УДК 004.056:32

ПОЛИТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Россошанский

Саратовский государственный университет,
кафедра политических наук

В статье рассмотрены основные факторы, актуализирующие проблему информационной безопасности в контексте национальной безопасности современной России. Акцент сделан на политической составляющей информационно-коммуникационных процессов и их особенностях. Проанализированы потенциальные последствия увеличения технологических возможностей средств массовой коммуникации, обоснована необходимость создания политико-правовых механизмов их ограничения.

Political Aspects of Information Safety

A.V. Rossoshansky

The paper considers major factors making the problem of information safety urgent in the context of national safety of the modern Russian Federation. The political component of information and communication processes and their features are stressed. Potential consequences of the increase of technological opportunities of the mass media are analyzed, the necessity to design political and legal mechanisms for their restriction is proved.

Одним из стратегических направлений развития государственности в современной России является обеспечение ее безопасности на уровне, адекватно отвечающем современным реалиям глобализирующегося мирового сообщества. Обеспечение безопасности является многоаспектной проблемой, касающейся политической, экономической, культурной, военной сферы и т.д. Важное место среди них занимает информационная безопасность.

Эффективность реализации выделенных направлений безопасности зависит от состояния политической системы, от направленности, быстродействия и согласованности работы ее внутренних механизмов. В свою очередь, ключевые характеристики политической системы, например, такие как стабильность функционирования и развития, зависят от эффективности самих систем безопасности, где одну из главных ролей, в условиях всевозрастающей роли информации и средств ее распространения, играет обеспечение информационной безопасности. Зарождающееся «информациональное общество» строится таким образом, что именно сбор, анализ и передача необходимой информации становятся «фундаментальными источниками производительности и власти»[1]. Не случайно, по мнению большинства исследователей, именно информационно-коммуникационные факторы сыграли одну из ключевых ролей в разрушении социалистической системы и в революционных преобразованиях в странах Восточной Европы[2].

Происходит стремительное увеличение информационных ресурсов, производимых человечеством. Оно сопровождается включением значительного числа трудоспособного населения в сферу интеллектуального труда, развитием интеллектуальной собственности, появлением новых информационных технологий. Осуществляется трансформация традиционных институтов демократической государственности. Это приводит к тому, что имеют место две противоречивые тенденции «одновременное развитие чрезвычайной социальной зависимости и акцентированной индивидуализации»[3]. Обусловлено это тем, что следствием достижений в области информации и информатизации человечества происходит феноменальное увеличение темпов прироста объема его суммарных знаний. Так, в 70-е гг. XX в. этот объем увеличивался вдвое один раз в 10 лет. В 80-е гг. — один раз в пять лет. С конца 90-х гг. объем знаний человечества удваивается практически каждый год[4].

Одновременно с открытостью как основной тенденцией развития информационного общества и прогрессом информационных технологий, актуализируется и проблема защиты информации. Важным источником угроз интересам человека является использование во вред его интересам персональных данных, накапливаемых различными структурами, в том числе органами государственной власти, а также расширение возможности скрытого сбора информации, составляющей его личную и семейную тайну, сведений о его частной жизни.

Это происходит в силу того, что информация является стратегическим национальным ресурсом, одним из основных богатств государства, претендующего на достойное

место в международном сообществе. Сегодня экономический, оборонный и политический потенциал страны в значительной мере определяется уровнем развития ее информационной инфраструктуры, но при этом пропорционально возрастает и уязвимость национальных информационных ресурсов по отношению к негативным воздействиям. Вышесказанное в полной мере относится и к России, так как ее стремительная информатизация, вызванная проходящими политическими и экономическими процессами, ведет к тому, что благополучие страны все в большей степени зависит от безопасности ее информационных ресурсов[5].

Сегодня одной из основных тенденций развития современного общества является его информатизация, что автоматически выдвигает вопросы рассмотрения информационной безопасности на передний план. Поэтому совокупность функций СМИ в современных условиях обязательно должна включать информационную безопасность[6]. Стремительное развитие и широкое использование информационно-коммуникационных технологий (ИКТ) ознаменовали собой переход человечества на абсолютно новую ступень развития, явившись результатом революции в сфере информатизации. ИКТ трансформировали не только принципы и формы сбора, обработки и передачи информации, они начали оказывать мощнейшее воздействие на политический, культурный, экономический и военно-стратегический аспекты жизни общества, становясь одним из основных факторов обеспечения и поддержания устойчивого развития. С определенной точки зрения мир «...представляет собой не что иное, как движущуюся во времени информацию, даже если речь идет о вполне неподвижных на первый взгляд предметах»[7]. По образному выражению другого исследователя информация представляет собой «нейроны», воздействующие на жизненные центры общества, или «кровяные шарики», она создает «систему кровоснабжения» для любых движений, поступков, поведения, отношения людей и ассоциаций»[8].

Демократизация политической системы и внедрение института конкурентных выборов в постсоветской России показали особую значимость ИКТ в политических и особенно избирательных кампаниях[9]. Информатизация выступает как новый этап в развитии производственных сил, при котором обмен информации, ее оперативная обработка и эффективное применение являются определяющими условиями всестороннего развития общества[10].

Этот процесс обусловлен действием двух факторов: увеличением объема информации, необходимой для обеспечения систем жизнедеятельности общества и совершенствованием технологии накопления и распространения информации. В результате происходит разрастание информационной сферы, которая становится не просто локальным сегментом общественной жизни общества, а материей, пронизывающей все социально-политическое пространство от состояния которой зависит личная жизнь человека, характер общественных отношений, положение государства на международной арене.

К основным эффектам коммуникационных процессов Е.В. Бушуева, например, относит: «индивидуальный ответ, отклик»; «кампания в средствах массовой коммуникации»; «эффект индивидуальной реакции»; «коллективная реакция»; «распространение инноваций»; «распределение информации (событийного порядка); «социализация»; «социальный контроль»; «представление социальной реальности»; «институциональные изменения»; «влияние на результаты событий»; «культурные изменения»[11]. Многообразие данных эффектов, на наш взгляд, свидетельствует не только о возрастании значимости информационно-коммуникационных процессов в жизни любого общества, в совершенствовании всех сфер его развития, но и об увеличении потенциальных и уже существующих проблем в этой области.

Обусловлено это тем, что воздействие СМИ носит крайне противоречивый характер. Например, по мнению некоторых исследователей, телевидение и интернет «протезирует» несостоявшиеся формы гражданского участия и социальной солидарности «(клубы по интересам, ассоциации и союзы разного рода, формы самоорганизации потребительского или досугового поведения, наконец, реальные политические партии), создавая целые сферы чисто визуальной чужой жизни, виртуально-телевизионной реальности»[12]. Очевидно, что возможные последствия такой виртуализации представляют собой угрозу не только для нравственного здоровья общества, его адекватной саморефлексии возни-

кающих социальных проблем, внутренних и внешних угроз, но в конечном итоге и для национальной безопасности страны. Поэтому нельзя не согласиться с Ю.В. Родионовой в том, что необходимо выделять и учитывать информационно-идеологический аспект безопасности[13].

Анализируя эффективность функций современных российских СМИ, известный журналист В. Третьяков констатирует, что они пока слабо реализуются в контексте общенациональных интересов, с точки зрения интегрирования общества и повышения уровня его культуры[14]. Поэтому нельзя не согласиться с К.В. Ветровым в том, что для осуществления комплекса мер «концептуального и практико-политического плана, минимизирующих проявления негативных тенденций в средствах массовой информации, нужно все-таки, чтобы сами СМИ глубоко осознали необходимость перемен»[15].

В результате, развитие новой информационной структуры, которая включает не только Интернет, но также и спутниковое теле- и радиовещание, сотовую связь, то есть интерактивные средства массовой информации, воздействует на экономику, социальную структуру, государство, право и требует особого внимания к проблеме региональной, государственной и международной информационной безопасности. Такое состояние информационной сферы, детерминирующее формирование информационного общества задает условия, при которых информационная безопасность становится одним из элементов национальной безопасности.

В социально-политическом контексте объектом информационной безопасности могут быть государство, регион, общество, отдельный индивид. Однако вне зависимости от объекта, его безопасность характеризуется безопасностью его свойств и функций, структурных составляющих[17]. На наш взгляд, взаимосвязь систем национальной и информационной безопасности в полной мере представлена в доктрине информационной безопасности Российской Федерации. Согласно ей, под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества[18].

В Доктрине выделяются четыре вида угроз информационной безопасности Российской Федерации.

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

2. Угрозы информационному обеспечению государственной политики Российской Федерации.

3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных и информационных ресурсов.

4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Как видно, все угрозы информационной безопасности РФ составляют, по сути, две группы[19]:

Первая группа (к ней относятся угрозы первого и второго вида) – угрозы, обусловленные негативными явлениями, процессами и действиями в сфере власти и гражданского общества, в сфере деятельности государственных структур разных уровней, средств массовой информации, правоохранительных органов. Появление этих угроз связано прежде всего с неадекватными формами взаимодействия государства и общества, власти и гражданина, личности и права.

В конкретизированной формулировке к угрозам данной группы относятся, например, следующие:

- принятие властными органами разных уровней нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям принятых в российском обществе;
- манипулирование информацией (дезинформация, сокрытие или искажение информации)
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики и т.д.

Вторая группа угроз информационной безопасности (к ней в Доктрине отнесены угрозы третьего и четвертого видов) – это угрозы, которые обусловлены негативными явлениями и противозаконными действиями в рамках существующих информационных и телекоммуникационных систем, систем связи, а также на рынке информационных технологий.

Эти угрозы существенным образом отличаются от угроз, относящихся к первой группе, прежде всего тем, что в их формировании и реализации доминируют не правовые, духовно-идеологические и социально-психологические аспекты, а технические и организационно-технологические.

К этой группе угроз относятся:

– противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

– противоправные сбор и использование информации; нарушения технологии обработки информации;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– несанкционированный доступ к информации, находящейся в банках и базах данных; нарушение законных ограничений на распространение информации.

Такое подразделение угроз информационной безопасности подчеркивает дуальную природу самой информационной безопасности. Дело в том, что информационная безопасность является междисциплинарной отраслью научного знания.

С одной стороны, система информационной безопасности – это комплекс организационно-технических мероприятий и программно-аппаратных средств, обеспечивающих надежное хранения информации и безопасную передачу данных, то есть иными словами защиту информации. Для этого необходима продуманная политика безопасности, в которой отражаются не только технические аспекты ее реализации, но и четко определены уровни доступа участников к той или иной информации, их ответственность за те или иные действия, выходящие за разрешенные рамки. В содержание такой политики безопасности входит внедрение централизованного контроля и управления сетью по которой передается информация, что позволяет

получать исчерпывающую информацию о попытках несанкционированного доступа к той или иной информации, а также программные средства - антивирусные системы, шифрующие пакеты, системы обнаружения «уязвимостей», вторжений, активного аудита, фильтрации контента и т.д.[20]

С другой стороны, информационная безопасность имеет социально-политическое и правовое наполнение, которое, в свою очередь, подразделяется на ряд аспектов.

В ряде работ информационная безопасность рассматриваться, как состояние социума, при котором обеспечена надежная и всесторонняя защита личности, общества и государства от воздействия на них особого вида угроз, выступающих в форме организованных либо стихийно возникающих информационных потоков, осуществляемых в интересах регрессивных, реакционных или экстремистски настроенных политических и социальных сил и направленных на осознанную деформацию общественного и индивидуального сознания, следствием чего выступает девиантное поведение личности, усиление социально-политических, экономических и духовных коллизий, нарастает, развивается и закрепляется психологическая и психическая напряженность социума. В этом случае при операционализации понятия информационная безопасность неявно использовалась категория «состояние защиты», без конкретизации свойств объекта, которым она необходима и источников этой защиты.

На наш взгляд, ограниченность такого подхода в том, что информационная безопасность сводится к одной лишь защите от негативной информации. Причем в качестве источников таких угроз указываются только регрессивные, реакционные или экстремистски настроенные политические и социальные силы. Однако информационная безопасность включает также в себя гарантии доступа к информации, использование информационных ресурсов, противостояние культурной экспансии со стороны других стран, сохранение национальной и языковой самобытности и многое другое. Кроме того, это понятие включает защиту от манипулирования информацией, которая может осуществляться с помощью СМИ. Субъектами такого манипулирования являться различные политические силы, а объектом личность и общество в целом. Сильное влияние подобные манипуляции имеют в период избирательных компаний, смысл которых заключаться в одностороннем освещении событий, в умолчании или даже искажении различных фактов.

Понятие информационной безопасности отражает не только статическое состояние социума, но и его динамику, то есть взаимодействия между обществом и государством, наличие и активность структур гражданского общества. Исходя из этого, информационная безопасность представляет собой такое состояние институтов государства и общества, при котором обеспечивается надежная защита национальных интересов страны и ее населения в информационной сфере. В данном определении подчеркивается основная предпосылка защиты национальных интересов – необходимое состояние государственных институтов и гражданского общества. Именно на государство и общественные структуры возлагается обязанность обеспечения информационной безопасности. Кроме этого, указывается, что национальные интересы являются центральной характеристикой, связывающей между собой индивида, общество, государство.

Примечания

1. *Кастельс М.* Информационная эпоха: экономика, общество и культура. М., 2000. С. 42–43, 48.
2. См., напр.: *Гуторов В.А.* Массовые коммуникации и власть в эпоху трансформации коммунистических режимов в странах центральной и Восточной Европы // Власть, государство и элиты в современном обществе: Сб. науч. тр. / Под ред. А.В. Дуки и В.П. Мохова. Пермь, 2005. С.74–101.
3. *Луман Н.* Медиакоммуникации. М., 2005. С.9.
4. *Поляков Ю.А.* Информационная безопасность и средства массовой информации. М., 2004. С.76.
5. *Шерстюк В.П.* Проблемы обеспечения информационной безопасности в современном мире // Математика и безопасность информационных технологий. М., 2004.
6. См.: *Прошина М.Г.* СМИ как институт гражданского общества в России. Саратов, 2007. С.31.
7. *Бритков В.Б., Дубровский С.В.* Информационные технологии в национальном и мировом развитии // Общественные науки и современность. 2000. №1. С.9.
8. Право и информатизация общества. М., 2002. С.11.
9. См.: *Грачев М.Н.* Политика, политическая система, политическая коммуникация. М., 1999. С.134–136; Политические коммуникации XXI века: Материалы Всерос. науч.-практ. конф. Казань, 27–28 февраля 2006 г. Казань, 2006; *Березин Б.М.* Сущность и реальность массовой коммуникации. М., 2002.
10. *Белов В.Г.* Парадигма информационного общества и становление информационного права // Право и информатизация общества. М., 2002. С.36.

[11] *Бущуева Е.В.* Современные подходы к исследованию эффектов массовой коммуникации // Правовая политика и правовая жизнь. 2007. №2. С.91–92.

[12] *Дубин Б.* От инициативных групп к анонимным медиа: массовые коммуникации в российском обществе // Pro et contra. 2000. Т.5, №4. С.41.

[13] *Родионова Ю.В.* СМИ и информационная политика регионов России // Политический консалтинг: горизонты новой реальности: Материалы Всерос. науч.-практ. конф. Казань, 24 февр. 2004 г. Казань, 2004. С.83.

[14] См.: *Третьяков В.* Играющая журналистика // Лит. газ. 2004. №14.

[15] *Ветров К.В.* Средства массовой информации в постсоветской России: Особый путь вдоль проторенной дороги. М., 2004. С.74.

[16] *Стрельцов А.А.* Обеспечение информационной безопасности России: теоретические и методологические основы. М., 2002. С.46.

[17] Доктрина информационной безопасности Российской Федерации // Рос. газ. 2000. 28 сент.

[18] См.: *Садовничий В.А.* Информационная безопасность: новые угрозы мировому сообществу // Глобальная информатизация и безопасность России. М., 2001. С.6.

[19] См.: *Рубанов В.А.* Согласование задач управления и обеспечения безопасности при информатизации мегаполиса // Информационная безопасность России в условиях глобального информационного общества: Материалы Всерос. конф. Москва, 27–28 янв. 2004. М., 2004. С.21–26.

[20] См. напр.: *Мешкова Т.А.* Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности: Автореф. … канд. полит. наук. М., 2003. С.4–5; *Митрохина Е.Ю.* Информационная безопасность личности как социальная проблема // Глобальная информатизация и безопасность России. М., 2001. С.106–107.

УДК 328:004

«ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО»: ОСНОВНЫЕ ТРАКТОВКИ ПОНЯТИЯ И ФУНКЦИОНАЛЬНОСТИ

А.Ю. Цаплин

Саратовский государственный университет,
кафедра политических наук
E-mail: can2002@yandex.ru

В статье рассматриваются основные научные трактовки понятия «электронное правительство», проводится их сравнительный анализ, раскрываются основные характеристики, функции, структурные элементы, принципы и цели организации.

"Electronic Government": Main Treatments of the Concept and Functionality

A.Yu. Tsaplin

The paper discusses basic scientific treatments of the "electronic government" concept, their comparative analysis is made, basic characteristics, functions, structural elements, principles and organization purposes are disclosed.

В отечественной научной литературе нет однозначной трактовки понятия *«e-Government»*. Дословно оно переводится как «электронное правительство». Однако существует мнение, что прямой перевод e-Government не совсем соответствует положению вещей, поскольку здесь необходимо иметь в виду сетевую инфраструктуру не только исполнительной власти, но и в целом всех органов государственной власти и местного самоуправления. С этих позиций М.Н.Грачев отождествляет термин *«e-Government»* с понятием «электронная инфраструктура институтов публичной власти», которая объединяет в себе технологии информационного взаимодействия между органами власти и гражданами, органами власти и институтами гражданского общества, включая бизнес структуры и общественные объединения, а также между разными государственными и муниципальными учреждениями. В этой связи термин «электронное правительство» соотносится с одним из функциональных компонентов данной инфраструктуры, связанным с деятельностью органов исполнительной власти[1].

В рамках такого подхода e-Government отождествляется с понятием «электронное государство», которое отражает деятельность всех ветвей власти, основанную на достижениях в области информационных технологий.

В узком смысле понятие «электронное правительство» означает использование в органах государственного управления современных технологий, в том числе и Интернет-технологий, на основе чего происходит изменение взаимодействия как внутри органов власти, так и с общественностью. Такая трактовка совпадает с прикладными задачами электронного правительства, направлен-