А.В.Макарычева

Информационная безопасность в Латинской Америке: пути адаптации к новым угрозам

Статья посвящена сложному процессу адаптации латиноамериканских государств к угрозам информационной безопасности. Для анализа использован метод кейс-стади: на примере двух государств региона — Бразилии и Никарагуа, находящихся на разных полюсах по уровню развития технологий, — автор наглядно рассматривает стратегии этих стран по борьбе с новыми угрозами.

Ключевые слова: Латинская Америка, информационная безопасность, Бразилия, информационные преступления, Никарагуа.

Тема информационной безопасности затрагивает все больше государств и регионов в современном мире. Правительства ряда стран Латинской Америки относят сетевые атаки и другие противоправные действия в сети к приоритетным вызовам для национальной безопасности[1]. Прежде всего важно отметить, что развитие Интернета и выявление новых угроз происходит в регионе неравномерно. Например, Мексика начала активно использовать интернет-технологии одной из первых в регионе — в 1989 г.[2], а одной из последних стала Доминиканская Республика, подключившаяся к сети спустя почти семь лет. При этом сегодня разрыв не только не сокращается, а еще больше увеличивается. Темпы выработки соответствующих мер по обеспечению информационной безопасности государств, в свою очередь, также сильно различаются. Исследователи условно делят страны Латинской Америки на две группы: к первой относятся государства, имеющие национальную программу в области информационной безопасности, а ко второй — те, которые по ряду причин пока не успели ее выработать. К последней группе в 2016 г. относились четыре из пяти стран региона[3]. В двух из трех государств отсутствует специализированное управление по отслеживанию информационных преступлений[4].

Анна Владимировна Макарычева — аспирант кафедры мировых политических процессов Московского государственного университета международных отношений (МГИМО МИД России) (makarycheva.a.v@my.mgimo.ru).

Вместе с тем, фактор наличия стратегии является очень важным, но не определяющим, поэтому представляется целесообразным изучить систему мер противодействия информационным угрозам одного из государств, где достигнуты определенные успехи на пути выработки политики в области противодействия информационным угрозам, а также одного из тех, где реализация подобных мер находится пока на не очень высоком уровне. При этом важно учитывать, что государствам с передовыми технологиями в силу высокой степени информатизации процессов в социальной, государственной и даже производственной сферах может быть нанесен гораздо более серьезный урон — не только на уровне пользовательских компьютеров, но и критической инфраструктуры[5].

В целом по региону за последние несколько лет число преступлений в информационной сфере увеличилось почти на 35%[6], при этом только за первый триместр 2017 г. этот показатель достиг 40%[7]. В 2015 г., по данным лаборатории Касперского, было зафиксировано почти 28 млн попыток заражения сетевыми вирусами в Бразилии, почти 16 млн в Мексике и 5 млн в Колумбии[8]. От вируса «WannaCry» в регионе больше всех пострадали Мексика и Бразилия[9]. Важно отметить, что в латиноамериканском регионе есть понимание того, что добиться ощутимых результатов в борьбе с транснациональными угрозами можно только совместными усилиями на региональном и глобальном уровнях[10], однако в настоящее время меры локального характера существенно преобладают над региональными решениями. Справедливости ради отметим, что довольно активная работа ведется на уровне региональных организаций — прежде всего, Организации американских государств (ОАГ) и Экономической комиссии ООН для Латинской Америки и Карибского бассейна (Comisión Económica para América Latina y el Caribe, CEPAL). На базе этих организаций выпускаются многочисленные доклады и статьи, в которых даются различные пути выхода из нее, методы комплексного решения возникающих проблем[11].

Если учитывать общемировую конъюнктуру, то следует отметить, что государства Латинской Америки занимают довольно неплохие позиции. Так, в глобальном рейтинге доклада Международного союза электросвязи (International Telecommunication Union, ITU), где оценивается деятельность структур, занимающихся обеспечением информационной безопасности, Бразилия находится на пятой строчке наравне с Германией, Великобританией; Уругвай и Колумбия занимают 8-е и 9-е места, соответственно[12]; Аргентина — на 15-й позиции, Чили — на 16-й, а Мексика и Перу — на 18-м месте[13].

ДОСТИЖЕНИЯ В БОРЬБЕ С ИНФОРМАЦИОННЫМИ УГРОЗАМИ

Переходя к анализу мер, предпринимаемых государствами региона в целях пресечения и предотвращения противоправных действий в информационном пространстве, отметим, что оценка мер по противодействию подобным угрозам должна вестись по четырем основным направлениям. Во-первых, это — технологический аспект, подразумевающий уровень развития соответствующих технологий. Во-вторых, — организационный, включающий в себя оценку действий по борьбе с новыми угрозами и структуры компетентных органов. Третий аспект связан с проработкой законодательной базы. Одним из передовых государств региона в этой области является

Уругвай — первое неевропейское государство, присоединившееся к Конвенции Совета Европы о защите персональных данных и активно совершенствующее собственное законодательство[14]. И последний, четвертый, фактор обеспечения информационной безопасности — это работа с населением. Здесь важно понять, какие образовательные программы реализуются с целью формирования грамотного подхода к использованию сети и, в частности, интернет-сайтов. Социологический аспект представляется крайне важным, ведь именно граждане являются основными пользователями Интернета и наиболее уязвимы перед его возможными угрозами.

В качестве примера, где успешно решаются вопросы обеспечения информационной безопасности, была выбрана Бразилия. Этот выбор был сделан не случайно, так как государство опубликовало стратегию в области противодействия угрозам информационного характера под названием «Национальная стратегия безопасности информационно-коммуникационных технологий и кибернетической безопасности Федеральной государственной администрации»[15] только в 2015 г., в то время как первый документ, связанный с обеспечением информационной безопасности, появился в 2000 г.: им стала Директива № 3.505/2000, выпущенная одним из подразделений той же администрации. При этом в стране ежегодно выходили документы по данной проблематике, принимались меры по противодействию возникающим угрозам[16].

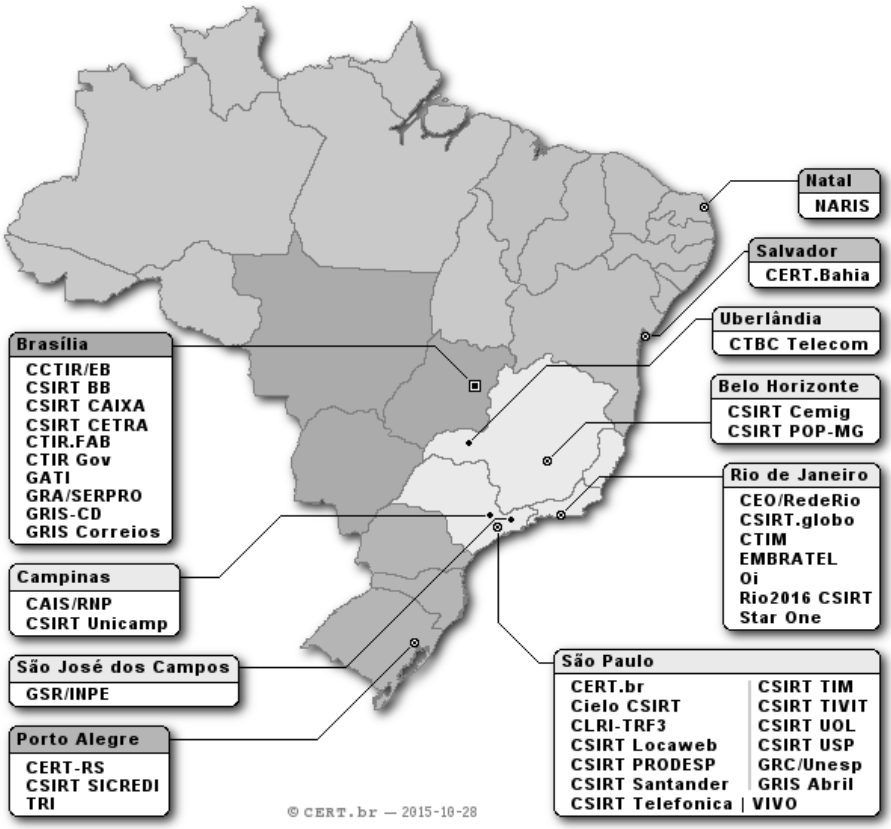
Из 206 млн жителей Бразилии доступ к сети имеют 139 млн, что составляет примерно 66%[17]. Что касается первых двух аспектов, прежде всего, необходимо упомянуть «Белую книгу национальной обороны», изданную в 2008 г. и обновляемую каждые четыре года. Отдельный пункт данного документа посвящен вопросам информационной безопасности. Обеспечение информационной безопасности, согласно изучаемому документу, охватывает целый комплекс мер по предотвращению возможных актов агрессии, включая работу спецслужб, научные разработки, внедрение новых технологий, а также активную работу по защите информации и активов, размещённых в сети Интернет[18]. Кроме того, в 2010 г. в Бразилии был создан Центр кибернетической безопасности (Centro de Defesa Cibernética, CDCiber), который успешно справлялся с отражением сетевых атак во время Чемпионата мира по футболу 2014 г. и Олимпиады в г. Рио-де-Жанейро в 2016 г. Оба мероприятия помогли осуществить прорыв в области обороны от кибератак[19]. В тот период существенно возросло количество противоправных действий в сети, направленных на Бразилию и включающих *фишинг*, DoS-атаки и т.п.[20]. В 2017 г. именно на эту страну приходится наибольшее число подобных нападений в регионе — порядка 54%[21].

За несколько лет существования CDCiber не только была детально разработана политика в области отражения и предотвращения угроз информационной безопасности, но и созданы и внедрены первая национальная система антивирус «Defensa BR», а также Система кибероперaций (El Sistema de Operaciones Cibernéticas, SIMOC), с помощью которой совершенствовалась техника выявления информационных атак на компьютерные сети, а также велась дальнейшая разработка механизмов их защиты[22]. С 2016 г. в бразильской армии возникла новая структура — Управление кибернетической безопасности (Comando de Defesa Cibernética, ComDCiber), нацеленное на координацию работы по предотвращению информационных угроз и

разработке новейших технологий в компьютерной области. С 2014 г. планируется создание Национальной школы по защите от киберугроз для подготовки высококвалифицированных кадров в данной области[23]. В настоящее время экспертов по информационной безопасности активно привлекают для участия в научных форумах и выставках инноваций[24].

Среди мер, предпринятых в отношении инцидентов в интернет-пространстве, нельзя не упомянуть создание ряда групп реагирования на инциденты в области информационной безопасности в рамках административных и правительственных структур, привлекающих к работе представителей частного сектора и академических кругов (см. картограмму ниже).

КАРТА ГРУПП РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В СЕТИ (БРАЗИЛИЯ)



Источник: https://www.cert.br/csirts/brasil/

Например, CERT-RS — это группа реагирования на чрезвычайные компьютерные происшествия, CSIRT PRODESP — группа реагирования на инциденты, связанные с информационной безопасностью. Следует обратить внимание и на центр TRI — «Время реагирования на инциденты», действующий при Федеральном университете Рио-Гранди-ду-Сул и наравне с правительственными центрами относящийся к внутренним группам[25].

Выделяются также национальные объединения, например, CERT.br — Центр изучения, реагирования и разрешения инцидентов Бразилии[26].

В общем, подобные центры занимаются анализом противоправной деятельности, связанной с происшествиями в сети, а также соответствующим реагированием и мерами противодействия этой деятельности. Они могут быть созданы как на уровне правительства, так и на уровне компаний и в зависимости от этого варьироваться по размерам и масштабам своих функций. Кроме того, такие центры могут носить и ситуационный характер, то есть быть «ad hoc» и создаваться под урегулирование конкретной ситуации[27]. В сентябре 2017 г. состоялся шестой Бразильский форум групп реагирования на чрезвычайные ситуации, в рамках которого особый акцент был сделан на сотрудничестве между различными группами в целях обеспечения безопасности интернет-сети[28].

Обращаясь к предпоследнему аспекту анализа, касающемуся правовой базы, отметим, что в Бразилии многие государственные структуры выступают за необходимость разработки адекватной правовой базы, которая защищала бы интересы всех пользователей сети, в том числе, например, Управление безопасности информационно-коммуникационных технологий и Центр по защите от киберугроз (CDCiber), о котором мы уже упоминали ранее. К ключевым законам в области информационной безопасности относятся Закон № 12.965/2014[29], устанавливающий принципы и гарантии использования сети Интернет в Бразилии, и Закон № 12737/12 об информационных преступлениях. Еще одним важным законом, который качественно отличает Бразилию от других стран региона, является Декларация прав для цифровой эпохи 2014 г., которая направлена на сохранение приватности в Интернете[30]. Данный закон, повествующий о будущем управления сетью Интернет, ставит Бразилию на передовые позиции в регионе в области защиты прав граждан в сети в сети[31].

Последним элементом нашего анализа является социальная составляющая, то есть степень понимания гражданами государства проблем информационной безопасности. В Бразилии показатели осведомленности населения об информационной безопасности и принципах ее обеспечения являются довольно низкими[32]. Для того чтобы исправить сложившуюся ситуацию в стране регулярно проводятся семинары и мастер-классы[33], выпускаются специализированные буклеты со всей необходимой информацией по теме. Повышается информированность частных компаний относительно необходимости иметь высокую степень защиты против возможных информационных угроз и нападений. Особое внимание уделяется защите предприятий с критической инфраструктурой. Постепенно увеличивается внутренний рынок технологий в области информационной безопасности. Ведется активная работа в сфере образования: например, в Университете Сан-Паулу предлагаются несколько программ, связанных с информационными технологиями[34].

Таким образом, несмотря на то, что Бразилия пока неизбежно сталкивается с трудностями, связанными, помимо прочего, с нехваткой технологий[35], в стране достигнут значительный прогресс в информационной области. Политика Бразилии в данной области носит очень сбалансированный и комплексный характер, ее дальнейшее развитие может существенно укрепить процессы налаживания системы предотвращения и эффективного реагирования на угрозы, возникающие в мире информационных технологий.

От стран, стоящих на передовых позициях в области информационной безопасности, таких, как Бразилия, Аргентина, Колумбия, разительно отличается Никарагуа, где ситуация с информационными технологиями в настоящее время находится в слабо развитом состоянии. Доступ к сети в стране имеют всего 19% граждан. Рост числа пользователей происходит довольно медленными темпами: за последние несколько лет он составил около 5%[36]. Серьезное препятствие для распространения Интернета в Никарагуа — высокая стоимость подключения[37]. В 2014 г. месячная стоимость высокоскоростного Интернета составила в среднем почти 16 долл., тогда как в Гондурасе — 12 долл., в Гватемале — 8 долл.[38].

Отметим, что очень многие проекты, реализовываемые в Никарагуа, являются результатом взаимодействия этого государства с другими странами, международными и региональными организациями. Одним из наиболее крупных проектов Никарагуа в области информационной безопасности стало создание в 2014 г. Центра передовых исследований высокоскоростного Интернета для развития (Centro de Estudios Avanzados en Banda Ancha para el Desarrollo, CEABAD), который был образован при поддержке Южной Кореи и Межамериканского банка развития (Inter-American Development Bank, IADB) с инвестициями около 3,2 млн долл.[39] и представляет собой одну из первых в Центральной Америке площадок для взаимодействия отраслевых специалистов. Ключевыми направлениями работы центра являются информационная безопасность, онлайн-образование и инновационное развитие городов[40].

Кроме того, в структуру Национальной полиции Никарагуа входит Центральная лаборатория криминалистики, созданная при финансовой поддержке Евросоюза. Лаборатория занимается борьбой не только с традиционными, но и с новыми вызовами безопасности, связанными с информационно-коммуникационными технологиями[41].

Правительство Никарагуа реализует ряд соглашений со Всемирным банком (World Bank, WB)[42] и IADB[43], согласно которым стране предоставляются займы на развитие высокоскоростного Интернета, прокладки оптоволокна и т.п. Палата интернет-сети и телекоммуникаций Никарагуа (Cámara Nicaragüense de Internet y Telecomunicaciones, Canitel), объединяющая сетевых операторов и интернет-компании, в мае 2017 г. выступила с инициативой установления сотрудничества с правительственными структурами в целях повышения доступности Интернета для граждан и обеспечения безопасного подключения[44].

Переходя к анализу технологического и организационного аспектов, обратим внимание на деятельность Совета по науке и технологиям Никарагуа (Consejo Nicaragüense de Ciencia y Tecnología, CONICYT), который занимается регулированием соответствующей сферы и является площадкой для взаимодействия правительства, частных компаний, университетов[45]. По линии Совета ведется работа по развитию национальной политики в области информационной безопасности и по просвещению населения по вопросам преступности в сети. Еще одной структурой, отвечающей за информационные технологии, является Комиссия электронного правительства Никарагуа (Comisión de Gobierno Electrónico de Nicaragua, GOBeNIC), в рамках которой разрабатываются проекты электронного правительства, а также ведется дискуссия между правительством страны и представителями инфраструктурных отраслей[46].

У Никарагуа пока нет определенной стратегии обеспечения информационной безопасности. Кроме того, в отличие от развитых в технологическом плане государств региона, в стране отсутствуют и группы реагирования на инциденты в сети[47].

Относительно законодательных мер стоит сказать, что при понимании необходимости вносить изменения, они происходят очень затянуто. Так, в Уголовном кодексе Никарагуа в ст. 198 вкратце сказано о мерах, которые следует принимать в случаях неправомерного доступа к информации, в ст. 245 речь идет о нанесении ущерба компьютерным системам. В 2012 г. парламент Никарагуа принял Закон о защите персональных данных, в котором изложены требования и меры наказания, предусмотренные за их нарушение[48]. В 2015 г. принят Закон о безопасности Никарагуа, в котором к угрозам причисляются «кибернетическая угроза», а также угроза нанесения ущерба критической инфраструктуре[49]. Аналогичные положения содержатся в Законе о государственной безопасности Республики Никарагуа[50].

Складывается впечатление, что на данном этапе в Никарагуа делается акцент именно на концептуализации самой проблемы, на ее обсуждении на всех возможных уровнях. О растущем интересе страны к проблематике информационной безопасности свидетельствуют многочисленные встречи и конференции[51]. Одним из мероприятий стал форум в области информационных технологий, организованный испанской корпорацией «Telefónica» в 2017 г.[52], где был отмечен прогресс, достигнутый Никарагуа в последние годы, особенно на фоне других государств Центральной Америки.

Если говорить об образовательных программах и просвещении населения, то следует отметить, что существующие проекты носят ограниченный характер. В 2015 г. правительство учредило Неделю безопасного использования Интернета. Цель данной акции, организованной министерством образования, частными компаниями и университетами, заключалась в продвижении идеи грамотного использования ИКТ, а также в гарантировании безопасности сети[53].

Изучив два государства Латинской Америки, которые находятся на разных полюсах в плане мер, предпринятых в области информационной безопасности, стоит отметить значительный отрыв, который присутствует на пути развития ИКТ-стран региона. Как правило, у наиболее развитых его стран новые институты, призванные реагировать на происшествия в сети, обычно встраиваются в структуры, существующие для борьбы с традиционными угрозами. В странах, мало развитых в технологическом отношении ситуация складывается следующим образом: в силу необходимости предпринимать хотя бы минимальные меры на данном направлении и отсутствия должных ресурсов у самого государства, такие страны прибегают к помощи других государств и международных организаций или негосударственных акторов.

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

[1] Agencia EFE. América. 16.III.2017.

[2] O.A.R o b l e s G a r a y. Evolución de Internet en América Latina y el Caribe. — Simposio Latinoamericano y del Caribe: las tecnologías de información en la sociedad. Aguacalientes, México, 1999, p. 257–264.

[3] Informe Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? — Banco Interamericano de Desarrollo (BID); Organización de los Estados Americanos. 2016, p. 9.

[4] Ibidem.

[5] Available at: https://www.efe.com/efe/america/politica/los-ciberataques-se-convierten-en-una-de-las-principales-amenazas-america/20000035-3210237 (accessed 06.09.2017).

[6] Available at: http://www.bbc.com/mundo/noticias/2015/11/151118_tecnologia_cibercrimen_ciberdelito_aumento_america_latina_lb (accessed 06.09.2017).

[7] Available at: http://www.cioal.com/2017/08/01/2017-hacia-cifras-record-40-incrementos-ciberataques-trimestre/ (accessed 06.09.2017).

[8] Available at: http://www.bbc.com/mundo/noticias/2015/11/151118_tecnologia_cibercrimen_ciberdelito_aumento_america_latina_lb (accessed 07.09.2017).

[9] Available at: https://regnum.ru/news/2275247.html (accessed 07.09.2017).

[10] Informe Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Op. cit., p. 4.

[11] Tendencias de seguridad cibernética en América Latina y el Caribe. — Organización de los Estados Americanos. 2014, p. 100; Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. — Organización de los Estados Americanos. Trend Micro, 2015, p. 60; P.E.M a r-t i n. Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos. Documento opinión. Instituto Español de Estudios Estratégicos, 2015, p. 17.

[12] Informe Índice Mundial de Ciberseguridad y Pérfiles de Ciberbienestar. ABI Research, Sector de Desarollo de las Telecomunicaciones, ITU, 2015, pp.1–2.

[13] Ibidem., p.3.

[14] Ibidem., p.19.

[15] Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015–2018: versão 1.0. Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasilia, Presidência da República, 2015.

[16] Ibidem., p.20–33.

[17] Internet World Stats, 2017.

[18] Libro Blanco de la Defensa Nacional. Brasil, 2012, p. 284.

[19] Available at: https://dialogo-americas.com/es/articles/brazilian-army-invests-cyber-defense (accessed 07.09.2017).

[20] Available at: https://firstvds.ru/technology/faq/ddos_problem (accessed 07.09.2017).

[21] Available at: https://www.tecmundo.com.br/seguranca-de-dados/116925-brasil-pais-sofre-ataques-ddos-america-latina.htm (accessed 07.09.2017).

[22] Ministerio de defensa. Proyectos estratégicos. Brasil, p. 26–27.

[23] Available at: http://www.infodefensa.com/latam/2014/02/03/noticia-discuten-brasil-sobre-defesa-cibernetica.html (accessed 07.09.2017).

[24] Available at: https://dialogo-americas.com/es/articles/brazilian-army-invests-cyber-defense (accessed 07.09.2017).

[25] Available at: https://www.cert.br/csirts/brasil/ (accessed 09.09.2017).

[26] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br).

[27] Available at: https://www.cert.br/certcc/csirts/csirt_faq-br.html (accessed 09.09.2017).

[28] Available at: https://www.nic.br/noticia/notas/6-forum-brasileiro-de-csirts-reforca-importancia-da-cooperacao-para-a-seguranca-na-internet/ (accessed 09.09.2017).

[29] Lei № 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[30] Available at; http://elcomercio.pe/mundo/latinoamerica/brasil-promulga-ley-protege-privacidad-internet-313291 (accessed 09.09.2017).

[31] Available at: http://www.redpolitica.mx/nacion/brasil-promulga-ley-de-privacidad-en-internet (accessed 09.09.2017).

[32] Available at: http://observatoriociberseguridad.com/country/br (accessed 12.09.2017).

[33] Available at: https://www.cgi.br/noticia/releases/cgi-br-e-nic-br-promovem-viii-seminario-de-protecao-a-privacidade-e-aos-dados-pessoais/ (accessed 12.09.2017).

[34] Available at: http://www.prpg.usp.br/index.php/pt-br/faca-pos-na-usp/programas-de-pos-graduacao/117-sistemas-de-informacao; http://www.prpg.usp.br/index.php/pt-br/faca-pos-na-usp/programas-de-pos-graduacao/608-ciencia-da-informacao (accessed 12.09.2017).

[35] P.C a m p o s d e O l i v e i r a. Brasil: Estrategia de seguridad y defensa (Escuela Superior de las Fuerzas Armadas), 2010.

[36] Available at: http://www.elnuevodiario.com.ni/nacionales/415534-acceso-internet-crece-pais/ (accessed 12.09.2017).
[37] Available at: http://www.laprensa.com.ni/2016/09/12/economia/2099198-nicaragua-triplica-conexion-internet-sigue-la-cola (accessed 12.09.2017).
[38] Available at: http://www.elnuevodiario.com.ni/economia/395163-internet-mas-caro-nicaragua/ (accessed 13.09.2017).
[39] Available at: http://www.elnuevodiario.com.ni/nacionales/335099-estrenan-centro-capacitacion-internacional-banda-a/ (accessed 13.09.2017).
[40] Available at: https://www.el19digital.com/articulos/ver/titulo:43552-desarrollan-taller-sobre-seguridad-informatica-en-nicaragua (accessed 13.09.2017).
[41] Available at: http://www.elnuevodiario.com.ni/nacionales/335099-estrenan-centro-capacitacion-internacional-banda-a/ (accessed 13.09.2017).
[45] Available at: https://www.interpol.int/es/Centro-de-prensa/Noticias/2016/N2016-089 (accessed 13.09.2017).
[42] Available at: http://www.centralamericadata.com/es/article/home/Nicaragua_20_millones_para_telecomunicaciones (accessed 13.09.2017).
[43] Available at: http://www.elnuevodiario.com.ni/nacionales/392933-millonaria-inversion-darmas-acceso-internet/ (accessed 13.09.2017).
[44] Available at: https://confidencial.com.ni/canitel-una-alianza-nacional-para-internet-en-nicaragua/ (accessed 13.09.2017).
[45] Available at: http://conicyt.gob.ni/index.php/quienes-somos/ (accessed 13.09.2017).
[46] Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Op. cit., p. 88.
[47] Available at: http://www.cert.org/incident-management/national-csirts/national-csirts.cfm (accessed 14.09.2017).
[48] Ley de protección de datos personales № 787, aprobada el 21 de Marzo del 2012.
[49] Available at: https://www.efe.com/efe/america/portada/aprueban-una-polemica-ley-de-seguridad-en-nicaragua-y-desaforan-a-dos-diputados/20000064-2778823 (accessed 14.09.2017).
[50] La Gaceta. Diario Oficial. 18.XII.2015, p. 240.
[51] Available at: https://www.el19digital.com/articulos/ver/titulo:24022-nicaragua-apunta-al-desarrollo-de-la-ciber-seguridad (accessed 14.09.2017).
[52] Available at: http://www.lavozdelsandinismo.com/ciencia-tecnica/2017-02-17/expertos-alaban-sistema-ciberseguridad-nicaraguense/ (accessed 14.09.2017).
[53] Available at: http://www.elnuevodiario.com.ni/nacionales/360817-inauguran-semana-uso-seguro-internet/ (accessed 14.09.2017).

Anna V.Makarycheva (makarycheva.a.v@my.mgimo.ru)
Moscow State Institute of International Relations (MGIMO-University), World politics department, post-graduate student

Information Security in Latin America: Adaptation Ways to the New Threats

Abstract. The article is aimed to study the ways of the Latin American countries adaptation to the information security threats. By analyzing two cases, Brazil and Nicaragua, the author shows the differences in the two countries' strategies of struggle against the new threats.
Key words: Latin America, the information security, Brazil, cyber crimes, Nicaragua.