УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

НОВЫЕ ФОРМЫ УПРАВЛЕНИЯ В ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ СРЕДЕ И ПРОБЛЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

Сулимин А. Н.

кандидат политических наук, доцент кафедры «Государственное и муниципальное управление» Астраханского филиала, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Россия), 414004, Россия, г. Астрахань, ул. Валерии Барсовой, д. 15, к. 12, Kratos84@yandex.ru

УДК 323(470)
ББК 66.2(2Рос)

Цель. Изучение информационных угроз российского общества и государства в условиях глобализации. Выявление основных направлений государственной политики по обеспечению информационной безопасности российского общества.

Методология и методы. Проводится анализ международных и российских программных документов, посвященных становлению глобального информационного сообщества. В качестве ключевого подхода в исследовании используется концепция сетевой власти информационного сообщества.

Результаты и практическая значимость. Автор делает выводы, что глобальные тренды информационного общества направлены на формирование надгосударственной сетевой власти понижающей роль государственных институтов РФ в социально-политических процессах. Характеризуются условия способствующие созданию системы государственной информационной безопасности в РФ.

Научная новизна. Раскрываются негативные факторы воздействия надгосударственной сетевой власти на открытость государственных институтов и информационную безопасности российского общества.

Ключевые слова: информационная безопасность, сетевая власть, глобализация, информационное общество, электронное правительство, персональные данные, универсальная электронная карта, Homo-informatucus.

NEW FORMS OF GOVERNANCE IN THE GLOBAL INFORMATION ENVIRONMENT AND PROBLEMS OF THE RF NATIONAL SECURITY

Sulimin A. N.

Candidate of Political Science, Associate Professor of Public and Municipal Management Department of the Astrakhan branch of the Russian Presidential Academy of National Economy and Public Administration (Russia), fl. 12, 15, Valerii Barsovoi str., Astrakhan, Russia, 414004, Kratos84@yandex.ru

Purpose. To study information threats for the Russian society and the state in globalization. To identify the main directions of public policy on information security of the Russian society.

Methodology and methods. The Russian and international policy documents on global information community development are analyzed. As a key research approach the concept of information community network power is used.

Сулимин А. Н.

Results and practical significance. The author draws the conclusions that global trends of information society are focused at creating supranational network power reducing the role of the RF public institutions in socio-political processes. Conditions contributing to the RF public information security system development are characterized.

Scientific novelty. Negative impacts of supranational network power on public institutions openness and information security of the Russian society are revealed.

Key words: information security, network power, globalization, information society, e-government, personal data, universal electronic card, Homo-informatucus.

Информационное общество является мейнстримом глобализации и объединяет с помощью информационно-коммуникативной сети Интернет всех его акторов. Интеграция социума с помощью виртуальных сетей имеет в своей основе объективный характер, так как на надгосударственном уровне провозглашается необходимость формирования принципов единого государственного управления. Лидеры стран «Группы восьми» 22 июля 2000 года приняли «Окинавскую хартию глобального информационного общества», в которой подчеркивалось, что информационно-коммуникативные технологии становятся новым драйвером мирового социально-экономического развития [8]. На Всемирной встрече в Женеве на уровне глав государств-членов ООН по вопросам глобального информационного общества был выработан «План действий по построению информационного общества». На этой встрече было решено, что государства берут на себя обязанность по созданию электронного правительства, которое выстраивается по единым международным стандартам на единой информационной и программной платформе [2].

В 2005 году «Тунисской программой для информационного общества» провозглашались цели электронного правительства в доступе к государственной информации и службам для получения государственных услуг с помощью информационно-коммуникативных технологий (ИКТ) из любого места [11]. Главная цель программ по выстраиванию информационного общества – снижение роли «государственного суверенитета» и «национальной безопасности», прозрачность деятельности всех органов власти для контроля со стороны глобальных сетей

Внедрение системы электронного правительства началось в США в 1993 году. Впоследствии система электронного государственного управления стала инструментом модернизации на единых принципах для многих развивающихся государств, как необходимый и неизбежный механизм развития демократии американского типа.

Российская Федерация взяла на себя обязанности выстраивания информационного общества и сотрудничества с другими странами, импортируя необходимые технологии открытого (электронного) государственного управления. Внедрение технологий открытости в деятельность органов власти России способствует снижению информационной безопасности государства и общества. Поэтому главной целью работы является анализ информационных угроз исходящих от технологий электронного правительства и выявление основных направлений укрепления системы информационной безопасности РФ.

1. *Новые технологии как инструмент утраты государственного суверенитета.* По мнению некоторых исследователей, создание институтов электронного правительства, способствует повышению управляемости демократических институтов [3]. Возникает вопрос: кто будет являться субъектом управления в этом случае? Ведь реализуя мероприятия информатизации, Россия следует не столько тенденциям внутреннего развития, сколько навязанным сверху международным обязательствам. Так для реализации мероприятий по выстраиванию электронного правительства России и Евросоюз разработали G2C-проект «Поддержка электронного правительства в Российской Федерации». Реализация проекта возложена на ирландскую компанию GDSI, действующую в консорциуме с Steinbeis GmBH (Германия) [9]. Однако технологии открытости органов государственной власти («электронного правительства») позволяют получить доступ к любой информации абсолютно всем пользователям «всемирной паутины». Облегчение доступа к получению, обработки и использованию информации, позволяет управлять социально-политическими процессами из любого места на земном шаре, подрывая монополию государства в сфере политической власти.

2. *Проблема незащищенности личных данных граждан РФ пользователей УЭК.* Для развития системы государственных и муниципальных услуг мероприятия электронного правительства предполагают внедрение универсальных электронных карт, в которых содержится обширный перечень персональных данных граждан [10]. УЭК может содержать следующую информацию: биометрические персональные данные человека (фото, рост, вес, рисунок радужной оболочки глаза, дактилоскопические данные, анализ ДНК, цифровая подпись), также личные данные (сведения о здоровье, социальном обеспечении, уплате налогов, передвижениях, покупках, финансовых операциях).

При введении новых типов идентификации персональных данных незащищенной становится информация не только обычных людей, но и категорий граждан, чье должностное положение существенно влияет на уровень безопасности и стабильности нашего государства – это государственные служащие, сотрудники госучреждений и госкомпаний и т.д.

Особенно актуальной представляется проблема «утечек» данных, в условиях передачи процедур обработки, хранения, распространения личной информации от государственных организаций коммерческим структурам («операторам»), что закрепляется в федеральном законе № 152 «О защите персональных данных» [6]. Академик РАЕН С. С. Ковалевский считает что, системы управления базами данных (СУБД) в РФ, основаны на западных разработках и имеют проблему «стеганографии» – скрытой передачи данных. В связи с этим он задается вопросом: «О какой безопасности может идти речь, когда всеми информационными ресурсами в России управляют западные операционные системы и СУБД, исходные коды которых известны только разработчикам»? [11, с.15].

В списке стран с высоким уровнем совершаемых преступлений в киберсфере, Россия занимает первое место [4, с. 46]. Это значит, что РФ не готова к внедрению новых информационных технологий, так как отсутствуют как стратегии, так и технологии обеспечения национальной информационной безопасности. Поэтому дальнейшая модернизация в сфере высоких технологий может обострить имеющиеся проблемы с преступностью и перевести значительное количество правонарушений в виртуальную сферу.

3. *Проблема появления недемократических технологий политического контроля над гражданами.* Современные информационные технологии позволяют установить контроль над человеком в условиях деидеологизации массового сознания общества. Благодаря технологии радиочастотной идентификации RFID (radio frequency identification) появилась возможность передавать и получать данные на расстоянии в автоматизированном режиме. Считывание информации с микроскопических чипов специальным сканером делает устройство RFID незаменимым для контроля над товарами, обеспечения безопасности в виде карт доступа, слежения за животными и детьми, багажом на авиалиниях, книгами в библиотеках. Внедрение чипа-RFID в биометрические паспорта (e-passport) на которых хранятся сведения о его владельце (двумерная и трехмерная фотографии, отпечатки пальцев, рисунок сетчатки глаз и запись голоса) упрощает процесс идентификации личности, что может являться эффективным инструментом контроля над преступными и девиантными элементами общества. Также данное устройство может использоваться криминальными структурами для «кражи личности» (Identity theft) – феномена в сфере киберпреступности западных стран.

Озабоченность вызывает появление технологий позволяющих имплантировать электронные идентификационные устройства в организм человека. Внедрение подобного рода технологий впервые началось в США, где на данный момент действует закон о здравоохранении, предусматривающий с 2013 года обязательную имплантацию каждому американцу микрочипа в руку [1, с. 35–36]. Если обратиться к российским программно-целевым документам, то и они также предусматривают создание управляемых биообъектов: «Наноэлектроника будет интегрироваться с биообъектами, и обеспечивать непрерывный контроль за поддержанием их жизнеспособности, улучшением качества жизни, и таким образом снижать расходы государства» [7].

Создание сервисов «одного окна» посредством замещения государственных обязанностей на платные государственные услуги подменяет социальные принципы коммерческими интересами. В этих условиях возникает риск окончательной утраты такой функции российской власти, как поддержание социального равенства и справедливости. Присвоение единого номера, каждому гражданину взамен фамилии и имени приведет к процессу обезличивания человека, потери личности и статуса субъекта правоотношений.

Информационная открытость системы государственного управления, передача государственных функций в коммерческий сектор значительно трансформируют роль государства в общественных отношениях. Формируется электронное государство (e-Government) с электронными людьми (Homo-informatucus), взаимодействующие между собой только посредством мощностей вычислительной техники, а не на базе каких-то всеобщих, социально значимых норм и процедур. Электронное взаимодействие между правительством и населением обуславливает становление нового политического порядка, где все изменчиво и нет места морально-этическим правилам, а значит и правовым нормам, так как право всегда основывалось на этике и морали.

Сетевая власть осуществляет свое господство имплицитно через отчуждение нематериальных (информационных) ресурсов общества. Государства более не в состоянии монопольно распоряжаться и контролировать информационные потоки, так как сетевая власть носит глобальный характер, она не привязана к конкретным территориям и присутствует всюду, где есть доступ к виртуальному миру. Контрольно-надзорные государственные институты неспособны эффективно предотвращать электронные преступления, совершаемые глобальной сетевой мафией. Сетевые формы контроля над обществами представляют угрозу национально-культурным

идентичностям, так как в динамичных условиях новые знания и правила быстро устаревают. Чем больше людей живут по этим правилам, тем быстрее они теряют свою ценность. Поэтому реальная девальвация в информационном обществе будет угрожать не денежным валютам, а национально-государственным традициям и общественным ценностям. Постоянный подрыв авторитета государственных институтов является следствием неспособности национальных государств осуществлять контроль над информационным обществом, которое становится все более глобальным.

Проблемы информационной безопасности в контексте открытости и незащищенности осознаются государственной властью РФ, что подтверждается принятием Федерального закона № 282-ФЗ, предписывающего обязательное хранение персональных данных на российских серверах [5]. Однако отсутствие границ у информационно-телекоммуникационных систем, наличие транснациональной киберпреступности делает сомнительной возможность полной сохранности персональных данных россиян внутри страны.

Итак, институционализация системы электронного правительства в РФ подрывает информационную безопасность, так как она не способна обеспечить защищенность законных прав личности в информационной среде. Угрозам подвергаются государственные институты, воспроизводящие социальный порядок, но не обеспечивающие информационный контроль над сферами массовой идеологии и культуры. Поэтому на государственном уровне необходима разработка адекватной стратегии информационной безопасности, учитывающей вызовы глобального информационного сообщества. Информационные системы государственной безопасности должны создаваться, как на структурном, так и на сетевом уровне и соответствовать требованиям технологической независимости от внешних информационных систем. Контроль над языковой сферой больших масс людей является конкурентным преимуществом в эпоху глобализации, так как информация имеет определенную символическую и языковую кодировку. Ответом на информационные угрозы глобализации может стать сбережение русского языка, как средства сохранения и передачи культурной идентичности. Поэтому российскому государству необходимо всеми возможными способами поддерживать носителей русского языка и максимально сберегать ареалы локализации русскоязычного населения, так и способствовать тенденциям русскоязычной глобализации.

Литература:

1. Головин В. Г., Большакова В. М. Электронная идентификация личности гражданина: за или против // Власть. 2014. № 8. С. 33–36.
2. Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии: Документ WSIS-03/GENEVA/DOC/4-R от 12 дек. 2003 г. [электронный ресурс]. URL: http:// www.un.org/ru/ documents/decl_conv/declarations/pdf/wsis_dec.pdf (дата обращения 21.01.2015).
3. Игнатова А. М. Открытые данные как новый способ взаимодействия государства и общества // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2015. № 1. Ч. II. С. 78–80.
4. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.
5. О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: Федеральный закон от 21 июля 2014 г. № 242-ФЗ // Российская газета. 2014. № 6435. 23 июля.
6. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 21.07.2014 г.) // Российская газета. 2006. 29 июля.
7. Об утверждении Стратегии развития электронной промышленности России на период до 2025 года: Приказ Министерства промышленности и энергетики РФ от 7 августа 2007 г. № 311 [электронный ресурс]. Доступ из справ.-правовой системы «Гарант».
8. Окинавская хартия глобального информационного общества от 22 июля 2000 года: Сайт Кремля [электронный ресурс]. URL: http://archive.kremlin.ru/text/docs/2000/07/123786.shtml (дата обращения 21.01.2015)
9. Программа институциональной реформы Поддержка электронного правительства в Российской Федерации – проект G2C [электронный ресурс]. URL: http://federalbook.ru/files/SVAYZ/saderzhanie/Tom%2010/II/Abramichev.pdf (дата обращения 22.01.2015).
10. Сулимин А. Н. Риски вступления России в глобальное информационное сообщество // Вестник ПАГС. 2014. № 41. С. 21–25.
11. Тунисская программа для информационного общества: Документ WSIS-05/TUNIS/DOC/6(REV.1)-R от 15 ноября 2005 г. [электронный ресурс]. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения 24.01.2015).
12. Яковлева О. А. Новые технологии и права человека. Рязань: Зерна, 2012. 208 с.

References:

1. Golovin V. G., Bolshakova V. M. Electronic identification of citizen's personality: for or against // Vlast'. 2014. № 8. P. 33–36.
2. Declaration of principles Developing information society – a global challenge in the new millennium:

Document WSIS-03 / GENEVA / DOC / 4-R December 12, 2003 [e-resource]. URL: http:// www.un.org/ru/ documents/decl_conv/declarations/pdf/wsis_dec.pdf (access date 21.01.2015).
3. Ignatova A. M. Open data as a new way of interaction between state and society // Historical, philosophical, political and legal sciences, cultural studies and art history. Issues of theory and practice. 2015. № 1. Part II. P. 78–80.
4. Karpova D. N. Cybercrime: a global problem and its solution // Vlast'. 2014. № 8. P. 46–50.
5. On Amendments to certain Legislative Acts of the Russian Federation as regards to specifying the personal data processing in information-telecommunication networks: Federal Law of July 21, 2014 № 242-FL // Rossiiskaya gazeta. 2014. № 6435. July 23.
6. On personal data: Federal Law of July 27, 2006 № 152-FL (as amended on 21. 07.2014) //Rossiiskaya gazeta. 200.6 July 29.
7. On approval of the Strategy for the electronic industry development of Russia for the period up to 2025: Order of the RF Ministry of Industry and Energy, August 7, 2007 № 311 [e-resource]. Access from ref.-legal system "Garant".
8. The Okinawa Charter on Global Information Society on July 22, 2000: The website of the Kremlin [e-resource]. URL: http://archive.kremlin.ru/text/docs/2000/07/123786.shtml (date of access 21.01.2015)
9. The institutional reform program Support to e-government in the Russian Federation – Project G2C [e-resource]. URL: http://federalbook.ru/files/SVAYZ/saderzhanie/Tom%2010/II/Abramichev.pdf (date of access 22.01.2015).
10. Sulimin A. N. Risks of Russia's entry into the global information society // Vestnik PAGS. 2014. № 41. P. 21–25.
11. Tunis Agenda for the Information Society: Document WSIS-05 / TUNIS / DOC / 6 (REV.1)-R on November 15, 2005. [e-resource]. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (date of access 24.01.2015).
12. Yakovleva O. A. New technologies and human rights. Ryazan: Zerna, 2012. 208 p.