтанных угроз, возникающих вследствие технических неисправностей и других причин. Именно последнее обстоятельство позволяет рассматривать их в качестве самостоятельного источника дестабилизирующих факторов.

Разумеется, каждому источнику свойственны определенные виды дестабилизирующих факторов. В межгосударственных отношениях это, как правило, конфликты различных масштабов и сфер проявления (экономика, политика, идеология, дипломатия и т. д.). К основным видам наиболее важных для нас внутригосударственных дестабилизирующих факторов следует отнести:

а) правовой вакуум в большинстве вопросов обеспечения информационной безопасности;

б) преднамеренное или непреднамеренное нарушение имеющегося законодательства по вопросам информационной безопасности;

в) политические и военные конфликты различного масштаба;

г) злоумышленные действия преступных элементов и групп в отношении информационных источников;

д) отказы, сбои, технические ошибки информационных систем или средств;

е) природные явления и процессы, затрудняющие получение, передачу, прием и хранение информации или разрушающие информационные системы и т. д.

Эта совокупность источников вместе с присущими им видами дестабилизирующих факторов формирует целый спектр информационных угроз, воздействующих на состояние информированности политического руководства страны. К ним относятся: похищение, уничтожение, потеря, сокрытие, разглашение, фальсификация, компрометация полезной (истинной) информации, а также фабрикация, распространение и внедрение заведомо ложной информации (дезинформация). В результате снижается информированность субъектов государственного управления, у них создается искаженное представление о протекающих в обществе и мире социальных процессах.

Публикуемая в настоящее время информация зарубежных исследовательских организаций отличается от прежних документов более высоким уровнем обобщения и аналитичности, достижение которого возможно только при наличии обширной базы фактологических и социологических данных. Эта особенность позволяет сделать вывод, что, помимо собственных возможностей и отработанных методик социально-экономических и политических процессов, в подготовке докладов все чаще используются экспертные и

аналитические работы «местных» – отечественных – исследователей. Осуществляется переход от самостоятельной аналитической обработки первичных материалов (взглядов отдельных политиков, программных документов партий, общественных движений и т. п.) к исследованию аналитико-синтетических документов и материалов альтернативных исследовательских структур. То есть можно говорить о формировании качественно нового по своим параметрам информационного канала для зарубежных политических исследовательских организаций: у них циркулирует информация, подготовленная квалифицированными специалистами России, хорошо знающими социально-политическую и экономическую ситуацию в стране. В условиях отсутствия общественных регуляторов использования такой информации неконтролируемость и юридическая неопределенность функционирования последней может нанести значительный ущерб безопасности в самых различных областях.

Качество информации и, естественно, ее ценность для политических кругов Запада (куда в конечном итоге она попадает) определяется следующими факторами:

1) профессиональной специализацией новых информационных структур, в которых по каждому направлению информационной деятельности задействованы ведущие специалисты-аналитики по данному кругу проблем;

2) переходом от принципа информационной избыточности к принципу информационной достаточности, который реализуется с помощью поисковых экспертных систем и позволяет фиксировать лишь значимую для данного круга вопросов информацию, многократно снижать так называемые «информационные помехи»;

3) задействованием региональных респондентских сетей, которые позволяют оперативно проводить необходимые социологические опросы и исследования, постепенным переходом к формированию региональных и межрегиональных систем социально-политического и военного мониторинга;

4) созданием специализированных прогностических экспертных систем, позволяющих осуществлять веерное альтернативное моделирование поведения «политического субъекта» и давать количественные оценки вероятности действий;

5) активным использованием компьютерных систем анализа и обработки информации на новейшей машинной базе.

В общем итоге в отличие от традиционных информационных источников (анализа печатных изданий, опроса граждан и т. п.) уровень и качество нового информационного канала может оказать решающее воздействие на выработку активной политики западных государств в отношении России.

3. Изменение социально-экономического и политического развития России обуславливает необходимость постоянного совершенствования системы защиты информации. Наличие нерешенных вопросов обеспечения безопасности информации в условиях закономерного роста открытости общества создает предпосылки несанкционированного доступа к информационным ресурсам. Поскольку Россия становится все более активным субъектом мировой политики и экономики, это влечет за собой необходимость обеспечения безопасности значительных объемов конфиденциальных сведений. Переход развитых стран мира в информационную стадию развития с такими неизбежными последствиями, как информационные преступления, информационный терроризм и даже возможность проведения информационных войн, ставит на повестку дня вопрос о возрастающем значении проблем защиты информации каждого государства. Для России здесь основная задача состоит в том, чтобы обеспечить такой уровень безопасности информации, который гарантировал бы сохранение и упрочение российской демократической государственности, политической и социальной стабильности общества, защиту прав и свобод граждан в информационной сфере, равноправное вхождение страны в мировое информационное пространство, в том числе при включении ее информационных ресурсов в глобальные информационно-телекоммуникационные сети.

4. В современных условиях для России исключительно важным является формирование негативного глобального общественного мнения о недружественных приготовлениях, открытых и тайных (специальных) акциях США и НАТО. Здесь нет необходимости заниматься фальсификацией или искажением фактов действительности: объективно внешняя политика США и НАТО направлена на реализацию национальных интересов США в мире и достижение

глобальных интересов НАТО на международной арене, установление одного центра силы (экономической, политической, военной) в общей системе международных отношений. В то же время здесь есть насущная необходимость вести данную работу систематически, а не эпизодически (в период кризисных ситуаций, связанных с провокациями, военными конфликтами, локальными войнами и т. п.), с привлечением всех политических средств, особый упор делая на дипломатию и средства массовой информации и коммуникации. Отдельные попытки такой работы были проявлены руководством МИД РФ в период югославского кризиса, когда особая позиция России в вопросе использования военной силы НАТО против боснийских сербов реально раскрыла несоответствие между «миротворческими» устремлениями США и их союзников и их действиями против мирного населения Боснии.

5. Политическая борьба не терпит сослагательного наклонения: используя компромиссы, она остается бескомпромиссной по своей сути. Сегодня в ней трудно переоценить роль информационного противоборства, направленного на разобщение усилий как отдельных государств, так и их коалиций. Для этого необходимо грамотно и умело использовать противоречия как внутри отдельных государств, так и их коалиций. К примеру, единое атлантическое пространство, сформированное под эгидой США, выполняет важные оборонно-стратегические функции, но цена гарантий для европейских государств при этом достаточно велика: континентальной Европе угрожает растворение в англо-американской системе с утратой национального многообразия и самобытности западноевропейских государств, поскольку американизация Европы – это не только геополитическая зависимость, но и культурный униформизм, растворение в обезличенной духовной индустрии, скроенной по меркам примитивного массового общества. Двуосность Европы (континентальная – океаническая, романская – германская, католическая – протестантская) уже имеет тенденцию превратиться в американизированную одномерность.

Таким образом, можно с известной долей вероятности предположить, что информационная безопасность личности, общества и государства в условиях глобализации выдвигается в число приоритетных проблем современности.