5. Мудуев Ш. С. Особенности миграционных процессов в Дагестане // Проблемы миграции и опыт ее регулирования в полиэтничном Кавказском регионе. Москва, 2001.
6. Новейший политологический словарь / под ред. Д. Е. Погорелого. Ростов-на-Дону, 2010. 318 с.
7. Регионы России: социально-экономические показатели. Москва, 2013. 990 с.
8. Российский статистический ежегодник. 2013 / Росстат. Москва, 2013. 717 с.

References

1. Aleshkovskiy I. A. Mezhdunarodnaya migratsiya v nachale XXI veka: globalnye tendentsii i osobennosti Rossii [International migration at the beginning of the XXI century: global trends and features of Russia]. *Geopolitika i bezopasnost* [Geopolitics and Security], 2011, no. 4, pp. 81–91.
2. Araphanova L. Ya. Migratsionnye problemy v Respublike Ingushetiya [The migration problem in the Republic of Ingushetia]. *Migratsionnye protsessy na Yuge Rossii: realii, problemy, perspektivy* [Migration processes in the South of Russia: Realities, Problems and Prospects]. Rostov-on-Don, Northern Caucasus Academy of State Service Publ., 2008, no. 2, pp. 92–94.
3. *V Ingushetii uzhestochat migratsionnuyu politiku* [The migration policy in Ingushetia will betighen]. Available at: http://www.ingushetia.ru/m-news/archives/019204.shtml/.
4. Krasnoslobodcev V. P. Respublika Ingushetiya [The Republic of Ingushetia]. *Rossiya regionov: v kakom sotsialnom prostranstve my zhivem?* [Russian regions :what social space do we live in?]. Moscow, Pomatur Publ., 2005.
5. Muduev Sh. S. Osobennosti migratsionnykh protsessov v Dagestane [Features of migration processes in Dagestan]. *Problemy migratsii i opyt ee regulirovaniya v poliyetnichnom Kavkazskom regione* [Problems of migration and the experience of its regulation in the multiethnic Caucasus region]. Moscow, 2001.
6. *Noveyshiy politologicheskiy slovar* [Political Science Dictionary]. Ed. by D. E. Pogorelyy. Rostov-on-Don, 2010, 318 p.
7. *Regiony Rossii: sotsialno-ekonomicheskie pokazateli* [Regions of Russia: socio-economic indicators]. Moscow, 2013, 990 p.
8. *Rossiyskiy statisticheskiy ezhegodnik* [Statistical Yearbook of Russia]. 2013. Moscow, 2013, 717 p.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ И УГРОЗЫ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО СООБЩЕСТВА

Сулимин Александр Николаевич, кандидат политических наук, доцент
Российская академия народного хозяйства и государственной службы при Президенте РФ (Астраханский филиал)
Российская Федерация, 414024, г. Астрахань, ул. Б. Хмельницкого, 33а
E-mail: kratos84@yandex.ru

Целью научной статьи является изучение информационных угроз российского общества и государства в условиях глобализации и выявление основных направлений государственной политики по обеспечению информационной безопасности российского общества. Актуальность работы заключается в том, что современное общество вступило на информационную стадию своего развития, что изменяет традиционные формы взаимодействия между властью и обществом, а информация становится главной ценностью в общественных отношениях. Автором проводится анализ международных и российских программных документов, посвященных становлению глобального информационного сообщества. В качестве ключевого подхода в исследовании используется концепция сетевой власти информационного сообщества. Утверждается, что формирование институтов электронного правительства предусматривается соглашениями на межгосударственном уровне, целью которых является создание единой системы электронного правительства в мире. Система открытого государственного управления в России внедряется с помощью иностранных технологий, что подрывает национальную безопасность государства. Создание информационных систем автоматической обработки может привести к таким угрозам государственной и личной безопасности как утечка информации, скрытая передача данных, отслеживание физического состояния человека. Автор делает выводы, что глобальные тренды информационного общества направлены на формирование надгосударственной сетевой власти понижающей роль государственных институтов РФ в социально-политических процессах. Наиболее уязвимым сегментом государственной безопасности в информационном обществе становится национальная идентичность, которая трансформируется в сетевой тип

идентификации. Главными условиями укрепления национальной безопасности РФ является создание системы государственной информационной безопасности.

Ключевые слова: информационная безопасность, сетевая власть, глобализация, информационное общество, электронное правительство

RUSSIA'S INFORMATION SECURITY AND THREATS TO THE GLOBAL INFORMATION SOCIETY

Sulimin Aleksandr N., Ph.D. (Politicy), Associate Professor
Astrakhan branch of Russian Presidential Academy of National Economy and Public Administration
33a B. Khmelnitskogo Str., Astrakhan, 414024, Russian Federation
E-mail: kratos84@yandex.ru

The purpose of a scientific article is the study of information threats of Russian society and the state in the context of globalization. Modern society entered on information stage of the development that changes traditional forms of interaction between the power and society, and information becomes the main value of the public relations.The analysis of the international and Russian program documents devoted to formation of global information community is carried out. A theory of network power is main scientific approach of research. Formation of institutes of the electronic government is provided by agreements at the interstate level. Main purpose is creation of uniform system of the electronic government in the world. The system of open public administration in Russia is implemented with the help of foreign technology that undermines the national security of the state. The author draws conclusions that global trends of information society are directed on formation of the supranational network power lowering a role of the state institutes of the Russian Federation in socio-political processes. National identity is the most vulnerable segment of state security in information society which becomes transformed to supranational information type of political culture. The main condition of strengthening of national security of the Russian Federation is creation of system of the state information security.

Keywords: information security, network power, globalization, information society, electronic government

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. При этом субъективный фактор информатизации социально-политических процессов заключается в том, что на надгосударственном уровне провозглашается необходимость формирования принципов единого государственного управления. Лидеры стран «Группы восьми» 22 июля 2000 г. приняли «Окинавскую хартию глобального информационного общества», в которой подчеркивалось, что информационно-коммуникативные технологии становятся новым драйвером мирового социально-экономического развития [9]. 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 г. «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 [14].

В 2000-е гг. в рамках вышеуказанных программ Российская Федерация взяла на себя обязательства выстраивания информационного общества, импортируя необходимые технологии открытого (электронного) государственного управления. Внедрение технологий открытости в деятельность органов власти России определяет уровень информационной безопасности государства и общества. Поэтому необходимо провести анализ информационных угроз исходящих от технологий электронного

правительства и выявить основные направления 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, Россия при финансовой и методической поддержке Евросоюза разработала G2C-проект «Поддержка электронного правительства в Российской Федерации» [11]. По заказу Министерства экономического развития РФ и Министерства связи и массовых коммуникаций РФ реализация данного проекта была возложена на британо-ирландскую консалтинговую компанию GDSI. Согласно официальному сайту GDSI стоимость этой услуги составляет 2 млн. евро [16].

Таким образом, внедряемые *технологии открытости органов государственной власти («электронного правительства») позволяют транснациональным институтам не только получить доступ к стратегическим важным направлениям государственной политики, но и напрямую участвовать в их реализации. Определение целей, задач, принципов государственного управления со стороны негосударственных акторов нарушает монополию государственной власти на принятие политических решений, что подрывает принцип внешнего суверенитета российского государства.*

2. *Проблема незащищенности личных данных граждан РФ пользователей УЭК.* Переход на систему электронного документооборота в рамках мероприятий электронного правительства значительно ускоряет процессы коммуникации и принятия управленческих решений в государственных и коммерческих структурах. Однако главной целью данной технологии является обеспечение открытости управленческих процессов. В информационных системах никто не может гарантировать сохранность информации, поэтому 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» [7].

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»? [15, с. 15].

По словам IT-специалиста Всемирного Банка В. Медведева, все технологии управления базами данных универсальны и располагаются в США и Германии. 70 % российских организаций, включая Газпром, Пенсионный фонд РФ, Сбербанк, Ростелеком используют базу данных SAP, главный «облачный центр» которой находится на территории ФРГ. На базе германской SAP в РФ воссоздается система электронного правительства, представляющая собой электронный документооборот, основанный на едином языке XML и согласующую базы данных программу e-government – или «облачное управление» [3].

Законодательное и технологическое внедрение транснациональных баз данных сопровождается созданием электронных архивов с оцифровкой документов на бумажных носителях, что позволяет закачать значительный массив секретной информации в информационную сеть. В России оцифровкой большинства массивов бумажных данных занимается частная корпорация «Электронный Архив» (ЭЛАР), включая засекреченные документы государственных архивов, данные собранные при проведении переписи населения, информацию по открытию счетов в банках, выпуску карт социального обеспечения [10].

Для электронной идентификации граждан предполагается создание портативных баз данных – универсальных электронных карт, содержащих обширный перечень персональных данных [12]. УЭК может хранить следующую информацию о человеке: биометрические персональные данные (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).

По нашему мнению, введении новых типов идентификации персональных данных прямо пропорционально сопровождается снижением их защищенности, так как открытой 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. Сейчас Россия занимает первое место в списке стран с высоким уровнем совершаемых преступлений в киберсфере [5, с. 46]. Это значит, что РФ не готова к внедрению новых информационных технологий, так как отсутствуют стратегия и технология 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 и 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 беспроводным способом. 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. Данное устройство также может эффективно использоваться и криминальными структурами для «кражи личности» (Identity theft) – широко распространенной практики 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 г. обязательную имплантацию каждому американцу микрочипа в руку [1, с. 35–36]. Если обратиться к российским программно-целевым документам, то и они также предполагают создание управляемых биообъектов. Согласно тексту «Стратегии развития электронной промышленности РФ до 2025 г. «…наноэлектроника будет интегрироваться с биообъектами, и обеспечивать непрерывный контроль за поддержанием их жизнеспособности, улучшением качества жизни, и таким образом снижать расходы государства» [8].

Создание сервисов «одного окна» посредством замещения государственных обязанностей на платные государственные услуги подменяет социальные принципы коммерческими интересами. В этих условиях возникает риск окончательной профанации базовых конституционных принципов социального государства. 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 [13]. Формируется электронное госу-

дарство (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 [6]. Однако отсутствие внутреннего контура у информационно-телекоммуникационной системы РФ, наличие высокого уровня 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.

Список литературы

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. Режим доступа: http:// www.un.org/ru/ documents/decl_conv/declarations/pdf/wsis_dec.pdf, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).

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. 2. С. 78–80.
4. Интервью с В. Медведевым, главным IT-специалистом Всемирного Банка. Режим доступа:http://communitarian.ru/publikacii/interviu/kak_globaly_vystraivayut_elektronnoe_rabstvo_chast_i_04022015/, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
5. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.
6. 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.
7. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 21.07.2014 г.) // Российская газета. 2006. № 4431. 29 июля.
8. Об утверждении Стратегии развития электронной промышленности России на период до 2025 года : Приказ Министерства промышленности и энергетики РФ от 7 августа 2007 г. № 311. Режим доступа: http://www.garant.ru/products/ipo/prime/doc/91853/ свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
9. Окинавская хартия глобального информационного общества от 22 июля 2000 года. Режим доступа: http://archive.kremlin.ru/text/docs/2000/07/123786.shtml, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
10. Официальный сайт корпорации ЭЛАР. Режим доступа: http://www.elar.ru/, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
11. Программа институциональной реформы Поддержка электронного правительства в Российской Федерации – проект G2C. Режим доступа: http://federalbook.ru/files/SVAYZ/saderzhanie/Tom%2010/II/Abramichev.pdf, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
12. Сулимин А. Н. Риски вступления России в глобальное информационное сообщество // Вестник Поволжской академии государственной службы. 2014. № 41. С. 21–25.
13. Сулимин А. Н. Глобализация для России: от корпорации-государства к государству-цивилизации // Каспийский регион: политика, экономика, культура. 2014. № 3 (40). С. 95–102.
14. Тунисская программа для информационного общества: Документ WSIS-05/TUNIS/DOC/6(REV.1)-R от 15 ноября 2005 г. Режим доступа: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf, свободный. Загл. с экрана. Яз. рус. (Дата обращения 20.04.2015 г.).
15. Яковлева О. А. Новые технологии и права человека. Рязань: Зерна, 2012. 208 с.
16. Support to E-Government in the Russian Federation. 20.04.2014. Режим доступа: http://www.gdsi.ie/index.php/component/content/article/54-old/regional-and-rural-development-russian-federation/100-support-to-e-government-in-the-russian-federation, свободный. Загл. с экрана. Яз. рус.

References

1. Golovin V. G., Bolshakova V. M. Elektronnaya identifikatsiya lichnosti grazhdanina: za ili protiv [Electronic identification of citizens: pros and cons].*Vlast* [Authority], 2014, no. 8, pp. 33–36.
2. *Deklaratsiya printsipov Postroenie informatsionnogo obshchestva – globalnaya zadacha v novom tysyacheletii: Dokument WSIS-03/GENEVA/DOC/4-R ot 12 dek. 2003 g.* [The Declaration of principles building the information society: a global challenge in the new Millennium]. 20.04.2014. Available at: http:// www.un.org/ru/ documents/decl_conv/declarations/pdf/wsis_dec.pdf. (Accessed 20.04.2015).
3. Ignatova A. M. Otkrytye dannye kak novyy sposob vzaimodeystviya gosudarstva i obshchestva [Open data as new method of interaction of state and society]. *Istoricheskie, filosofskie, politicheskie i yuridicheskie nauki, kulturologiya i iskusstvovedenie. Voprosy teorii i praktiki* [Historical, Philosophical, Political and Law Sciences, Culturology and Study of Art. Issues of Theory and Practice], 2015, no. 1, pp. 78–80.
4. *Intervyu s V. Medvedevym, glavnym IT-spetsialistom Vsemirnogo Banka* [Interview with V. Medvedev, chief IT specialist of the World Bank]. 20.04.2014. Available at: http://communitarian.ru/publikacii/interviu/kak_globaly_vystraivayut_elektronnoe_rabstvo_chast_i_04022015. (Accessed 20.04.2015).
5. Karpova D. N. Kiberprestupnost: globalnaya problema i ee reshenie [Cybercrime: a global challenge and its solution]. *Vlast* [Authority], 2014, no. 8, pp.46–50.

6. O vnesenii izmeneniy v otdelnye zakonodatelnye akty Rossiyskoy Federatsii v chasti utochneniya poryadka obrabotki personalnykh dannykh v informatsionno-telekommunikatsionnykh setyakh: Federalnyy zakon ot 21 iyulya 2014 g. No. 242-FZ [On amendments to certain legislative acts of the Russian Federation in the part of governing the processing of personal data in information and telecommunication networks: the Federal law of July 21, 2014 No. 242-Fl]. *Rossiyskaya gazeta* [Russian Gazette], 2014, no. 6435.
7. O personalnykh dannykh: Federalnyy zakon ot 27 iyulya 2006 g. No. 152-FZ (red. ot 21.07.2014 g.) [On personal data: the Federal law of 27 July 2006 No. 152-Fl]. *Rossiyskaya gazeta* [Russian Gazette], 2006, no. 4431.
8. *Ob utverzhdenii Strategii razvitiya elektronnoy promyshlennosti Rossii na period do 2025 goda: Prikaz Ministerstva promyshlennosti i energetiki RF ot 7 avgusta 2007 g. No. 311* [About approval of Strategy of development of electronic industry of Russia for the period up to 2025: the order of the Ministry of industry and energy of the Russian Federation dated August 7, 2007 No. 311]. 20.04.2014. Available at: http://www.garant.ru/products/ipo/prime/doc/91853/. (Accessed 20.04.2015).
9. *Okinavskaya khartiya globalnogo informatsionnogo obshchestva ot 22 iyulya 2000 goda* [Okinawa Charter on global information society of 22 July 2000]. 20.04.2015 Available at: http://archive.kremlin.ru/text/docs/2000/07/123786.shtml. (Accessed 20.04.2015).
10. *Ofitsialnyy sayt korporatsii ELAR* [The official website of the ELAR Corporation]. 20.04.2014. Available at: http://www.elar.ru. (Accessed 20.04.2015).
11. Programma institutsionalnoy reformy Podderzhka elektronnogo pravitelstva v Rossiyskoy Federatsii – proekt G2C [The program of institutional reform Support e-government in the Russian Federation]. 20.04.2014. Available at: http://federalbook.ru/files/SVAYZ/saderzhanie/Tom% 2010/II/Abramichev.pdf. (Accessed 20.04.2015).
12. Sulimin A. N. Riski vstupleniya Rossii v globalnoe informatsionnoe soobshchestvo [The Risks of Russia's Joining the Global Information Community]. *Vestnik Povolzhskoy akademii gosudarstvennoy sluzhby* [Bulletin of the Volga Region Academy of Public Administration], 2014, no. 41, pp. 21–25.
13. Sulimin A. N. Globalizatsiya dlya Rossii: ot korporatsii-gosudarstva k gosudarstvu-tsivilizatsii [Globalization for Russia: from corporation-state to state-civilization]. *Kaspiyskiy region: politika, ekonomika, kultura* [The Caspian Region: Politics, Economics, Culture], 2014, no. 3 (40). pp. 95–102.
14. *Tunisskaya programma dlya informatsionnogo obshchestva: Dokument WSIS-05/TUNIS/DOC/6(REV.1)-R ot 15 noyabrya 2005 g.* [Tunis agenda for the information society: Document WSIS-05/TUNIS/DOC/6(Rev. 1)-R dated 15 November 2005]. 20.04.2014. Available at: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf. (Accessed 20.04.2015).
15. Yakovleva O. A. *Novye tekhnologii i prava cheloveka* [New technologies and human rights]. Ryazan, Zerna Publ., 2012, 208 p.
16. *Support to E-Government in the Russian Federation.* 20.04.2014. Available at: http://www.gdsi.ie/index.php/component/content/article/54-old/regional-and-rural-development-russian-federation/100-support-to-e-government-in-the-russian-federation/.

НЕКОНТРОЛИРУЕМАЯ МИГРАЦИЯ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Калгин Михаил Вячеславович, аспирант
Астраханский государственный университет
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а
E-mail: kalginmv@mail.ru

Все это в совокупности ведет к обострению социальной ситуации в принимающих обществах. Слишком массированный и почти неконтролируемый приток самых разных мигрантов, на глазах становится проблемой, которая из экономической превращается в социальную и начинает приобретать угрожающий политический облик. Практика показывает, что истинная цена миграции для принимающего государства, значительно выше потенциальных рисков и иррациональных страхов. В реальности основная масса мигрантов, пройдя период адаптации, начинает вносить свой вклад в социально-экономическое развитие страны. Однако помимо конструктивных сил имеет место быть и деструктивные силы, асоциальное поведение которых усиливает проблемы, связанные с обеспечением национальной безопасности страны.