УДК 316.774:351.746(5) + 327.2:004.77(7) **Г. Н. Валиахметова**

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АЗИИ

Статья посвящена анализу проблем, связанных с обеспечением информационной и кибербезопасности в странах Азии. В цифровую эпоху геополитическое пространство Азии становится полем масштабного информационного противостояния и кибервойн между США и новыми азиатскими центрами глобального влияния. Ведущие державы Азии активно включаются в процесс формирования международного режима информационной защищенности. Исследование выполнено в рамках междисциплинарного подхода. Автор провел сравнительный анализ позиций российских и зарубежных экспертных сообществ в области востоковедения, информационных технологий, международных отношений и безопасности.

Ключевые слова: Азия, Китай, Ближний Восток, США, информационная безопасность, кибербезопасность, угрозы, информационная война, управление Интернетом.

Стремительное развитие информационных и телекоммуникационных технологий (ИКТ) создает множество проблем в сфере международной и национальной безопасности. Информационное противостояние становится важной компонентой мировой политики. В процесс трансформации системы международных отношений и формирования новой безопасной среды обитания все более активно включаются азиатские государства и, несмотря на издержки «догоняющего» развития, образуют новые глобальные центры силы, способные бросить вызов США, в том числе в области глобального информационного превосходства. Соответственно геополитическое пространство Азии, сохраняя статус одного из главных мировых очагов международных и этноконфессиональных конфликтов, становится полем масштабных информационных столкновений.

Проблемы информационной безопасности появились в международно-политической и академической повестке дня после окончания холодной войны в результате изменения геополитической ситуации и информационной революции. Первоначально термин «информационная безопасность» использовался для обозначения проблем, порождаемых компьютерными сетями. Впоследствии он приобрел более широкий смысл, выходящий за рамки исключительно технологической сферы. На сегодняшний день единый понятийный аппарат в области международной информационной безопасности пока не выработан в связи с расхождениями в подходах государств к определению угроз в сфере ИКТ, подлежащих урегулированию на международном уровне.

Западный (США и страны ЕС) подход фактически сводит вопросы информационной безопасности к техническим проблемам контроля и соблюдения законности и правопорядка в телекоммуникационной сфере (защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, компьютерных вирусов и вредоносных программ и т. п.). Однако преимущественное использование приставки «кибер» выносит за скобки, например, проблемы призыва к терроризму и экстремизму в содержании контента. Исследователи

© Валиахметова Г. Н., 2015

и дипломаты России и стран Азии придерживаются расширительного подхода, разделяя информационную безопасность в соответствии с видами угроз на информационно-техническую (кибербезопасность) и информационно-социальную. Например, противодействие распространению идеологии терроризма через Интернет не входит в угрозы технического характера, но включено в понятие информационно-социальной безопасности, которая предполагает защиту психологического состояния общества и государства от негативного информационного воздействия. Российский подход к рассмотрению проблем международной информационной безопасности в контексте так называемой триады угроз (террористической, военной и криминальной) во многом перекликается с позицией экспертов ООН, которые выделяют три вида угроз: киберпреступность, кибертерроризм и использование информационного пространства в военно-политических целях [4; 6, *218*; 9, *196–201*].

В мировом экспертом сообществе нет единства и в вопросе об определении термина «информационная война», под которой в целом понимается стратегическое межгосударственное противоборство в информационном пространстве в форме борьбы с системами управления противника, а также в форме информационно-разведывательной, электронной, хакерской, кибернетической, экономической и психологической войны [5, *41–43*; 17].

Американские эксперты выделяют два типа стратегических информационных войн — первого и второго поколения. Война первого поколения (по сути кибервойна) понимается как комплексное информационное воздействие на систему государственного и военного управления противника с одновременным обеспечением надежной защитой собственной национальной информационной инфраструктуры. Инструментом ведения такой войны является кибероружие — совокупность новейших ИКТ и средств, которые позволяют получить несанкционированный доступ к информации и целенаправленно ее видоизменять (искажать, блокировать, копировать, уничтожать), преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, технических средств, компьютерных систем и информационно-коммуникационных сетей. Как и ядерное, информационное оружие может служить и для политического давления, и для сдерживания, обеспечивая политическое и военно-стратегическое преимущество над государствами, у которых его нет. На 2005 г. разработками в области информационного оружия занимались более 120 стран [5, *41–43*; 6, *218–219*; 17].

По мнению Вашингтона, наибольшую опасность для национального информационного пространства и информационной инфраструктуры США представляет Китай, который, по оценкам большинства экспертов мира, с внушительным отрывом лидирует в списке стран, осуществляющих хакерские атаки, кибершпионаж и распространение вредоносных программ [7, *169*; 12]. Так, беспрецедентное по масштабам каскадное отключение электроэнергии на северо-западе США в 2003 г., в результате которого пострадали около 50 млн человек в штатах Огайо, Нью-Йорк, Мичиган, а также в некоторых штатах Канады, было вызвано хакерской атакой. Спецслужбы США уверены, что за этой акцией стоял Пекин,

испытывавший возможности своих киберподразделений, специализирующихся на кибервойнах и способных при необходимости вывести из строя большинство объектов информационной инфраструктуры США. Другим примером может служить крупный скандал 2009 г., разгоревшийся после взлома китайскими хакерами учетных записей сотен пользователей, в том числе высокопоставленных американских чиновников, почтового сервиса Gmail компании Google [7, *169, 176*; 13].

Объектами кибершпионажа и хакерских атак с территории КНР становятся не только оппоненты Пекина на Западе, но и страны-конкуренты по восточноазиатскому региону, причем зачастую инициатива исходит от негосударственных акторов. Именно они сыграли ключевую роль в организации первой кибервойны против Индонезии в 1997–1998 гг. Поводом послужили антикитайские погромы, вспыхнувшие в связи с тем, что после азиатского финансово-экономического кризиса проживающие в Индонезии выходцы из Китая (хуацяо) практически полностью взяли под свой контроль распределение продовольствия на большей части страны. Джакарта обвинила власти КНР в организации кибератак на индонезийские правительственные сайты, их пик пришелся на национальный праздник Индонезии — День независимости (17 августа) [7, *177*]. Примечательно, что сама Индонезия прочно занимает второе после Китая место в мире по числу проведенных с ее территории кибератак. В первой десятке подобных стран также фигурируют такие азиатские государства, как Турция, Индия и Тайвань [12].

Следует отметить, что сам Китай весьма скромно оценивает собственные достижения в киберпространстве, подчеркивая, что кибербезопасность страны значительно уступает информационной защищенности ведущих мировых держав. Действительно, в мировом Индексе кибермогущества 2010–2011 гг. Китай занял лишь 13-е место, а в рейтинге стран с наиболее развитым сектором ИКТ — лишь 36-е [7, *169*]. Слабым звеном киберстратегии КНР является неспособность самостоятельно создавать новые технологии, а традиционная для Китая практика копирования и доработки иностранных технологий, по сути, удерживает страну в рамках «догоняющей» модели развития. Поэтому в последнее десятилетие приоритетным направлением инновационного развития КНР стала реализация собственных проектов в области ИКТ, а собственные китайские разработки благодаря своей относительной дешевизне уверенно завоевывают мировой рынок, что позволяет экспертам говорить о высоком потенциале Китая в сфере проведения операций в киберпространстве [7, *169–170*; 13]. Именно по этой причине Вашингтон считает постоянный рост импорта китайских микросхем в США серьезной угрозой национальной безопасности и стремится ужесточить контроль над поставками высокотехнологичной продукции из-за рубежа, в первую очередь из Китая [5, *53*; 13].

Кибервойны стали актуальны и для Ближнего Востока. Летом 2010 г. был обнаружен компьютерный вирус Stuxnet, который вывел из строя около 1 тыс. центрифуг на заводе по обогащению урана в Натанзе (Иран). К концу 2010 г. в мире насчитывалось уже порядка 100 тыс. компьютеров, зараженных этим вирусом, причем в основном в странах Азии — Иране (58,3 %), Индонезии (17,8 %) и Индии (10 %), а также в Пакистане и на Филиппинах [11, *234*]. Stuxnet — это

кибероружие, имеющее колоссальную разрушительную мощь, теоретически сравнимую с оружием массового уничтожения. Некоторые эксперты сравнивают произведенный Stuxnet эффект с атакой на Перл-Харбор и первыми ядерными взрывами в Хиросиме и Нагасаки. Вместе с тем на сегодняшний день вопрос о том, кем и для каких целей он был создан, так и остается открытым. Теоретически мотивы и возможности для создания подобного вируса имели не только государственные акторы (в числе потенциальных заказчиков упоминаются США, Израиль и даже Китай), но и частные компании (в первую очередь конкуренты Siemens в сфере поставок программного оборудования для систем управления на АЭС и крупных добывающих производств в Азии), а также неправительственные организации (в частности, экологическая «Гринпис»). Иными словами, в мировом экспертном сообществе нет единого мнения по вопросу о том, была ли кибератака Stuxnet частью кибервойны, кибертерроризма, киберпреступности или кибервандализма. Вместе с тем обнаружение вируса Stuxnet вызвало серьезную озабоченность мирового сообщества возможностью повторения подобных инцидентов на других ядерных и крупных промышленных объектах мира и поставило в международную повестку дня вопрос их киберзащиты [10; 11, *233–239*].

В мае 2012 г. Иран снова стал объектом кибератаки, предположительно со стороны разведывательных структур США и Израиля, которым эксперты приписывают авторство в создании сложной вредоносной программы Flame. Предполагается, что вирус был нацелен на похищение промышленной информации с правительственных компьютеров в Иране и ряде других ближневосточных стран [1].

Информационная война второго поколения — это манипулирование общественным сознанием и дестабилизация отношений между политическими движениями в целях провокации конфликтов на социальной, политической, национальной и религиозной почве; инициирование забастовок, массовых беспорядков и других акций социально-экономического протеста для формирования политической напряженности и хаоса; дискредитация органов государственного управления в глазах населения; подрыв международного авторитета государства-оппонента и его сотрудничества с другими странами; нанесение ущерба его жизненно важным интересам в различных сферах. Основным инструментарием ведения подобных операций являются национальные и транснациональные средства массовой информации, а также глобальные информационно-коммуникационные сети, посредством которых можно влиять на мировоззрение, политические взгляды, правосознание, менталитет и ценностные установки отдельной личности и общества в целом. Одна из форм ведения информационных войн второго поколения — «культурная экспансия» под лозунгом распространения «западных демократических ценностей», направленная на подрыв гражданского духа, размывание национального суверенитета, культурной и цивилизационной идентичности государств-оппонентов [5, *41–50*;17].

В 2010–2011 гг. Вашингтон озвучил основные направления цифровой дипломатии и стратегии США в глобальном информационном пространстве. В числе обозначенных Белым домом задач значатся дискредитация идеологических

противников США, а также противодействие информационной и внешней культурной политике Китая и Ирана, осуществляемой через Интернет и социальные сети. Приоритетному финансированию подлежат проекты, нацеленные на создание и распространение новых технологий, которые позволят обходить цензуру в сети, а также поддерживать местную оппозицию путем развертывания на территории третьих стран систем теневого Интернета и независимой мобильной связи [6, *214–215*; 14, 15, 18, 19].

Посредством информационных ресурсов Западу неоднократно удавалось сформировать образ КНР как автократии, где права человека жестко ограничиваются (события на площади Тяньаньмэнь 1989 г., в Тибете 2008 г., в Синьцзян-Уйгурском автономном районе 2009 г.). Также показательным стал инцидент с Google, когда весной 2010 г. интернет-поисковик в нарушение своих обязательств перед Пекином отказался фильтровать в сети запросы китайских пользователей, как это предусмотрено законодательством КНР в целях недопущения распространения информации, способной дискредитировать власть. В поддержку Google выступил Белый дом, обвинив Китай в отсутствии демократии и нарушении свободы слова, что осложнило и без того непростые отношения между двумя державами. Политическая подоплека скандала позволила США обрести мощные инструменты сдерживания китайского экспорта (в первую очередь ИКТ) на мировые рынки, а корпорация Google приобрела внушительный административный ресурс в Вашингтоне [7, *175*]. Со своей стороны Китай также широко использует возможности ИКТ для формирования позитивного имиджа страны на международной арене [3; 7, *178–180*].

Полем масштабного информационного противостояния стал арабский мир в период «арабской весны» 2010–2012 гг. В американских и подконтрольных местной оппозиции СМИ там была развернута скоординированная пропагандистская кампания с беспрецедентной критикой «обанкротившихся режимов», зачастую нацеленная на их «обезглавливание» путем моральной и политической дискредитации лидера в глазах местного населения и мирового сообщества (наиболее показательны примеры М. Каддафи в Ливии и Б. Асада в Сирии). Одновременно местному населению настойчиво внушалась мысль о «неизбежности перемен» и готовности Вашингтона оказать финансовую и моральную поддержку «идущим по пути демократии» оппозиционным силам. Особую роль сыграли мировые «независимые» (по сути, подконтрольные США) спутниковые и радиовещательные каналы. Их монополия на освещение событий в регионе в сочетании с информационной блокадой противника обеспечила протестному движению абсолютное информационное превосходство [5, *49–50*]. По иронии судьбы в этой информационной войне на стороне США выступил арабский телеканал «Аль-Джазира», который Белый дом традиционно обвинял в разжигании антиамериканских настроений на Ближнем Востоке и тенденциозной подаче материалов по Афганистану, Ираку и Палестине. Ряд экспертов полагает, что позиция «Аль-Джазиры» в период «арабской весны» была обусловлена некой политической подоплекой, в частности непомерно возросшими региональными амбициями Катара [8].

«Арабское пробуждение» на Ближнем Востоке и в Северной Африке также актуализировало вопрос об эффективности использования потенциала социальных сетей в современных информационных войнах. Для описания и анализа событий «арабской весны» первоначально использовались такие термины, как «твиттер-революции» и «движение "фэйсбуковской" молодежи». Многие обозреватели интерпретировали происходившие события в духе конспирологических версий, как происки Запада, поддерживающего антиправительственные выступления с целью закрепиться в геополитически важном регионе мира. Вместе с тем взгляд на социальные сетевые сервисы как на основную движущую силу арабских революций и версии о наличии в «арабской весне» элемента управления и координации ее событий из Вашингтона не выдержали серьезной критики со стороны ведущих специалистов мирового востоковедческого и айтишного сообщества, в том числе американского. По сути, речь идет о значимом, но не первостепенном или определяющем влиянии социальных медиа на организацию массовых протестов на Арабском Востоке. Вместе с тем эксперты признают, что кибертехнологии могут оказывать деструктивное влияние на международную безопасность в случае их ориентации на подрыв режимов в авторитарных странах, шпионаж и разведку в рамках соответствующего политического курса заинтересованных региональных и внерегиональных игроков [2, *67–74, 83*; 6, *216–217*]. Глобальная сеть, кроме того, может не только выступать в качестве эффективного инструмента демократизации, но и способствовать усилению авторитарных тенденций, ограничивающих свободу граждан, поскольку сервисы Web 2.0 предоставляют новые возможности не только прозападно ориентированным группам, но и радикально-экстремистским организациям, о чем свидетельствует, в частности, появление в Интернете многочисленных сайтов исламистских радикальных организаций, призывающих к участию в так называемом всемирном джихаде.

Наглядным примером информационных войн второго поколения также могут служить иракский кризис 2003 г., ливийская кампания 2011 г., кризис вокруг ядерных программ Ирана и КНДР, текущий сирийский кризис, многолетнее информационное противостояние по линии Запад — исламский мир и т. д.

Вашингтон отводит Интернету роль мощного стратегического оружия и в вопросах контроля над ним своими главными соперниками считает Китай и Россию. По мнению американских экспертов, эти две страны могут пойти по пути фрагментации глобального информационного пространства, что очевидно противоречит интересам США в области национальной безопасности [9, *186–200*; 16]. Неприятие Китаем существующего международного режима управления Интернетом обусловлено тем, что основные функции по присвоению имен и адресов закреплены за подотчетной США Корпорацией по распределению имен и адресов (ICANN). Китайская критика в отношении ICANN особенно усилилась после выдачи домена .tw Тайваню, который рассматривается Пекином как составная часть КНР. Пекин призывает распустить действующую, по его мнению, в американских интересах корпорацию и сформировать под эгидой ООН подлинно международную организацию для управления Интернетом. В отсутствие таковой Китай предлагает создать альтернативные системы доменных имен — DNS-расширения

для автономного Интернета, функционирующего в рамках одной страны, что позволит усилить контроль государств над местными сегментами глобальной сети и механизмами глобального управления Интернетом. Международными площадками, где КНР и Россия ставят на обсуждение подобные проблемы, являются Генеральная Ассамблея ООН и саммиты ШОС [3; 7, *177–178*; 16].

Горячие дискуссии на данную тему в новом ключе поставили вопрос о соблюдении принципа суверенитета государства в эпоху ИКТ. С одной стороны, международное право признает недопустимым вмешательство во внутренние дела любой страны. Поэтому никто не оспаривает легитимность действий государств, которые из опасений вмешательства в свои внутренние дела со стороны определенных стран или международных организаций, в том числе под предлогами гуманитарного характера, накладывают определенные ограничения на доступ в Интернет и распространение информации в Сети в пределах своей территории. Примечательно, что регулярные попытки заблокировать доступ к сервисам Facebook, YouTube, Blogspot имеют место не только в странах преимущественно авторитарного типа (Китай, Вьетнам, Иран, Саудовская Аравия, Египет, Пакистан, Мьянма, Северная Корея), но и в таких демократических государствах, как Сингапур [6, *220–221*; 9, *204*; 16]. Оставаясь в рамках действующего международно-правового поля, крупные интернет-корпорации (Google, Yahoo! и др.) сотрудничают с авторитарными режимами, предоставляя местным властям конфиденциальную информацию о своих пользователях и блокируя определенные типы поисковых запросов [3; 6, *219*]. Примером масштабного целенаправленного отключения Интернета на территории суверенного государства стал Египет, где весной 2011 г. по настоятельной просьбе правительства компании отключили доступ к глобальной сети с мобильных устройств [9, *203–205*].

С другой стороны, в подобной ситуации возникает опасность распада глобального информационного пространства на несколько самостоятельных систем. Вопрос об обоснованности подобных опасений остается открытым, поскольку, например, Пекину удается контролировать содержание масштабного китайского сегмента глобальной сети (цензура контента, фильтрация трафика, блокирование иностранных социальных веб-сервисов Facebook, Twitter, Livejournal и т. д.), придерживаясь при этом открытой модели развития. На сегодняшний день Китай стабильно удерживает первое место в мире по общему числу и темпам роста интернет-пользователей [3; 7, *178–180*].

Очевидно, что в условиях глобализации и динамичного развития ИКТ ни одно государство не может в одиночку обеспечить безопасность национального информационного пространства, однако механизмы предотвращения и парирования подобных угроз пока находятся на начальной стадии формирования. Государства Азии активно включаются в процесс строительства здания международного режима информационной безопасности. Их разногласия с Западом в этой сфере обусловлены разными доктринальными и правовыми подходами, а также логикой развития современного мирового политического процесса, характерной чертой которого является соперничество за глобальное и региональное лидерство, неизбежное в условиях незавершенности трансформации системы международных

отношений. Сегодня оппоненты уже готовы сотрудничать в таких сферах, как противодействие терроризму и преступной деятельности в Интернете, а также в решении проблем, связанных с мошенничеством с кредитными картами, детской порнографией, пропагандой насилия и нездорового образа жизни и т. д. Вместе с тем следует признать, что информационное противостояние на геополитическом пространстве Азии усиливает асимметричную составляющую современных конфликтов и способствует росту международной напряженности.

---

1. Громкие случаи кибератак и взломов в мире в 2000–2014 гг. // РИА Новости. 14.08.2014 [Электронный ресурс]. URL: http://ria.ru/spravka/20140814/1019983404.html (дата обращения: 06.09.2014).

2. *Демидов О.* Социальные сетевые сервисы в контексте международной и национальной безопасности // Индекс безопасности. 2013. № 1 (104). С. 65–86.

3. *Евдокимов Е.* Политика Китая в глобальном информационном пространстве // Международные процессы. 2011. Т. 9, № 1 (25) [Электронный ресурс]. URL: http://www.intertrends.ru/twenty-fifth/009.htm (дата обращения: 25.08.2014).

4. *Карасев П. А.* Обеспечение международной информационной безопасности // Политические и военно-экономические аспекты обеспечения международной и региональной безопасности. М., 2012. С. 56–61.

5. *Корсаков Г.* Информационное оружие супердержавы // Пути к миру и безопасности. Вып. 1 (42). М., 2012. С. 34–59.

6. *Зиновьева Е.* Цифровая дипломатия США: возможности и угрозы для международной безопасности // Индекс безопасности. 2013. № 1 (104). С. 213–229.

7. *Ибрагимова Г.* Стратегия КНР в киберпространстве: вопросы управления Интернетом и обеспечения информационной безопасности // Там же. С. 169–184.

8. *Лажми Н.* «Аль-Джазира», или Протестная журналистика // Ближний Восток, Арабское пробуждение и Россия: что дальше? М., 2012. С. 108–116.

9. Международная информационная безопасность и глобальное управление Интернетом: взгляд из Женевы глазами российских и международных экспертов : материалы круглого стола // Индекс безопасности. 2013. № 1 (104). С. 185–206.

10. *Пискунова Н.* Кибербезопасность и атомная энергетика: все еще предстоит // Там же. 2014. № 1 (108). С. 213–218.

11. *Симоненко М.* Stuxnet и ядерное обогащение режима международной информационной безопасности // Там же. 2013. № 1 (104). С. 233–248.

12. Страны, из которых чаще всего совершаются хакерские атаки // Rate I. 17.08.2013 [Электронный ресурс]. URL: http://www.rate1.com.ua/ehkonomika/tekhnologii/2708/ (дата обращения: 06.09.2014).

13. *Юрченко Г.* Киберборьба по взглядам руководства Китая // Военно-политическое обозрение. 18.07.2012 [Электронный ресурс]. URL: http://www.belvpo.com/ru/13593.html (дата обращения: 25.08.2014).

14. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington. Washington D.C.: The White House, May 2011 [Electronic resource]. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf (дата обращения: 06.09.2014).

15. IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy. U. S. Department of State. 2010, Sept. 1 [Electronic resource]. URL: http://www.state.gov/m/irm/rls/148572.htm (дата обращения: 06.09.2014).

16. *Knake R.* Internet Governance in an Age of Cyber Insecurity. N. Y.: Council on Foreign Relations, 2010.

17. *Libicki M.* Cyberdeterrence and Cyberwar. Santa Monica (Calif.): RAND, 2009 [Electronic resource]. URL: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (дата обращения: 6.09.2014).

18. Public Diplomacy: Strengthening U. S. Engagement with the World. A Strategic Approach for the 21st Century, 2010 [Electronic resource]. URL: http://www.carlisle.army.mil/DIME/documents/Public%20Diplomacy%20US%20World%20Engagement.pdf (дата обращения: 6.09.2014).

19. *Rid Th., Hecker M.* War 2.0: Irregular Warfare in the Information Age. Westport (Calif.) : Praeger, 2009.

Рукопись поступила в редакцию 8 сентября 2014 г.

УДК 341 + 316.4.063:339.742(7/8=134)

Ю. С. Безбородов
О. В. Сухова

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ ВАЛЮТНОЙ ИНТЕГРАЦИИ ЛАТИНСКОЙ АМЕРИКИ

В работе анализируются международно-правовые аспекты интеграционных процессов, причем акцент делается на двух различных сторонах интеграции — глобализации и регионализации. Интеграция рассматривается авторами с двух точек зрения — как процесс и как результат. При этом результат интеграции выражается как определенное пространство, территория, на которой протекают интеграционные процессы, и как институциональная система, созданная для управления интеграционными процессами. Авторы указывают на объективный характер тенденции к валютной интеграции государств на примере снижения количества валют в мире. В работе анализируются процессы валютной интеграции Латиноамериканского региона.

Ключевые слова: интеграция, Латинская Америка, международное право, валютная интеграция.

Южная Америка является интересным регионом для изучения международно-правовых аспектов региональных интеграционных процессов. Именно в Южной Америке отчетливо проявляются как интеграционные, так и дезинтеграционные начала (или — на несколько иных уровнях — глобализм и регионализм) в отношениях между государствами этого региона. К способствующим интеграционным процессам характеристикам региона можно отнести относительную изолированность государств от других центров; культурную, историческую, экономическую и правовую общность государств; схожие географические характеристики — такие как наличие выхода к морю, и т. п. К дезинтегрирующим качествам региона можно отнести различия в политическом строе государств региона; орографическую неоднородность региона, заключающуюся в резко различающихся характеристиках рельефа (горы и равнины, например), отказ южноамериканских стран поддерживать НАФТА (хотя этот факт одновременно является интегрирующим фактором, но на региональном уровне) и др.

© Безбородов Ю. С., Сухова О. В., 2015