РАЗВИТИЕ БИО- И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТЕКСТЕ ЛИЧНОСТНОЙ БЕЗОПАСНОСТИ

Е.С. Зиновьева, Ю.И. Войтенко

Московский государственный институт международных отношений (университет) МИД России. Россия, 119454, Москва, пр. Вернадского, 76.
МИД России, 119200 Москва, Смоленская-Сенная пл., 32/34.

Развитие постиндустриального общества инициирует глубокие экономические, технологические и культурные изменения в укладе жизни всего человечества. Революционные прорывы в области новых технологий, таких как биотехнологии и информационные технологии, отражаются во всех сферах человеческой деятельности, напрямую влияя на самого человека, в том числе и в контексте безопасности.

В статье с позиций теории личностной безопасности рассмотрены последствия широкого распространения биотехнологий и информационных технологий во внешнеполитической деятельности государств. Приводится подробная характеристика основных направлений использования биометрических технологий во внешнеполитической и консульской практике государств, рассмотрены вызовы и угрозы информационной безопасности, возникающие в связи с широким распространением биотехнологий, перечислены основные вызовы и угрозы личностной безопасности, возникающие на современном этапе развития и применения указанных технологий. При этом вызовы и угрозы личностной безопасности, связанные с использованием технологий, помещены в более широкий контекст общемировых тенденций научно-технологического развития. В заключении формулируются рекомендации в области внешней политики государств и международного сотрудничества, которые позволили бы нивелировать новые угрозы международной и личностной безопасности, возникающие на современном этапе развития биотехнологий.

Авторы приходят к выводу, что обеспечить этичное регулирование новых технологий, учитывающее вопросы личностной безопасности, возможно в рамках многосторонних партнерств на национальном и международном уровне, в работе которых принимали бы участие не только государства, но и представители гражданского общества, бизнеса и исследовательского сообщества.

Ключевые слова: биометрические технологии, информационные технологии, внешняя политика государств, международная безопасность, личностная безопасность.

Личностная безопасность и современные тенденциинаучно-технологического развития

Развитие постиндустриального общества инициирует глубокие экономические, технологические и культурные изменения в укладе жизни всего человечества. Революционные прорывы в области новых технологий отражаются во всех сферах человеческой деятельности, напрямую влияя на самого человека. Очевидна тенденция к сближению естественных наук и наук о человеке. Особый статус приобретают современные биотехнологии и информационно-коммуникационные технологии, опосредованно (и иногда и прямо) влияя на инструменты внутренней и внешней политики государств.

Научно-технологическое развитие оказывает влияние на динамику международной системы, и, следовательно, на природу международной безопасности на современном этапе. Традиционно, международная безопасность в реалистской традиции определялась как защита от военных угроз на уровне государства, однако современные тенденции технологического развития актуализируют проблематику личностной безопасности, что предполагает необходимость «перехода от преимущественного рассмотрения проблем государственной безопасности к анализу угроз существованию человека и способов защиты от них» [4].

Теория личностной безопасности (также используются термины «человеческая безопасность», «безопасность человека») в последние годы привлекает значительное внимание российских и зарубежных исследователей, в том числе Д. Балуева [4], П.А. Цыганкова [5], а также Р. Пэриса [27], Д. Барнетта, В. Агнера [24] и др.

Как отмечает Д. Балуев, понятие личностной безопасности шире, чем исключительно физическая безопасность человека, она также включает в себя удовлетворение материальных потребностей человека, защиту человеческого достоинства, включая возможность участия в жизни общества. При этом личностная безопасность не может быть обеспечена для одной группы за счет другой[4].

В результате развития современных био-технологий, которые используются с опорой на возможности информационно-коммуникационных технологий, появляются новые вызовы и угрозы, связанные не с традиционной трактовкой безопасности как отсутствием военно-политических угроз в межгосударственных отношениях, но с личностной безопасностью, а именно с защитой человека от «электронного тоталитаризма» и повсеместного контроля над частной жизнью, учет прав лиц с ограниченными возможностями и пр.

Использование биометрических технологий во внешнеполитической практике государств

Во внешней политике государства на современном этапе наиболее активно используется такой инструмент биотехнологий, как биометрия, а именно распознавание личности человека по его врожденным биологическим характеристикам, индивидуальным для каждого человека (например, лица, голоса, почерка, отпечатков пальцев, геометрии кисти руки, рисунка радужной оболочки глаза, ДНК). Согласно Техническому отчету Международной организации гражданской авиации (ИКАО) «О включении средств биометрической идентификации в машиносчитываемые проездные документы» понятие «биометрия» или «биометрическая идентификация» означает автоматизированные средства распознавания живого человека с помощью измерения физиологических или поведенческих характеристик» [25].

Отправной точкой к активному использованию биометрии во внешней политике государств стали события 11 сентября 2001 г. в США, после которых Совет Безопасности ООН принял резолюцию № 1373, обязавшую государства, в том числе, усилить меры по предупреждению фальсификации, подделки или незаконного использования документов, удостоверяющих личность. В результате были введены документы нового поколения – биометрические паспорта. Био-паспорт – это документ, в который встроен электронный носитель, микрочип, на котором содержатся индивидуальные данные о личности владельца паспорта, в том числе и биометрическая информация о нём, например отпечатки пальцев или рисунок сетчатки глаза [16].

После введения биометрических паспортов мировые державы приступили к выдаче «биометрических виз» - обязательной процедуре получения биометрических данных граждан, желающих получить визу. Характерно, что переход к биометрическим документам проходил в форсированном режиме, при очевидном давлении на страны со стороны США. 25 ноября 2002 года Конгресс США принял Закон о защите госграницы (U.S. Enhanced Border Security and Visa Entry Reform Act), в соответствии с которым граждане 27 стран мира, которые имели соглашения с США о безвизовом режиме (Западная Европа, Япония, Австралия, Новая Зеландия, Сингапур и Бруней), могли беспрепятственно въезжать на территорию США сроком до 90 дней только при условии наличия у них биометрических паспортов. С 30 сентября 2004 года власти США обязали европейцев проходить процедуру дактилоскопии на своей границе. Новые правила стали распространяются даже на те страны, гражданам которым прежде виза была не нужна.

Кроме того, не без участия США в биометрических паспортах для записи информации стали использовать RFID – чипы (Radio Frequency IDentification - радиочастотная идентификация), которые можно сканировать на расстоянии и узнать все об обладателе паспорта без его ведома. (В США сам термин «биометрия» не популярен, чаще американцы употребляют аббревиатуру RFID). Как отмечают специалисты, RFID – метки

легко отследить, они быстро читаются, позволяя одномоментно контролировать огромное количество людей. Данная технология активно разрабатывалась и использовалась в недрах министерства обороны США в середине прошлого века и после рассекречивания стала применяться американскими компаниями для «чипирования» домашних животных, а впоследствии и людей. Сегодня биометрические технологии, прежде всего, биопаспорта, активно используются не только в США, но и рядом других государств, в частности, в странах Западной Европы.

Прежде всего, использование новых технологий было призвано обеспечить национальную безопасность государств от новых вызовов и угроз, в особенности, транснационального терроризма, нелегальной миграции и организованной преступности за счет идентификации каждого человека. Вместе с тем, в настоящее время нет данных об успешных операциях по противодействию терроризму, базирующихся на использовании биометрических технологий. Более того, согласно заявлению министра внутренних дел Великобритании Чарльза Кларка в интервью BBC, идентификационные документы с биометрией не смогли бы предотвратить серию терактов в общественном транспорте Лондона [3]. Вместе с тем, биометрические технологии потенциально могут быть использованы террористическими организациями. В 2008 г. сотрудники нидерландского университета Radboud University доказали, что из микросхем, которые используются в паспортах, террористы могут создать паспорт-бомбу, которая может срабатывать при приближении к ней паспорта, выданного в заданной стране или при пересылке ее в определенное посольство [28]. Таким образом, на сегодняшний день эффективность биометрических технологий в разрешении проблем безопасности, стоящих перед современными государствами, представляется спорной. Развитие современных информационных технологий позволяет обойти систему безопасности новых биометрических паспортов, что в свою очередь дополняет повестку дня информационной безопасности, как на национальном, так и на международном уровне.

Информационные вызовы и угрозы, связанные с развитием биометрических технологий

Безусловно, биометрический паспорт сложнее подделать, чем паспорт старого образца без чипа. Однако, как показывает опыт, биометрические технологии оказываются уязвимыми по отношению к хакерским атакам и взлому информации. Таким образом, развитие биотехнологий и их широкое использование во внешнеполитической практике государств дополняет повестку дня международной информационной безопасности [11].

В 2006 г. эксперты по компьютерной безопасности и журналист газеты «The Guardian» взломали чип нового британского биометрического паспорта и получили доступ к хранящейся на нем информации [10]. В этом же году немецкий хакер Люкас Грюнвальд за две недели не только взломал чип биометрического паспорта гражданина США, но и клонировал его. Он же доказал, что на чип можно записать любую произвольную информацию или полностью заблокировать его [14].

В марте 2007 г. хакеры из Великобритании за 15 минут взломали и скопировали британский биометрический паспорт, а затем в течение 48 часов полностью расшифровали данные чипа. В 2008 г. голландский учёный Йерун ван Бек по заказу британской газеты «The Times» клонировал чипы британских паспортов, принадлежащих ребенку и 36-летней женщине, и записал на копиях чипов новые данные и фотографии Усамы бен Ладена и палестинской террористки-смертницы Хибы Дарагме. Компьютерная программа сканирования паспортов в международном аэропорту Лондона, рекомендованная для проверки паспортов, идентифицировала их как настоящие. Самое интересное, что британские пограничники даже не взглянули на фотографии в паспорте, целиком доверившись технике [7].

В 2009 г. группа американских исследователей с помощью промышленного сканера RFID-чипов за 20 минут дистанционно просканировала и скопировала биометрический паспорт случайного прохожего. В 2010 году немецкие хакеры из клуба «Chaos Computer» в домашних условиях с помощью специального сканнера извлекли из встроенного в паспорта RFID чипа информацию, включая дополнительную информацию об отпечатках пальцев, и 6-значный код, который используется в качестве цифровой подписи к официальным документам [15].

Таким образом, развитие информационных технологий, которые могут быть использованы как транснациональными террористическими, так и преступными организациями, потенциально создает новое измерение угроз, связанное с широким использованием биометрических технологий во внешнеполитической практике государств. Вместе с тем, уязвимость био-метрических паспортов для кибер-преступников и потенциально кибер-террористов – это не единственная проблема, связанная с их широким использованием во внешнеполитической практике. В связи с тем, что новые био-метрические технологии в своем использовании тесно завязаны на информационно-коммуникационные технологии, в результате их широкого распространения возникает целый ряд угроз личностной безопасности.

Угрозы личностной безопасности, связанные с использованием биометрии во внешней политике

Широкое распространение и использование биотехнологий и информационных технологий

во внешнеполитической деятельности государств, и, прежде всего, в консульской работе, создали целый ряд вызовов и угроз личностной безопасности, в числе которых:

1. *Возможность тотального контроля.* По мнению правозащитников, биометрические технологии по-новому ставят вопрос о правах человека. Их общую позицию высказал бывший генеральный директор Международной организации по миграции Б. Маккинли: «Однажды может случиться так, что мы будем носить с собой документ, который позволит отследить все наши передвижения, правительство будет знать всё, что мы делаем, кто наши друзья и что угодно ещё. Данная технология может стать своего рода орудием тотального контроля. Это политическая проблема, и над ней необходимо работать»[17].

2. *Каждый гражданин, желающий получить визу, рассматривается как потенциальный террорист.* При этом, как считает ряд исследователей, создается презумпция виновности, когда каждый пересекающий границу человек обязан пройти унизительную процедуру сдачи отпечатков пальцев, чтобы доказать, что он не преступник. В случае искажения конфиденциальной информации о человеке в результате сбоя, вирусной атаки или умышленных действий третьих лиц, человек будет навсегда отказано в визе и он будет вынужден собирать доказательства своей невиновности. В 2004 г., например, агентами ФБР был задержан Б. Мэйфилд, чьи отпечатки пальцев по ошибке посчитали идентичными отпечаткам одного из подозреваемых в осуществлении взрыва поезда в Мадриде. В результате была брошена тень на репутацию невинного человека [20].

3. *Отказ в выдаче виз инвалидам,* не имеющим возможности предоставить отпечатки пальцев. Так, например, Великобритания отказала в предоставлении визы для безрукого гражданина Казахстана, аргументировав свое решение тем, что у него «нет отпечатков пальцев» [9].

4. *Вмешательство в частную жизнь граждан.* Биометрическая информация – это не просто конфиденциальная информация. По биометрическим данным человека специалисты могут определить состояние здоровья индивида, выявить врожденные или приобретенные болезни, объективно судить о некоторых способностях и наклонностях человека, которые можно использовать в различных целях: от заключения медицинской страховки до дискриминации при приеме на работу и шантажа.

5. *Проблема сохранности баз биометрических данных граждан.* Известны многочисленные случаи взлома таких баз хакерами и кражи баз данных чиновниками. Так, например, чиновник из израильского министерства социального обеспечения похитил в 2006 г. биометрические сведения девяти миллионов гражданах страны и продал данную информацию еврейскому преступному сообществу [13].

Участившиеся случаи «краж личности» представляют реальную опасность, когда мошенник присваивает себе любой набор из важных данных личности – имя и дату рождения, место проживания, номера паспорта, карточки медицинского страхования, отпечатки пальцев и т. д. – и может использовать эти данные в преступных целях, например, для доступа к финансовой информации и пр.

6. *Влияние биометрических технологий на здоровье человека.* Считается, что процедура сканирования сетчатки глаза безопасна. По мнению врачей-офтальмологов это не так: «сканирование сетчатки происходит с помощью инфракрасного света низкой интенсивности. Эти тепловые лучи поглощаются роговицей и хрусталиком лишь частично, и значительное их количество все-таки попадает на сетчатку. В зависимости от продолжительности и интенсивности такого воздействия, сетчатка может быть повреждена, что может привести к ухудшению зрения [3].

7. *«Чипизация граждан».* Биометрические технологии дали зеленый свет вживлению идентификационных чипов непосредственно в тело человека, что дает возможность не только контролировать чипированный объект, но потенциально и управлять им. В США, например, чипы в тело граждан вшиваются в рамках обязательного медицинского страхования [22] и в рамках социальных программ чипизации местного населения [23]. Данная процедура начинает приобретать уже глобальные масштабы. Комиссия Евросоюза 16 марта 2005 г. одобрила Заключение № 20 Европейской группы по этике в науке и новых технологиях, в которой, в частности, отмечается, что использование электронных имплантантов для слежки за людьми возможен, если такой контроль будет закреплен законодательно [26].

Получается, что кроме заявленных целей политиков – обеспечение безопасности государства – использование механизмов биополитики привело к ограничению неприкосновенности личной жизни и персональных данных граждан, к нарастающему присутствию государства в жизни гражданского общества. При этом переход на биометрические документы происходит без учета позиций гражданского общества, протесты, как правило, не принимаются во внимание, что обусловлено тем, что государственная безопасность ставится выше личностной. Подобная тенденция является достаточно распространенной и в других областях мировой политики [21]. В октябре 2013 г. гражданин Германии М.Шварц обратился в суд ЕС, после того, как ему отказали в выдаче паспорта без обязательной процедуры сдачи отпечатков пальцев. Суд признал, что сдача и хранение отпечатков идет вразрез с основными правами и свободами, представляя угрозу для частной жизни и сохранности персональных данных, однако цель повышения уровня безопасности оправдывает подобные меры [19].

Несмотря на то, что на законодательном международном уровне практически отсутствует специальные нормативные акты, регулирующие правовые принципы применения биометрии относительно прав и свобод человека, активно развиваются технологические аспекты ее использования. Более того, в будущем влияние биометрии будет только расти. Многие страны поставили себе цель собрать биометрические данные на каждого жителя планеты. Профессор, заведующий кафедрой МГТУ им. Баумана И.Спиридонов отмечает: «США перешли на всеобщую биометрическую регистрацию своих граждан, а ФБР приступило к созданию специального биометрического банка данных. Причем цель здесь действительно глобальная – получить биометрические данные на максимально большое число жителей всей Земли» [18]. Пентагон, например, в рамках новой программы Defense Cross-Domain Analytical Capability планирует разработать защищенную облачную базу данных для хранения всей собранной биометрической информации, с помощью которой можно будет идентифицировать человека в любой точке мира и в любом месте [2]. Причем сбор американцами биометрических данных граждан происходит не только легальными, но и нелегальными средствами [8].

Компания по вживлению чипов в тело человека будет набирать обороты во всем мире, пропаганда вживления имплантантов приобретет небывалый размах. Уже сейчас за чипизацию людей выступают и российские политики, в Санкт-Петербурге агитируют за чипизацию детей [1]. Реформа здравоохранения в России предусматривает, в частности, создание единого национального идентификатора пациентов, общей электронной базы данных, необходимых для чипизации, которая, судя по всему, будет проходить по американскому сценарию. Это самый негативный вариант развития биотехнологий, поскольку в данном случае станет реальной угроза безопасности не только биообъектам, но и суверенным государствам. Чипированные граждане будут связаны подобно всемирной паутине – интернету, которым пользуются все, однако ключевые инструменты управления сконцентрированы в США[11].

Очевидно, что за использованием биометрических технологий необходим контроль институтов гражданского общества, причем на международном уровне. В этих условиях возрастает востребованность т.н. многоуровневой дипломатии или многосторонних партнерств, которые позволят всем участникам политического процесса контролировать действия не только государств, но и науки и бизнеса, обеспечить механизмы контроля за этическими аспектами внедрения чипов в тело человека. Как известно, любая технология не является нейтральной с этической точки зрения, а последствия ее использования зависят от более широкого политического контекста. Для достижения максимальных преимуществ от использования биометрических технологий во внешней политике государств и международной практике необходимо сформировать такие многосторонние механизмы взаимодействия, которые учитывали бы не только соображения национальной и международной безопасности, но и личностной. Как представляется, обеспечить подобное регулирование новых технологий можно за счет многосторонних партнерств, в работе которых принимали бы участие не только государства, но и представители гражданского общества, бизнеса и исследовательского сообщества.

Список литературы

1. 5 канал телевидения Санкт-Петербурга. URL: http://www.youtube.com/watch?v=PXZkwSj8vfY. (дата обращения- 14.07.2014).
2. Агенты Пентагона опознают человека в любом уголке мира. URL: http://rnd.cnews.ru/tech/news/top/index_science.shtml?2013/06/03/530736. (дата обращения- 05.04.2014).
3. Балуев Д. Понятие human security в современной политологии // Международные процессы. 2003. № 1. С. 99-105. URL: http://www.intertrends.ru/one/008.htm
4. Безопасность человека в контексте международной политики: вопросы теории и практики. Материалы научного семинара. / Под ред. П.А. Цыганкова. М.: МГУ, 2011.
5. Биометрический паспорт – иметь или не иметь? URL: http://www.mignews.com/news/analitic/world/090713_141156_57386.html (дата обращения- 12.01.2014).
6. Биометрический паспорт можно украсть дистанционно. URL: http://www.pravda.ru/society/how/defendrights/06-02-2009/300968-rfid-0/. (дата обращения- 01.07.2014).
7. Биометрия: мечты становятся явью, или превращаются в кошмар? URL: http://mixednews.ru/archives/4424. (дата обращения- 18.03.2014).
8. Британия не дала визу безрукому казахстанцу – нет отпечатков пальцев. URL: http://www.profi-forex.org/novosti-mira/novosti-evropy/united_kingdom/entry1008162721.html. (дата обращения- 07.05.2014).
9. Британские журналисты взломали чип биометрического паспорта . URL: http://ecoteco.ru/news/n1328/. (дата обращения- 14.03/2014).
10. Зиновьева Е.С. Международная информационная безопасность. М.: МГИМО, 2014.
11. Зиновьева Е.С. Международное управление интернетом: конфликт и сотрудничество. М.: МГИМО, 2011.

12. Личная информация 9 млн. израильтян похищена из реестра населения страны. URL: http://www.securitylab.ru/news/409004.php. (дата обращения- 25.10.2014).
13. На defcon продемонстрировали возможность клонирования электронных паспортов. URL: http://www.securitylab.ru/news/271572.php. (дата обращения- 23.07.2014).
14. Немецкие хакеры взломали новые паспорта. URL: http://www.itsec.ru/newstext.php?news_id=69962. (дата обращения- 14.05.2014).
15. Орехова С.Н. Загранпаспорт с электронной начинкой. М., Технологии и право, 2003.
16. Руководитель международной организации по миграции подчеркивает важную роль биометрических паспортов в регулировании миграционных потоков. URL: http://www.secuteck.ru/newstext.php?news_id=49735. (дата обращения- 01.08.2014).
17. Спиридонов И. Умный паспорт // Российская газета. Неделя № 4989 (165).
18. Суд ЕС признал законным внесение в биометрические паспорта сведений об отпечатках пальцев. URL: http://www.biometrics.ru/news/sud_es_priznal_zakonnim_vnesenie_v_biometricheskie_pasporta_svedenii_ob_otpechatkah_palcev/(дата обращения- 18.03.2014).
19. Суд Орегона признал «Патриотический акт» антиконституционным. URL: http: http://lenta.ru/news/2007/09/27/unlawful/.(дата обращения- 05.09.2014).
20. Харкевич М.В. Усиление государства через его онтологическое ослабление. // Полис. 2012. № 5. С. 122- 129.
21. Чипизация в США: начало положено. URL: http://www.martime.com.ua/news/225/3852/.(дата обращения- 02.04.2014).
22. Школьникам Вайоминга начинают вживлять чипы. URL: http://www.parsec.ru/novosti/shkolnikam-vaiominga-nachinayut-vjivlyat-chipy. (дата обращения- 06.11.2014).
23. Barnett J., Adger W. Climate change, human security and violent conflict //Political geography. 2007. №. 6. Pp. 639-655.
24. Biometrics Deployment of Machine Readable Travel Documents: Technical Report, Version 2.0. ICAO, 2004.
25. Opinion on Ethical Aspects of Patenting Inventions Involving Human Stem Cells. URL: http://europa.eu.int/comm/european_group_ethics/docs/avis16_en.pdf. (дата обращения- 05.04.2014).
26. Paris R. Human security: Paradigm shift or hot air? // International security. 2001. №. 2. Pp. 87-102.
27. Students breach security in passport chips URL: http.//www.expatica.com/nl/news/local_news/RNW-Press-Review_-Tuesday-8-April-2008-.html (дата обращения - 03.05.2014).

Об авторах

Зиновьева Елена Сергеевна – к.полит.н., доцент кафедры мировых политических процессов МГИМО МИД России. 119454, Москва, проспект Вернадского, 76. E-mail: Zinovjeva@mail.ru
Войтенко Юрий Иванович – соискатель кафедры мировых политических процессов МГИМО МИД России, советник Консульского департамента МИД России. 119200 Москва, Смоленская-Сенная пл., 32/34. E-mail: y.voytenko@dks.ru

EVOLUTION OF BIOTECHNOLOGY AND INFORMATION TECHNOLOGY AND ITS IMPACT ON HUMAN SECURITY

E.S. Zinovieva, Yu.I. Vojtenko

Moscow State Institute of International Relations (University), 76 Prospect Vernadskogo, Moscow, 119454, Russia.
Ministry of Foreign Affairs of Russia, 119200, Smolenskaya-Sennaya pl., 32/34.

Abstract: *The development of post-industrial society initiates profound economic, technological and cultural change in the way of life of all mankind. The revolutionary breakthroughs in the field of new technologies such as biotechnology and information technology are reflected in all spheres of human activity, directly affecting the human security.*

The article analyzes the consequences of widespread usage biotechnology and information technology in the foreign policy practice on the basis of the human security theory. The detailed description of the main directions of the use of biometric technology in the foreign policy and consular practices is provided, the challenges and threats to information security associated with biometrics are analyzed, arising from widespread biotechnology are the main challenges and threats to as well as human security threats arising at the present stage of development and application of these technologies. Human security threats

associated with the use of biotechnology are placed in the broader context of global trends in scientific and technological development. The recommendations are formulated in the field of foreign policy and international cooperation, which would neutralize new threats to international and personal safety arising at the present stage of development of biotechnology.

The authors conclude that in order to ensure ethical regulation of new technologies that address issues of human security, it is necessary to organize multi-stakeholder partnerships at national and international level with the participation of states, representatives of civil society, business and the research community.

Key words: biometric technology, information technology, foreign policy, international security, human security.

References

1. 5 kanal televidenija Sankt-Peterburga. [5th TV Channel of Saint-Petersburg] URL: http://www.youtube.com/watch?v=PXZkwSj8vfY. (last accessed 14.07.2014).
2. Agenty Pentagona opoznajut cheloveka v ljubom ugolke mira. [Pentagon Agents can identify any person anywhere] URL: http://rnd.cnews.ru/tech/news/top/index_science.shtml?2013/06/03/530736. (last accessed 05.04.2014).
3. Baluev D. Ponjatie human security v sovremennoj politologii [The concept of human security in the contemporary Political Science] // Mezhdunarodnye processy. 2003. № 1. C. 99-105. URL: http://www.intertrends.ru/one/008.htm
4. Bezopasnost' cheloveka v kontekste mezhdunarodnoj politiki: voprosy teorii i praktiki. Materialy nauchnogo seminara [Human security in the context of international affairs: theory and practice. Materials of the scientific seminar] / Ed by. P.A. Tsygankov. M.: MGU, 2011.
5. Biometricheskij pasport – imet' ili ne imet'? [Is biometric passport worth having?] URL: http://www.mignews.com/news/analitic/world/090713_141156_57386.html (last accessed 12.01.2014).
6. Biometricheskij pasport mozhno ukrast' distancionno. [Biometric passport can be issued distantly] URL: http://www.pravda.ru/society/how/defendrights/06-02-2009/300968-rfid-0/. (last accessed 01.07.2014).
7. Biometrija: mechty stanovjatsja jav'ju, ili prevrashhajutsja v koshmar? [Biometrics: a dream or a nightmare?] URL: http://mixednews.ru/archives/4424. (last accessed 18.03.2014).
8. Britanija ne dala vizu bezrukomu kazahstancu – net otpechatkov pal'cev. [Great Britain refused visa to the armless Kazakhstan citizen because hee couldn't provide fingerprints] URL: http://www.profi-forex.org/novosti-mira/novosti-evropy/united_kingdom/entry1008162721.html. (last accessed 07.05.2014).
9. Britanskie zhurnalisty vzlomali chip biometricheskogo pasporta. [British journalists hacked the biometric passport chip] URL: http://ecoteco.ru/news/n1328/. (last accessed 14.03/2014).
10. Zinov'eva E.S. Mezhdunarodnaja informacionnaja bezopasnost'. [International information security] M.: MGIMO, 2014.
11. Zinov'eva E.S. Mezhdunarodnoe upravlenie internetom: konflikt i sotrudnichestvo. [International Internet governance: conflict and cooperation] M.: MGIMO, 2011.
12. Lichnaja informacija 9 mln. izrail'tjan pohishhena iz reestra naselenija strany. [Private information of 9 mln Israelis was stilen from the roster of the country's population] URL: http://www.securitylab.ru/news/409004.php. (last accessed 25.10.2014).
13. Na defcon prodemonstrirovali vozmozhnost' klonirovanija jelektronnyh pasportov. [The possibility to clone electronic passports was dedmonstrated at defcon] URL: http://www.securitylab.ru/news/271572.php. (last accessed 23.07.2014).
14. Nemeckie hakery vzlomali novye pasporta. [German hackers hacked new passports] URL: http://www.itsec.ru/newstext.php?news_id=69962. (last accessed 14.05.2014).
15. Orehova S.N. Zagranpasport s jelektronnoj nachinkoj. [Electronic foreign passports] M., Tehnologii i pravo, 2003.
16. Rukovoditel' mezhdunarodnoj organizacii po migracii podcherkivaet vazhnuju rol' biometricheskih pasportov v regulirovanii migracionnyh potokov. [The head of the IOM stressed the important role of biometric passports in regulating migration] URL: http://www.secuteck.ru/newstext.php?news_id=49735. (last accessed 01.08.2014).
17. Spiridonov I. Umnyj passport [Smart passport] // Rossijskaja gazeta. Nedelja № 4989 (165).
18. Sud ES priznal zakonnym vnesenie v biometricheskie pasporta svedenij ob otpechatkah pal'cev. [The Court EU approved the inclusion of the fingerprints into biometric passports] URL: http://www.biometrics.ru/news/sud_es_priznal_zakonnim_vnesenie_v_biometricheskie_pasporta_svedenii_ob_otpechatkah_palcev/ (last accessed 18.03.2014).

19. Sud Oregona priznal «Patrioticheskij akt» antikonstitucionnym. [The Court of Oregon declared Patriot Act as unconstitutional] URL: http: http://lenta.ru/news/2007/09/27/unlawful/.(last accessed 05.09.2014).
20. Kharkevich M.V. Usilenie gosudarstva cherez ego ontologicheskoe oslablenie [Strengthening of the state through its ontological weakening] // Polis. 2012. № 5. P. 122- 129.
21. Chipizacija v SSHA: nachalo polozheno. [The introduction of personal chips in USA has started] URL: http://www.martime.com.ua/news/225/3852/.(last accessed 02.04.2014).
22. Shkol'nikam Vajominga nachinajut vzhivljat' chipy. [Chips are to be implanted to the schoolchildren at Wyoming] URL: http://www.parsec.ru/novosti/shkolnikam-vaiominga-nachinayut-vjivlyat-chipy. (last accessed 06.11.2014).
23. Barnett J., Adger W. Climate change, human security and violent conflict //Political geography. 2007. №. 6. Pp. 639-655.
24. Biometrics Deployment of Machine Readable Travel Documents: Technical Report, Version 2.0. ICAO, 2004.
25. Opinion on Ethical Aspects of Patenting Inventions Involving Human Stem Cells. URL: http://europa.eu.int/comm/european_group_ethics/docs/avis16_en.pdf. (last accessed 05.04.2014).
26. Paris R. Human security: Paradigm shift or hot air? // International security. 2001. №. 2. Pp. 87-102.
27. Students breach security in passport chips URL: http.//www.expatica.com/nl/news/local_news/RNW-Press-Review_-Tuesday-8-April-2008-.html (дата обращения - 03.05.2014).

About authors

Elena S. Zinovieva – PhD in Political Science (kandidat nauk), associate professor at the Department of World Politics, MGIMO-University. Prospect Vernadskogo, 76, Moscow, 119454, Russia. E-mail: zinovjeva@mail.ru
Yuriy I. Vojtenko – PhD student MGIMO-University, Counselor at the Consular Department, Ministry of Foreign Affairs of Russia, 119200, Smolenskaya-Sennaya pl., 32/34. E-mail: y.voytenko@dks.ru