DOI: 10.17976/jpps/2022.03.09

ЗАЩИТА КИБЕРПРОСТРАНСТВА В СТРАНАХ ЛАТИНСКОЙ АМЕРИКИ

Е.Ю. Косевич

КОСЕВИЧ Екатерина Юрьевна, кандидат политических наук, старший научный сотрудник Международной лаборатории исследований мирового порядка и нового регионализма, Национальный исследовательский университет "Высшая школа экономики"; научный сотрудник Центра политических исследований, Институт Латинской Америки Российской академии наук, Москва, email: ekaterina.kosevich@gmail.com

Косевич Е.Ю. 2022. Защита киберпространства в странах Латинской Америки. *Полис. Политические исследования*. № 3. С. 108-123. https://doi.org/10.17976/jpps/2022.03.09

Исследование осуществлено в рамках Программы индивидуальных исследований факультета мировой экономики и мировой политики НИУ ВШЭ в 2020 г.

Статья поступила в редакцию: 27.09.2019. Принята к публикации: 16.03.2020

Аннотация. Принятие национальной стратегии кибербезопасности является подтверждением осознания страной важности защищенности киберинфраструктуры, цифровой экономики и бизнес-среды, от которых уже в значительной степени зависит информационное и экономическое благополучие. Однако лишь немногие государства Латинской Америки разработали и приняли собственную национальную стратегию в области кибербезопасности. Статья посвящена анализу ключевых аспектов стратегий в области кибербезопасности Колумбии, Парагвая, Коста-Рики, Чили и Мексики. Автор рассматривает их руководящие принципы и цели, а также органы и институты, ответственные за реализацию и мониторинг результатов указанных стратегий. Кроме того, дается характеристика национальной политики кибербезопасности, разработанной в Бразилии – крупнейшей стране Латинской Америки, на долю которой приходится наибольшее число киберпреступлений региона. Особое внимание уделено состоянию отрасли информационных технологий в каждой из этих латиноамериканских стран.

Ключевые слова: Латинская Америка, информационное пространство, кибербезопасность, национальные стратегии кибербезопасности, информационные технологии, интернет, Колумбия, Парагвай, Чили, Коста-Рика, Мексика, Бразилия.

Растущее признание интернета как главной инфраструктуры, обеспечивающей экономическую и социальную сторону жизни, в последние годы привлекло особое внимание к вопросам, связанным с его управлением. Концепт "управление интернетом" включает в себя разработку и применение правительствами, частным сектором, гражданским обществом, а также техническим сообществом соответствующих норм, правил и процедур, обеспечивающих работоспособность, эффективное развитие и безопасное использование Глобальной сети [Кибербезопасность и управление интернетом... 2013; DeNardis, Musiani 2016]. Это понятие охватывает вопросы согласованности действий при обмене информацией через интернет, а также меняющуюся государственную политику в данной области [DeNardis 2009; Mueller 2017].

В научных исследованиях особое внимание уделяется поиску наиболее эффективных форм (многосекторальных или многосторонних) политических решений, касающихся безопасного использования глобальной информационной сети. В этом контексте неоднозначные мнения высказывались по поводу роли, которую должны играть профильные организации, такие как Корпорация по

управлению доменными именами и *IP*-адресами (*ICANN*), Всемирная встреча на высшем уровне по вопросам информационного общества (*WSIS*), организованные под эгидой ООН, а также международный Форум по управлению интернетом (*IGF*) [Де Босси 2005; Dutton 2015]. Вместе с тем в основе широкого понятия "управление интернетом" заложена идея единого процесса [Dutton 2015]. Исследователи сходятся во мнении, что управление интернетом нацелено на решение задач различных видов, а сложный характер взаимодействия ключевых участников, задействованных для поиска оптимальных вариантов, в итоге и поддерживает Глобальную сеть в рабочем состоянии.

Одной из важных составляющих управления интернетом выступает понятие кибербезопасности [Проблемы кибербезопасности... 2006]. Существует множество определений данного термина, но наиболее общей является следующая трактовка: "Кибербезопасность – это совокупность мер и мероприятий, предпринимаемых как юридическими (частными и публичными), так и физическими лицами для уменьшения рисков, с которыми они сталкиваются в киберпространстве, с целью снижения вероятности успешных кибератак" [Lewis 2018]. Подобные действия направлены на противостояние киберугрозам и смягчение киберрисков, однако не способны полностью искоренить их. Несмотря на то, что именно это является главной задачей кибербезопасности, единого мнения относительно правовой, политической и технической областей применения этого явления пока нет [Valenzuela 2017].

Стоит отметить, что концепт *кибербезопасность* включает в себя не только защиту и своевременное реагирование на кибератаки, совершаемые в информационном пространстве, но и разработку, осуществление необходимых мер по предупреждению взлома систем третьими лицами, включая своевременную реакцию на любые угрозы безопасности в интернете, обеспечение защиты идентификационных данных и надлежащее функционирование цифровых устройств. В техническом отношении кибербезопасность – это инструмент, обеспечивающий функционирование инфраструктуры, необходимой для эффективной работы интернета, включая маршрутизацию и проверку подлинности сервера.

В последние десятилетия как в отечественной, так и в зарубежной научной литературе вопросам кибербезопасности и защиты цифрового пространства уделяется значительное внимание [Eriksson, Giacomello 2009; Barnard-Wills, Ashenden 2012; Dunn Cavelty 2015; Шариков 2015; Международная информационная безопасность... 2019]. Современные исследования в области международных отношений и мировой политики, затрагивающие эти темы, можно разделить на четыре основные группы. В первую входят работы, посвященные изучению политики, разработкой которой занимаются специализированные *think tanks*, а также оценке роли международных организаций и программ в области развития информационных технологий [Касенова 2012; Ablon et al. 2014]. Во вторую – исследования, в которых представлен критический анализ отношений между информацией и властью [Day 2001; Морозов 2002; Проблемы информационной безопасности... 2016]. Третья группа включает в себя работы, нацеленные на изучение формирования и развития небезопасной информационной среды с позиций тотального контроля и цензуры [Deibert, Rohozinski 2010; Международная информационная безопасность... 2011; Роговский 2014]. Четвертая группа состоит из научных трудов, в которых анализируются опыт и техника реализации киберугроз [Dunn Cavelty 2008; Паршин и др. 2011; Betz, Stevens 2013].

Консенсус по поводу единых механизмов управления кибербезопасностью, которые на сегодняшний день существенно различаются по странам,

несмотря на тот факт, что киберпространство по своей природе глобально, так и не был достигнут [Казарин, Тарасов 2013]. Все это заставляет задуматься о трактовке информационной безопасности с позиций партнерства при использовании информационной среды на национальном и международном уровнях, а также о целесообразности разработки унифицированных инструментов предотвращения киберугроз.

С технической точки зрения понятие кибербезопасности непосредственно связано с противодействием информационным угрозам и рискам, а также способностью к соответствующим действиям и реакциям на кибератаки, включая кибертерроризм, кибершпионаж, киберпреступность, которые могут исходить как от отдельных хакеров, преступных организаций, так и от государств [Булавин 2014]. Стратегии кибербезопасности тесно связаны с конкретными ситуациями, с которыми сталкиваются все пользователи сети на местном или региональном уровнях. Концепция кибербезопасности должна обеспечивать возможность противостояния конкретным угрозам, наиболее часто возникающим на местном уровне, одновременно будучи интероперабельной и совместимой в глобальном разрезе. А при принятии подобной стратегии государственным органам необходимо учитывать культурные, национально-этнические и политические особенности страны.

При разработке государственной политики в области кибербезопасности следует принять во внимание два компонента: управление рисками и киберустойчивость. Управление рисками – это рациональный и соразмерный подход к обеспечению кибербезопасности, способствующий использованию соответствующих технических инструментов для того, чтобы эффективно справляться с возникающими в киберпространстве опасностями [Марков, Цирлов 2007]. Киберустойчивость отражает способность государственного и частного секторов при возникновении потенциальных атак и угроз их информационной безопасности поддерживать свою целостность и главные функции, а также быстро восстанавливаться после перенесенных нападений [Janczewski, Colarik 2008].

Именно национальные стратегии кибербезопасности призваны стать стратегическим вектором в организации противодействия новейшим информационным угрозам. И несмотря на то, что в научной литературе можно встретить самые разные подходы к содержанию, целям и задачам подобных концептуальных документов, все они сходятся на том, что на практике подобные концепции должны носить комплексный характер, затрагивая самые различные аспекты обеспечения безопасности киберпространства.

В настоящем исследовании автор поставил следующие задачи:

– представить краткий обзор концепций кибербезопасности и киберзащиты, разработанных ведущими латиноамериканскими государствами;

– выявить основные механизмы их реализации, отталкиваясь от следующих критериев: главные цели, которые они преследуют; характер подобных концепций; органы, ответственные за их реализацию.

– определить ключевые особенности национальных стратегий, а также политики кибербезопасности, за счет которых каждое из рассмотренных латиноамериканских государств стремится обеспечить безопасное развитие информационно-коммуникационной инфраструктуры;

– оценить степень их преемственности по отношению к концепциям ведущих западных стран.

Выдвигается гипотеза, что Латинская Америка, социально-политическая и экономическая жизнь которой традиционно характеризуется сплоченностью и взаимозависимостью, выстраивает собственную модель защиты киберпространства в регионе, ориентированную на использование сбалансированной, позитивной и объединительной методики. В основе исследования лежит системный подход с применением сравнительного анализа, а также сочетанием регионального и странового подходов.

Проблемы кибербезопасности не обошли стороной Латинскую Америку, пока еще заметно отстающую от западных стран по уровню внедрения информационных технологий, цифровой трансформации и диджитализации. За последние пять лет количество кибератак в регионе увеличились на 40%, что составляет более 700 млн компьютерных атак ежегодно[1]. Статистика, опубликованная Сетевым информационным центром Латинской Америки и Карибского бассейна (*Latin America and Caribbean Network Information Centre, LACNIC*) – регионального интернет-регистратора, управляющего реестром интернет-адресов в регионе, – подтверждает, что киберпреступления ежегодно наносят ущерб латиноамериканским странам на сумму в 90 млрд долл.[2]

В совместном исследовании, проведенном в 2016 г. Организацией американских государств (ОАГ) и Межамериканским банком развития, отмечается, что 16 из 32 стран Латинской Америки и Карибского бассейна вовсе не способны противостоять кибератакам[3]. При этом к концу второго десятилетия XXI в. лишь шесть латиноамериканских стран разработали национальную стратегию защиты информационного пространства. Ими стали: Колумбия, уже успевшая не только принять подобную стратегию в 2011 г., но и обновить ее в 2016 г.; Панама, Парагвай, Чили и Коста-Рика, одновременно анонсировавшие в апреле 2017 г. собственные стратегии кибербезопасности, и Мексика, последняя из стран региона принявшая стратегию в этой сфере в ноябре 2017 г. Такое мизерное число стран, начавших формирование систем национальной кибербезопасности, которая уже стала для них стратегической проблемой государственной важности, можно объяснить следующими причинами [Hernández 2018: 54-69]. *Недостаток финансовых ресурсов*, направляемых для решения такого рода проблем, а также *отсутствие практического опыта* и явная *нехватка специализированных знаний* для разработки и реализации необходимых мер совместно блокируют принятие подобных концепций в рамках всего региона [Torres 2013].

В отличие от североамериканских стратегий, которые нацелены на глобальное геополитическое доминирование, латиноамериканские концепции носят *оборонительный характер*, будучи ориентированными именно на противодействие потенциальным угрозам [Betz, Stevens 2011]. При этом страны Латинской Америки полностью переняли у Соединенных Штатов практику создания команд компьютерной безопасности по реагированию на инциденты (*computer emergency response team, CERT*) – специальных групп экспертов по

[1] América Latina registró en 2017 unos 677 millones de ataques informáticos. https://www.efe.com/efe/america/tecnologia/america-latina-registro-en-2017-unos-677-millones-de-ataques-informaticos/20000036-3687233 (accessed 15.08.2019).

[2] OEA: Ciberdelito: 90.000 millones de razones para perseguirlo. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16 (accessed 11.09.2019).

[3] Informe Ciberseguridad. 2016. Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Banco Interamericano de Desarrollo (BID). Organización de los Estados Americanos.

кибербезопасности, занимающихся сбором информации о киберинцидентах, их классификацией и нейтрализацией[4].

КОЛУМБИЯ

Колумбия традиционно является одной из самых проблемных стран региона в вопросах безопасности. Постепенно проблема экспоненциального роста преступности распространилась и на цифровую среду. В конце первой декады XXI в. руководство страны попыталось остановить рост киберпреступлений, от которых страдали как колумбийские, так и международные компании, работающие в стране, и возвело восстановление безопасности цифрового пространства в ранг стратегической задачи. Так, в Национальном плане развития Колумбии на 2010–2014 гг. появилось обязательство по разработке политики, направленной на предотвращение компьютерных преступлений.

Колумбия стала первой страной Латинской Америки, утвердившей в 2011 г. полноценную Национальную стратегию кибербезопасности. Весной 2016 г. был принят уже новый вариант Стратегии, получившей название "Национальная политика в сфере цифровой безопасности" (*Política Nacional de Seguridad Digital*)[5]. Обновленный план заметно изменил подходы и концепции предшествующего, включив раздел "управление рисками", представляющий собой нахождение *равновесия* между оценкой вероятных угроз и затрат по их устранению.

Главной целью Стратегии стало снижение эффективности киберугроз через развитие потенциала возможных пострадавших, а также своевременное выявление и управление рисками информационной безопасности.

Колумбийская концепция зиждется на четырех принципах: *защита прав человека и основных ценностей*; *адаптация инклюзивного подхода*, предполагающего участие всех заинтересованных сторон; *гарантия солидарной ответственности*, *содействие сотрудничеству* между пользователями сети; а также *применение подхода, основанного на управлении рисками*.

В Стратегии выделены пять вспомогательных задач:

1. *Создание институциональной основы* для кибербезопасности. Для этого учреждается пост Национального координатора по вопросам информационной безопасности, который должен занимать чиновник из Департамента национального планирования. В его функции входит руководство и мониторинг реализации Стратегии, а также межведомственное согласование всех мероприятий, затрагивающих сферу цифровой безопасности. Создана Национальная комиссия по вопросам информационных технологий (*Comisión Nacional Digital y de Información Estatal*), которая стала верховной инстанцией страны, курирующей ИТ-отрасль.

2. *Формирование особых условий,* позволяющих всем заинтересованным сторонам управлять рисками информационной безопасности в рамках их экономической деятельности. За выполнение этой задачи несет ответственность колумбийское правительство.

3. *Построение государственно-частного информационного партнерства* как на национальном, так и на международном уровнях. За решение этой задачи отвечает федеральное правительство.

[4] Equipo de Respuesta ante Emergencias Informáticas. https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas (accessed 11.07.2019).

[5] República de Colombia. 2016. Politica nacional de seguridad digital. Documento CONPES. Consejo nacional de política económica y social. Departamento nacional de planeación. Bogotá, D.C. Borrador No. 2.

4. *Укрепление национальной обороны и суверенитета в информационном пространстве*. Здесь речь идет о разработке новейших методов и средств предотвращения, обнаружения, локализации, реагирования, восстановления и защиты, а также о сохранении целостности и повышении устойчивости к кибератакам жизненно важных инфраструктурных объектов, четкий перечень которых пока отсутствует. В стране сформирована команда *CERT*, находящаяся в ведении Верховного финансового управления Колумбии (*Corporación Financiera Colombiana*) и администрации президента[6].

5. С*оздание постоянно действующих механизмов* для развития сотрудничества в области информационной безопасности как на национальном, так и на международном уровнях. Колумбия планирует присоединиться к международным конвенциям в области информационной безопасности и гарантировать их соблюдение.

Органами, ответственными за реализацию данного проекта, являются Министерство национальной обороны, Министерство информационных технологий и связи, Департамент национального планирования (*Departamento Nacional de Planeación*) и Национальное управление разведки (*Dirección Nacional de Inteligencia*). Министерство информационных технологий и связи (*Ministerio de Tecnologías de la Información y las Comunicaciones, MTIC*) отвечает за развитие разнопланового сотрудничества между многочисленными заинтересованными сторонами.

Колумбийская стратегия ориентирована на обеспечение защиты в киберпространстве с помощью специальной системы технических средств противодействия угрозам, при явном предпочтении активных политик в области кибербезопасности пассивным. В течение последних трех лет военные расходы Колумбии являются самыми высокими в регионе, превышая ежегодно 10 000 млн долл. США. Значительная часть этой суммы направляется на развитие информационных технологий военного назначения. С оглядкой на опыт США и Эстонии в стране уже было создано специальное военное подразделение "Группа цифровых трансформаторов" (*Grupo de Transformadores Digitales del Ejército, GETDE*), специализирующееся на киберзащите и правомочное проводить как оборонительные, так и наступательные операции.

При этом в колумбийской Стратегии важное значение придается эффективному управлению информационными рисками для обеспечения безопасной жизни общества. Об этом свидетельствует частое упоминание в тексте документа термина "заинтересованные стороны", подчеркивающего признание колумбийскими властями того факта, что кибербезопасность является проблемой, затрагивающей интересы не только государства, но и граждан. Колумбия уделяет повышенное внимание развитию международного сотрудничества в борьбе с киберпреступностью, делая особый акцент на равное участие всех государств в развитии и управлении интернетом. Это подтверждает закрепленный в Стратегии тезис о том, что отсутствие конкретных механизмов международно-правового регулирования, ограничивающих использование технических средств для поражения информационных систем, не позволяет применять их без согласования с международными организациями и иностранными государствами.

ПАРАГВАЙ

Именно в Парагвае за период с 2010 по 2014 г. был зафиксирован наибольший рост количества интернет-пользователей в Латинской Америке, поэтому

[6] Grupo de Respuesta a Emergencias Cibernéticas de Colombia. http://www.colcert.gov.co (accessed 11.07.2019).

руководство страны решилось укрепить информационную безопасность посредством принятия в 2017 г. соответствующей Стратегии.

Главными целями парагвайского проекта являются: *распространение культуры кибербезопасности* для максимизации положительной отдачи от ИКТ, а также *повышение осведомленности населения* о безопасном использовании интернет-технологий; *продвижение проектов "Исследования, разработки и инновации"* за счет усиления взаимодействия между государственным и частным секторами, гражданами и научными кругами; *защита критической информационной инфраструктуры,* ответственность за безопасность которой солидарно распределяется между частными операторами связи и государством; м*аксимально эффективное реагирование на киберинциденты*, посредством выделения масштабных государственных финансовых ресурсов Центру мониторинга и реагирования на компьютерные атаки Парагвая (*CERT – PY*); *финансирование и снабжение необходимой техникой* всех организаций, ответственных за расследование компьютерных преступлений; *проведение курсов повышения квалификации по ИТ* для сотрудников учреждений, отвечающих за отправление правосудия, а также *укрепление международного сотрудничества* по вопросам борьбы с киберпреступлениями; *создание информационной инфраструктуры*, способной гарантировать безопасное информационное пространство.

Стратегия опирается на шесть принципов: соразмерность применяемых мер; эффективность использования ресурсов; принцип разделенной между всеми членами общества ответственности; внедрение технологических инноваций для развития цифровой экономики; международное сотрудничество, а также государственный контроль и надзор в области кибербезопасности.

Институциональная структура кибербезопасности Парагвая состоит из Национального координатора, осуществляющего мониторинг и контроль выполнения Стратегии, и Национальной комиссии по вопросам активизации сотрудничества в области кибербезопасности. В состав последней входят семь специализированных подкомитетов, также ответственных за достижение основных целей стратегического проекта.

Стратегический проект подтверждает гибкий характер государственной политики Парагвая, проводимой в сфере обеспечения информационной безопасности, способной быстро подстроиться под изменения трансформирующейся цифровой среды. В документе неоднократно подчеркивается, что киберпреступность носит трансграничный характер, а это предполагает тесное международное взаимодействие. Первостепенной задачей политики страны в сфере кибербезопасности является именно укрепление партнерства государственного и частного секторов, гражданского общества, а также научного сообщества, что в разворачивающемся информационном противоборстве способно обеспечить Парагвай конкурентоспособным преимуществом[7]. Но в отличие от североамериканской и китайской концепций кибербезопасности стратегия Парагвая не предусматривает развитие наступательного киберпотенциала, а также использование новейших информационных технологий в военно-политических целях. Это говорит о стремлении Парагвая за счет постепенного укрепления государственно-частного партнерства со временем нарастить собственный ресурс мягкой силы [Clarke, Knake 2010].

[7] Presidencia de la Republica de Paraguay. 2017. Secretaría Nacional de Tecnologías de la Información y la Comunicación de Paraguay. Ministerio de tecnologías de la información y comunicación. Decreto № 459. Plan Nacional de Ciberseguridad. Asuncion.

КОСТА-РИКА

На сегодняшний день Коста-Рика является вторым по величине экспортером программного обеспечения в Латинской Америке после Уругвая. Без преувеличения можно заявлять, что эта страна превратилась в регионального лидера по уровню развития отрасли информационных технологий. Рынок программного обеспечения (ПО) (*software*) и ИТ-услуг Коста-Рики составляет 1,4% всей национальной промышленности, а на его долю приходится более 1,7% ВВП страны[8]. Начиная с 2000 г. этот сектор экономики показывает уверенный и постоянный рост. В стране работают более 1 500 предприятий, деятельность которых связана с разработкой ПО, главным покупателем которого являются США.

У страны уже есть опыт создания правовой и институциональной базы, координирующей работу индустрии информационных технологий. Так, Палата информационно-коммуникационных технологий Коста-Рики (*Cámara de Tecnologías de Información y Comunicación, CAMTIC*) была создана еще в 1998 г. как некоммерческая организация, выражающая и защищающая интересы отрасли. В 1999 г. в стране была запущена инициатива "*PRO-SOFTWARE*", проект, задействовавший бизнес-сообщество, академические круги и правительство, целью которого стало создание благоприятных условий для компаний, работающих в отрасли ИТ. В 2003 г. был принят Стратегический план развития индустрии программного обеспечения, главной задачей которого стала активизация развития информационного сектора экономики. Неудивительно, что обеспечение кибербезопасности, а также угрозы, к которым могут привести "пробелы" в этой области, не остались без внимания правительства страны.

Национальная стратегия кибербезопасности Коста-Рики опирается на четыре принципа: приоритет интересов граждан, для повышения качества жизни которых государство обязуется содействовать развитию ИКТ; уважение прав человека и неприкосновенность частной жизни; согласованность действий и солидарная ответственность всех заинтересованных сторон при планировании и реализации Стратегии, а также международное сотрудничество как с государственными, так и с частными организациями[9].

Главными целями Стратегии выступают разработка системы мер, направленных на достижение безопасного использования ИТ, развитие сотрудничества многочисленных заинтересованных сторон и продвижение образовательных мероприятий в информационной сфере. Указанные цели разбиты на восемь подцелей: *достижение согласованности действий всех субъектов национальной экономики*; *повышение уровня информированности населения* по вопросам информационной безопасности; *развитие потенциала Коста-Рики в области кибербезопасности*; с*оздание эффективной нормативно-правовой базы* в области кибербезопасности и ИКТ; *выход на новый уровень защищенности от компьютерных атак критической информационной инфраструктуры*; *управление информационными рисками*; *активизация международного сотрудничества*; *поэтапная реализация Стратегии*, *контроль за ее выполнением и оценка достигнутых результатов*.

Что касается институциональной структуры Коста-Рики, то главным органом, ответственным за политику в области кибербезопасности, является Министерство

[8] Por qué Uruguay es el principal exportador de software per cápita en América Latina. http://www.2121.org.uy/novedades/noticias/item/1175-por-que-uruguay-es-el-principal-exportador-de-software-per-capita-en-america-latina (accessed 19.09.2019).

[9] Estrategia Nacional de Ciberseguridad de Costa Rica. (2017). Ministerio de Ciencia, Tecnología y Telecomunicaciones, Estrategia Nacional de Ciberseguridad Costa Rica. San José, C.R.: MICITT.

науки, технологий и телекоммуникаций (*Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT*), при котором учрежден пост Национального координатора, оценивающего степень выполнения поставленных задач. Центр реагирования на инциденты информационной безопасности (*CSIRT – CR*), созданный еще в 2012 г., ответственен за обнаружение, предупреждение и ликвидацию последствий компьютерных атак. Помимо этого, сформирован особый Консультативный комитет, состоящий из представителей министерства, судебной власти, Управления коммуникаций (*Superintendencia de Comunicaciones*), гражданского общества, научных кругов и предпринимательского сектора.

Несмотря на то, что в стране создана комплексная система обеспечения кибербезопасности, Коста-Рика выступает категорически против использования информационно-коммуникационных технологий в военно-политических целях [Geers 2009]. Позиция страны состоит в том, что для повышения уровня кибербезопасности на уровне государства необходимо осуществление комплекса мероприятий правового, технологического, организационного и политико-дипломатического содержания. Отличительной особенностью коста-риканской Стратегии кибербезопасности стало то, что она ориентирована в первую очередь на развитие внутреннего информационного потенциала, действуя с оглядкой на своего главного покупателя ИТ-услуг – США. Это подтверждает и то, что особое внимание в документе уделено проведению образовательных и информационных мероприятий. Именно сохранение места заметного игрока на глобальном рынке программного обеспечения, которое уверенно удерживает страна на протяжении последних десятилетий, является главной задачей национальной стратегии кибербезопасности. Следует подчеркнуть, что в этом отношении концепция носит ярко выраженный экономический характер.

Чили

В экономике Чили отрасль информационных технологий занимает важное место. Чилийские компании ИТ-сектора в среднем ежегодно экспортируют ПО на 340 млн долл., прежде всего в страны Латинской Америки, а также в меньшей степени с США и Европу. В 2001 г. в стране была создана Ассоциация предприятий информационных технологий (*Asociación Chilena de Empresas de Tecnologías de la Información*), лоббирующая интересы отрасли. В 2005 г. учрежден Национальный инновационный совет по конкурентоспособности (*Consejo Nacional de Innovación para la Competitividad*), ответственный за выработку государственной политики в сфере ИТ. В 2014 г. он переименован в Национальный совет по инновациям в целях развития (*CNID*), а в его обязанности стало входить формирование институциональной среды инновационного развития и активизация сотрудничества государства и бизнеса в этой сфере. Кроме того, Чили является одной из самых продвинутых стран Латинской Америки по показателю проникновения интернета с более чем 70% населения. Все это постепенно привело к необходимости формирования национальной политики в области обеспечения кибербезопасности, работа над которой велась более трех лет.

В чилийской Стратегии кибербезопасности подробно расписаны основные цели на краткосрочную и среднесрочную перспективу, а также перечислены ответственные за ее реализацию учреждения[10]. Декабрь 2022 г. выступает верхним пределом по достижению пяти ключевых целей:

[10] Gobierno de Chile. 2017. Política Nacional de Ciberseguridad. Santiago de Chile.

1. *Создание ИКТ-инфраструктуры,* которая с точки зрения управления рисками способна противостоять кибератакам разного уровня сложности, а также быстро восстанавливаться после них. Для достижения этого предполагается комплекс мероприятий, в частности: создание надежного и гибкого киберпространства; определение и ранжирование объектов критически важной ИКТ-инфраструктуры, затрагивающих деятельность секторов водоснабжения, здравоохранения, общественной безопасности, энергетики, телекоммуникаций, финансовых услуг, государственного управления, транспорта, обороны и гражданской защиты;

2. *Гарантии реализации прав и свобод человека и гражданина в киберпространстве.* Для достижения этой цели правительство Чили обязуется предотвращать правонарушения, минимизировать риски и угрозы в информационной среде; обновить и усилить законодательство; обеспечить многосекторальную профилактику киберугроз;

3. *Формирование культуры кибербезопасности в обществе.* Этого планируется достичь за счет повышения информированности пользователей ИКТ как о рисках и угрозах, с которыми они могут столкнуться, так и об юридической ответственности за киберпреступления;

4. *Расширение международного сотрудничества в целях повышения уровня защиты в области кибербезопасности*. Эта цель соотносится с принципом внешней политики Чили, в основе которого лежит развитие сотрудничества с другими странами и многосторонней дипломатии для снижения рисков конфликта в киберпространстве;

5. *Развитие индустрии кибербезопасности Чили* для достижения стратегических целей страны. Здесь особая значимость придается развитию инноваций в области кибербезопасности для оборонного сектора страны, а также необходимости повышения спроса на ИКТ и государственного содействия (посредством госзаказов) развитию индустрии в целом.

Институциональную структуру возглавляет Межведомственный комитет по кибербезопасности, который отвечает за координацию мероприятий и оценку достигнутых результатов. За технические вопросы, такие как управление киберинцидентами, возникающими в Государственной сети связи (*Red de Conectividad del Estado*), несет ответственность общенациональная команда *CSIRT.* Примечательно, что в среднесрочной перспективе предполагается создание целой системы Команд реагирования на инциденты в области кибербезопасности (*CSIRT*), состоящей из одной общенациональной команды, отвечающей за сбор и систематизацию всей информации, и еще нескольких специализированных команд, курирующих информбезопасность важнейших отраслей экономики страны. Кроме того, в краткосрочной перспективе планируется создание специализированного Консультативно-совещательного совета.

Чили глубоко интегрирована как в региональный, так и в международный рынок информационных технологий, что обуславливает главную особенность ее национальной стратегии кибербезопасности – нацеленность прежде всего на развитие инновационного потенциала государства, а также активизацию и расширение сотрудничества в области ИКТ. С другой стороны, документ признает важность борьбы с увеличивающимся числом государственных и негосударственных акторов, совершающих противоправные действия в цифровом пространстве. При этом подчеркивается, что грани между этими акторами становятся все более размытыми. Однако в отличие от стран Запада

чилийская концепция в первую очередь направлена на обеспечение противодействия угрозам, исходящим от отдельных киберпреступников. А борьбе с посягательствами со стороны разведок недружественных государств и кибертеррористов уделяется лишь второстепенное внимание. В отличие от стратегий других латиноамериканских стран, в чилийском проекте особое внимание уделено продвижению и поощрению уважения прав человека, гарантирующих, что любые мероприятия, осуществляемые в рамках проекта, не будут ограничивать доступ граждан к сети интернет. Кроме того, подчеркивается неукоснительность соблюдения принципа сетевого нейтралитета.

МЕКСИКА

Индустрия информационных технологий и коммуникаций играет заметную роль в развитии мексиканской экономики и повышении благосостояния страны [Kosévich 2017]. Сфера ИКТ обеспечивает работой более 78 тыс. человек, а темпы роста за последнюю декаду превышают экономический рост Мексики. Вместе с тем проблема киберпреступности также не обошла стороной это государство: наносимый ею ежегодный ущерб оценивается в 3 млрд долл. Именно Мексика стала источником рассылки большинства спам-писем в регионе, а также получателем 53% всех вредоносных программ, запускаемых по всему миру. Стоит добавить и то, что показатель киберпреступлений, совершенных в период с 2015 по 2017 гг., увеличился с 11% до 23%[11]. Все это привело к тому, что государство и бизнес-сообщество осознали важность обеспечения национальной кибербезопасности, и уже к 2019 г. Мексика превратилась в регионального лидера по показателю инвестиций в индустрию цифровой безопасности [Косевич 2019].

Мексика последней из рассматриваемых в статье латиноамериканских стран приняла собственную Национальную стратегию кибербезопасности. В документе подчеркивается, что принятие подобного стратегического проекта было вызвано экспоненциальным ростом количества как крупных киберпреступлений, так и случаев мелкого кибер-мошенничества[12].

Руководящими принципами Стратегии являются уважение прав человека и основных свобод; профилактический подход; развитие трансграничного, междисциплинарного и многостороннего сотрудничества.

Главной целью проекта заявлено повышение уровня информационной безопасности в политической, экономической и социальной сферах общественной жизни, что позволит гражданам, а также государственным и частным организациям ответственно использовать ИКТ для достижения целей устойчивого развития Мексики.

В мексиканском варианте Стратегии закреплены восемь ключевых направлений деятельности в сфере кибербезопасности[13]: *развитие культуры кибербезопасности*; *наращивание потенциала*; *обеспечение эффективной координации в случае возникновения киберугроз*; *применение трехсекторной модели* "Исследования-разработки-инновации" с использованием средств бюджета; *разработка и принятие новейших стандартов и технических регламентов*; *защита критически важной*

[11] La ciberseguridad en Mexico debe atenderse de forma prioritaria. URL: https://elceo.com/tecnologia/la-ciberseguridad-en-mexico-debe-atenderse-de-forma-prioritaria-expertos/ (accessed 15.08.2019)

[12] Gobierno de México. 2017. Estrategia de Ciberseguridad. Mexico D.F.

[13] В документе подчеркивается, что все указанные мероприятия будут осуществляться в рамках Закона "О национальной безопасности" (принят 31 января 2005 г.).

инфраструктуры; *создание нормативно-правовой базы*, регулирующей эту сферу; *ведение статистики и мониторинг достижения основных целей*.

За реализацию и обновление проекта, а также за координацию деятельности правительства в этой сфере ответственен Подкомитет по кибербезопасности, созданный в октябре 2017 г. и находящийся в непосредственном ведении Межсекретариальной комиссии по развитию электронного правительства (*Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, CIDGE*). В состав Подкомитета входят несколько специализированных учреждений, ответственных за обеспечение защиты киберпространства Мексики.

Главной особенностью национальной стратегии Мексики стало то, что она носит трансграничный характер, будучи ориентированной на повышение уровня безопасности как национальных, так и региональных информационных систем. Это объясняется особым геополитическим положением страны, которая находится на стыке Северной и Южной Америки. Вместе с тем особое внимание в стратегическом проекте уделяется обеспечению экономической безопасности и стабильности развития национальной индустрии информационных технологий и коммуникаций. Мексиканская концепция нацелена на развитие сотрудничества, осуществляемого посредством обмена информацией, передовыми практиками, признавая важность проведения совместных учений по кибероборонe, как на национальном уровне (при участии государственного и частного секторов), так и с соседями по региону. Кроме того, в документе подчеркивается важность проведения научных исследований и разработок в области кибербезопасности – практике, распространенной не только в США, но и в европейских странах.

БРАЗИЛИЯ

Система национальной кибербезопасности Бразилии формировалась под влиянием нескольких факторов. Ими стали и пугающий рост числа хакерских атак, с которыми страна оказалась не в состоянии справиться, и ее неудержимое желание “не остаться позади” крупнейших мировых держав в разворачивающемся противостоянии киберугрозам. На протяжении последнего десятилетия Бразилия ежегодно входила в число стран, наиболее подверженных киберпреступлениям. Одновременно в Бразилии наблюдался заметный рост числа людей, имеющих доступ в интернет – на сегодня это более 70% населения.

Разработка политики в области кибербезопасности и киберзащиты в Бразилии велась в контексте принятия инициатив по укреплению потенциала национальной обороны. В рамках федерального правительства была создана иерархическая система принятия стратегических решений в сфере кибербезопасности: начиная с Президента Республики, Бразильского разведывательного управления (*ABIN*) и заканчивая Кабинетом институциональной безопасности Республики (*Gabinete de Segurança Institutional da Presidência da República*). Ответственными за согласование плана мероприятий в области информационной защиты стали созданный в 2010 г. “Центр киберзащиты” (*CDCiber*), находящийся в одном блоке с бразильской армией и Министерством обороны, и Министерство юстиции, действующее в этой сфере через федеральную полицию. Специализированного агентства, отвечающего за реализацию государственной политики в этой области, в Бразилии пока создано не было.

Главной задачей политики кибербезопасности Бразилии является повышение уровня защищенности объектов критически важной инфраструктуры и органов государственной власти, а также упрочение киберпотенциала страны.

В качестве основных ее целей можно назвать следующие: увеличение объема бюджетных ресурсов, выделяемых на кибербезопасность, а также достижение высокого уровня защищенности правительственных учреждений.

В системе вооруженных сил главнокомандующим в этой сфере является Центр киберзащиты (*CDCiber*), в подчинении которого находятся Центр исследований, реагирования и обработки инцидентов безопасности (*CERT.br*), Федеральная служба по обработке данных (*Serpro*), а также ряд исследовательских центров, созданных при правительстве и ряде других высших государственных органов власти и управления, ответственных за системное администрирование.

Во главе угла бразильской политики в сфере кибербезопасности находится Стратегия национальной обороны, утвержденная в 2008 г. и обновленная в 2012 г. Именно в этом документе обеспечение кибербезопасности впервые было причислено к числу стратегических задач Бразилии. Полномочия в области обеспечения киберзащиты были переданы армии. В 2012 г. Министерством обороны Бразилии была утверждена Политика киберзащиты (*Portaria Normativa nº 3.389/MD de 21 de Dezembro de 2012*), в которой были закреплены руководящие принципы, цели и обязательные мероприятия в этой сфере. Данный документ взял за основу Декрет № 3.505, принятый еще в 2000 г. (*Decreto nº 3.505/2000*) и впервые закрепивший основные аспекты политики кибербезопасности для организаций и учреждений федерального государственного управления.

Весь комплекс государственных мер Бразилии в отношении формирования системы национальной кибербезопасности имеет ряд недостатков, несмотря на предпринятые попытки конкретизировать ее аспекты. В частности, это касается невнимания к вопросам соблюдения прав человека при реализации мероприятий в данной области, а также отсутствию главного ответственного учреждения.

Таким образом, можно выделить две главные особенности бразильской политики кибербезопасности. Во-первых, ее ориентированность на продвижение Бразилии в качестве сильного глобального игрока в области кибербезопасности. Достижение этого планируется посредством ускоренного наращивания внутренних инвестиций в сектор информационных технологий, создания рабочих мест, а также установления партнерских отношений между государственным и частным секторами. Бразилия демонстрирует явную нацеленность на решение задач ускорения развития информационной инфраструктуры и технологий военного назначения, что в среднесрочной перспективе позволит достигнуть ей информационного превосходства в регионе. Во-вторых, в отличие от других латиноамериканских стран, в Бразилии информационная безопасность входит в сферу компетенции Министерства обороны, а, следовательно, и армии. Такая милитаризация вызвала обоснованную критику бразильской общественности в отношении того, что была создана "тяжеловесная" система управления киберугрозами, в которой особое внимание уделяется маловероятным опасностям, таким, как кибервойны и кибершпионаж в ущерб лучшей подготовленности к решению реальных задач, таких как кибермошенничество.

В течение последнего десятилетия в Бразилии особое внимание уделялось созданию государственных специализированных структур для ведения кибервойн и кибероперациий – того, чего нет ни в одной другой латиноамериканской

стратегии кибербезопасности. А в случае возникновения информационных инцидентов и угроз предусматривается проведение не только оборонительных, но и наступательных операций, что подтверждает высокую степень преемственности по отношению к североамериканским стратегиям [Cruz Lobato 2017].

* * *

Исходя из результатов сравнительного анализа стратегий и политики кибербезопасности шести латиноамериканских стран, можно заключить, что формируемая в регионе парадигма информационной безопасности опирается на следующие единые принципы: защита прав человека и основных ценностей, согласованность действий и солидарная ответственность всех заинтересованных сторон, а также развитие трансграничного, междисциплинарного и многостороннего сотрудничества. Ускорение развития информационной инфраструктуры и оптимизация ресурсов киберзащиты выступают в качестве общих приоритетных задач.

Нацеленность Латинской Америки в первую очередь на создание условий, обеспечивающих снижение риска использования новых технологий для силового разрешения межгосударственных противоречий, а также на обеспечение согласованной деятельности в этой сфере на международном уровне бесспорно являются заметным достижением этого региона в решении новейших проблем кибербезопасности. Подобный подход может стать примером для других стран и регионов.

DOI: 10.17976/jpps/2022.03.09

CYBERSPACE SECURITY IN LATIN AMERICAN COUNTRIES

E.Yu. Kosevich[1,2]

[1] *HSE University. Moscow, Russia*

[2] *Institute of Latin American Studies, Russian Academy of Sciences. Moscow, Russia*

KOSEVICH, Ekaterina Yurievna, Cand. Sci. (Polit. Sci.), Senior Research Fellow, International Laboratory on World Order Studies and the New Regionalism, HSE University; Research Fellow, Center for Political Studies, Institute of Latin American Studies, Russian Academy of Sciences, email: ekaterina.kosevich@gmail.com

Kosevich, E.Yu. (2022). Cyberspace security in Latin American countries. *Polis. Political Studies*, 3, 108-123. (In Russ.) https://doi.org/10.17976/jpps/2022.03.09

Acknowledgements. Support from the Individual Research Program of the School of World economy and International Affairs at National Research University – Higher School of Economics is gratefully acknowledged.

Received: 27.09.2019. Accepted: 16.03.2020

Abstract. The adoption of a national cybersecurity strategy testifies to a country's awareness of the importance of protecting cyber infrastructure, the digital economy and the business environment, on which information and economic well-being are already highly dependent. However, only a few Latin American countries have developed and adopted their own national cybersecurity strategy. This article analyzes key aspects of the cybersecurity strategies of Colombia, Paraguay, Costa Rica, Chile and Mexico. The author considers their guidelines and goals, as well as the bodies and institutions responsible for the implementation and monitoring of the results of these strategies. In addition, the author offers a description of the national cybersecurity policy developed in Brazil, the largest country in Latin America, which currently accounts for the largest number of cybercrimes in the region. Particular attention is paid to the state of the information technology industry in each of these Latin American countries.

Keywords: Latin America, national cybersecurity strategies, information space, information technology, cybersecurity, Internet, Colombia, Paraguay, Chile, Costa Rica, Mexico, Brazil.

References

Ablon, L., Libicki, M.C., & Golay, A.A. (2014). Markets for cybercrime toolsand stolen data: hackers' bazaar. Santa Mónica: RAND.

Álvarez-Valenzuela, D. (2017). Los desafíos de la ciberseguridad en Chile. *Revista Chilena de Derecho y Tecnología,* 6(2), 1-2. https://doi.org/10.5354/0719-2584.2017.48027

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: cyber war, cyber terror and risk. *Space and Culture*, 15(2), 110-123.

Betz, D.J., & Stevens, T. (2011). Cyberspace and the state: toward a strategy for cyber-power. Adelphi Series: Routledge.

Betz, D.J., & Stevens T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, 44(2), 147-164.

Clarke, R.A., & Knake, R.K. (2010). Cyber war: the next threat to national. Security and what to do about it. New York, NY: Ecco.

Cruz Lobato, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. *Revista Latinoamericana de Estudios de Seguridad,* 20, 16-30. https://doi.org/10.17141/urvio.20.2017.2576

Day, R.E. (2001). The modern invention of information: discourse, history and power. Carbondale: Southern Illinois University Press.

Deibert, R.J., & Rohozinski, R. (2010). Risking security: policies and paradoxes of cyberspace security. *International Political Sociology,* 4(1), 15-32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

DeNardis, L. (2009). Protocol politics: the globalization of internet governance. Cambridge: MIT Press.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D.L. Cogburn, L. DeNardis, & N.S. Levinson (Ed.), *The Turn to Infrastructure in Internet Governance* (pp. 3-21). London: Palgrave MacMillan.

Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. London: Routledge.

Dunn Cavelty, M. (2015). The normalization of cyber-international relations. In O. Thränert, & M. Zapfe (Ed.), *Strategic Trends 2015: Key Developments in Global Affairs* (pp. 81-98). Zurich: CSS.

Dunn Cavelty, M., & Jaeger, M.D. (2015). (In)visible Ghosts in theMachine and the Powers that Bind: The Relational Securitization of Anonymous. *International Political Sociology,* 9(2), 176-194. https://doi.org/10.1111/ips.12090

Dutton, W.H. (2015). Multistakeholder Internet governance? Background Paper: Digital Dividends. https://thedocs.worldbank.org/en/doc/591571452529901419-0050022016/original/WDR16BPMultistakeholderDutton.pdf

Eriksson, J., & Giacomello G. (2009). Who Controls the Internet? Beyond the obstinacy or obsolescence of the state. *International Studies Review,* 11(1), 205-230. https://doi.org/10.1111/j.1468-2486.2008.01841.x

Geers, K. (2009). Strategic cyber security. Santa Monica: NATO, RAND Corporation.

Hernández, J.C. (2018). Estrategias nacionales de ciberseguridad en América Latina. Universidad de Granada. *Análisis GESI,* 8.

Janczewski, L.J., & Colarik, A.M. (2008). Cyber warfare and cyber terrorism. New York, NY: New Press.

Kosévich, E.Y. (2017). México: estrategia de seguridad y de la lucha contra el crimen organizado. *Iberoamérica*, 1, 74-95.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software*, 3(4), 161-176.

Lewis, A.J. (2018). Economic impact of cybercrime. No slowing down. McAfee y Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Maciel, M.F., & Pereira de Souza, C.A. (2011). Multi-stakeholder participation on Internet governance: An analysis from a developing country, civil society perspective. Association for Progressive Communications. https://www.apc.org/sites/default/files/NoN_Multistakeholder_InternetGovernance.pdf

Mueller, M. (2017). Is cybersecurity eating internet governance? causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, 19(6), 415-428. http://dx.doi.org/10.1108/DPRG-05-2017-0025

Mueller, M., & Klein, H. (2014). Sovereignty, national security, and internet governance: proceedings of a workshop. Syracuse University: Georgia Institute of Technology School of Public Policy.

Torres, M. (2013). Ciberguerra. Manual de Estudios Estratégicos y Seguridad Internacional. Madrid: Plaza & Valdés.

Bulavin, A.V. (2014). Concerning approaches of the USA and China to cybersecurity. *Society: Politics, Economics, Law*, 1, 27-31. (In Russ.)

Chereshkin, D.S. (Ed.). (2006). Problemy kiberbezopasnosti sovremennogo obshchestva [The cybersecurity challenges of modern society]. Moscow: URSS.

de Bossey, Ch. (2005). Report of the working group on internet governance. (Russ. ed.: de Bossey, Ch. Doklad rabochei gruppy po upravleniyu Internetom). https://www.un.org/ru/development/ict/wgig_report.pdf

Kasenova, M.B. (2012). Internet corporation for assigned names and numbers in Internet management. *The Review of Economy, the Law and Sociology,* 4, 164-169.

Kasenova, M.B., & Demidov, O.V. (Ed.). (2013). Kiberbezopasnost' i upravlenie internetom: dokumenty i materialy dlya rossiiskikh regulyatorov i ekspertov [Cybersecurity and Internet governance: documents and materials for Russian regulators and experts]. Moscow: Statut.

Kazarin, O.V., & Tarasov, A.A. (2013). Modern concepts of cybersecurity of leading foreign countries. *Vestnik RGGU. Seriya: Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaya bezopasnost'*, 14, 58-74. (In Russ.)

Komov, S.A. (Ed.). (2011). Mezhdunarodnaya informatsionnaya bezopasnost': problemy i resheniya [International information security: problems and solutions]. Moscow.

Kosevich, E.Yu. (2019). The frontier's barriers – security or threat for Mexican-American relations. *Latinskaya Amerika,* 6, 39-48. (In Russ.) https://doi.org/10.17976/jpps/2002.05.15

Markov, A.S., & Tsirlov, V.L. (2007). Risk management – regulatory vacuum of information security. *Open Systems Journal*, 8, 63-67. (In Russ.)

Krutskikh, A.V. (Ed.) (2019). Mezhdunarodnaya informatsionnaya bezopasnost': teoriya i praktika. V 3-kh tt. T. 1 [International information security: theory and practice. In 3 vols. Vol. 1]. Moscow: Aspect Press.

Morozov, I.L. (2002). Informational security of a political system. *Polis. Political Studies*, 5, 134-145. (In Russ.). https://doi.org/10.17976/jpps/2002.05.15

Parshin, S.A., Gorbachev, Yu.E., & Kozhanov, Yu.A. (2011). Kibervoiny – real'naya ugroza natsional'noi bezopasnosti? [Cyber warfare – a real threat to national security?]. Moscow: KRASAND.

Rogovskii, E.A. (2014). Kiber-Vashington: global'nye ambitsii [Cyber Washington: global ambitions]. Moscow: Mezhdunarodnye otnosheniya.

Sharikov, P.A. (2015). Problemy informatsionnoi bezopasnosti v politsentrichnom mire [Problems of information security in a polycentric world]. Moscow: Ves' Mir.

Zagorskii, A.V., & Romashkina, N.P. (Ed.). (2016). Problemy informatsionnoi bezopasnosti v mezhdunarodnykh voenno-politichekikh otnosheniyakh [Problems of information security in international politico-military relations]. Moscow: IMEMO RAN.

Литература на русском языке

Булавин А.В. 2014. О подходах США и Китая к обеспечению кибербезопасности. *Общество: политика, экономика, право.* № 1. С. 27-31.

Де Босси Ш. 2005. Доклад рабочей группы по управлению Интернетом. https://www.un.org/ru/development/ict/wgig_report.pdf

Казарин О.В., Тарасов А.А. 2013. Современные концепции кибербезопасности ведущих зарубежных государств. *Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность*. № 14. С. 58-74.

Касенова М.Б. 2012. Корпорация Интернета по распределению имен и адресов в механизме управления Интернетом. *Вестник экономики, права и социологии*. № 4. С. 164-169.

Кибербезопасность и управление интернетом: документы и материалы для российских регуляторов и экспертов. 2013. Отв. ред. М.Б. Касенова. М.: Статут.

Косевич Е.Ю. 2019. Приграничные стены: безопасность или угроза для мексикано-американских отношений. *Латинская Америка*. № 6. С. 39-48. https://doi.org/10.31857/S0044748X0005098-6

Марков А.С., Цирлов В.Л. 2007. Управление рисками – нормативный вакуум информационной безопасности. *Открытые системы. СУБД*. № 8. С. 63-67.

Международная информационная безопасность: проблемы и решения. 2011. Под общ. ред. С.А. Комова. М.

Международная информационная безопасность: теория и практика. В 3-х тт. Т. 1. 2019. Под общ. ред. А.В. Крутских. М.: Аспект Пресс.

Морозов И.Л. 2002. Информационная безопасность политической системы. *Полис. Политические исследования*. № 5. С. 134-145. https://doi.org/10.17976/jpps/2002.05.15

Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. 2011. Кибервойны – реальная угроза национальной безопасности? М.: КРАСАНД.

Проблемы информационной безопасности в международных военно-политических отношениях. 2016. Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН.

Проблемы кибербезопасности современного общества. 2006. Под. ред. Д.С. Черешкина. М.: URSS.

Роговский Е.А. 2014. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения.

Шариков П.А. 2015. Проблемы информационной безопасности в полицентричном мире. М.: Весь Мир.