ESTRATEGIAS DE SEGURIDAD CIBERNÉTICA EN LOS PAÍSES DE AMÉRICA LATINA*

Ekaterina Yu. Kosévich
Ph.D. (Politología), investigadora (ekaterina.kosevich@gmail.com)

Universidad Nacional de Investigaciones "Escuela Superior de Economía"
Federación de Rusia, 101000, Moscú, calle Myasnitskaya, 20

Recibido el 18 de noviembre de 2019

Resumen. *El artículo presenta un panorama de las estrategias de la seguridad cibernética que al día de hoy han sido adoptadas tan solo en siete países de América Latina. Se hace énfasis en los aspectos clave de las estrategias de la seguridad cibernética de Colombia, Panamá, Paraguay, Costa Rica, Chile, México y Brasil. Se exponen sus objetivos y se enumeran los servicios, organismos e instituciones encargadas de la implementación y monitoréo de los resultados obtenidos en la aplicación de las estrategias mencionadas. Se ofrecen las características del actual sistema de seguridad cibernética en Brasil, país que carga con la mayor tasa de los delitos cibernéticos cometidos en la región.*

Palabras clave: *América Latina, estrategias nacionales de seguridad cibernética, espacio informativo, tecnologías de información, seguridad cibernética, Internet*

* Artículo publicado con el apoyo financiero de Fundación Rusa para la Investigación Básica, proyecto núm. 19-114-50011.

DOI*: 10.37656/s20768400-2020-1-07*

CYBER SECURITY STRATEGIES OF LATIN AMERICA COUNTRIES*

Ekaterina Yu. Kosevich
Ph.D. (Politology), researcher (ekaterina.kosevich@gmail.com)

National Research University «Higher School of Economics»
20, Myasnitskaya, Moscow, 101000, Russian Federation

Received on November 18, 2019

Abstract. *Thanks to the active development of information technology and the creation of a global information space, the basis of which is the Internet, new opportunities have been opened to the world. However, this has led to the emergence of new types of dangers - cybercrime, cyber attacks and cyber warfare. The need to counter them, as well as the need to create a secure information environment, has led states to create their own national cybersecurity systems, as well as to adopt national strategies in this area. In most countries of Latin America, there is still no mechanism for ensuring information security, which makes them vulnerable to information attacks. The article gives an overview of national cybersecurity strategies that have been approved in only seven countries of region. The paper highlights key aspects of the cybersecurity strategies of Brazil, Colombia, Panama, Paraguay, Chile, Costa Rica and Mexico. Their main goals are examined, and the relevant services, bodies and institutions responsible for the implementation and monitoring of the results of these strategies are listed.*
Keywords: *Latin America, national cybersecurity strategies, information space, information technology, cybersecurity, Internet*

* Acknowledgments: The reported study was funded by RFBR, project number 19-114-50011.

DOI: *10.37656/s20768400-2020-1-07*

СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ СТРАН ЛАТИНСКОЙ АМЕРИКИ*

Екатерина Юрьевна Косевич
Канд. полит. наук, научный сотрудник (ekaterina.kosevich@gmail.com)

Национальный исследовательский университет
«Высшая школа экономики»
РФ, 101000, Москва, Мясницкая, д. 20

Статья получена 18 ноября 2019 г.

Аннотация. *В статье дается обзор национальных стратегий кибербезопасности, которые на сегодняшний день были утверждены лишь в шести странах Латинской Америки. В работе освещены ключевые аспекты стратегий кибербезопасности Колумбии, Панамы, Парагвая, Коста-Рики, Чили и Мексики. Рассматриваются их цели,*

перечисляются соответствующие службы, органы и институты, ответственные за реализацию и мониторинг результатов указанных стратегий. Дается характеристика современной системы национальной кибербезопасности, созданной в Бразилии, на долю которой приходится наибольшее число кибер-преступлений своего региона.

Ключевые слова: *Латинская Америка, национальные стратегии кибербезопасности, информационное пространство, информационные технологии, кибербезопасность, интернет*

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-114-50011.

DOI*: 10.37656/s20768400-2020-1-07*

La segunda década del siglo XXI se caracteriza, entre otras cosas, por una mayor introducción de las tecnologías de información (TI). La pujante incorporación de las tecnologías de computación al ámbito social, político-económico e incluso militar las ha hecho vulnerables a los ataques cibernéticos. Tal circunstancia, a su vez, ha planteado la necesidad de buscar nuevos enfoques y soluciones tecnológicos que sean capaces de garantizar la seguridad de información.

América Latina, que de momento atrasa notablemente de los países occidentales en la implementación de las tecnologías de información, transformación digital y digitalización, tampoco es ajena a los problemas de esta índole. En los últimos cinco años la cantidad de los ataques cibernéticos en la región aumentaron en 40%, lo que significa que se producen más de 700 millones de ataques al año [1, 2, pp. 12-46]. El número de los ataques cibernéticos contra las instituciones financieras en América Latina ha crecido en 50% [3]. Anualmente, los ciberdelitos les causan daño a los países de América Latina por un monto de US$90 mil millones [4, 5]. Los tres países que acumulan el

mayor número de los delitos cibernéticos son: Brasil (recibe el 55% de todos los ataques que se cometen en la región), México (es blanco del 17% de los ataques) y Colombia (el 9%) [6].

En una investigación conjunta, llevada a cabo en 2016 por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se destaca que 16 de los 32 países de América Latina y el Caribe son totalmente incapaces de contrarrestar los ataques cibernéticos [7, pp. 180-185].

Aun así, tan solo siete países latinoamericanos han diseñado estrategias nacionales para proteger su espacio informativo. Se trata de Brasil, que desde los años 2000 ha ido elaborando políticas de Estado en este campo; Colombia, que no solo había logrado adoptar semejante estrategia en 2011, sino que la renovó en 2016; Panamá, que elaboró su plan de seguridad del espacio cibernético en 2013; Paraguay, Chile y Costa Rica, que en abril de 2017 anunciaron simultáneamente estrategias propias de la seguridad cibernética; y México, que fue el último en su región en tener proyecto estratégico nacional (fue presentado en noviembre de 2017) [8].

Tan escaso número de los países involucrados en la formación de los sistemas de seguridad cibernética nacional que para ellos ya se ha tornado un problema estratégico de importancia estatal [9, 10], puede explicarse por la *insuficiencia de los recursos financieros* que se asignan para la solución de esta clase de problemas, *falta de experiencia práctica y* evidente *escasez de conocimientos especiales* necesarios para la elaboración e implementación de tales medidas. Todo esto en su conjunto impide que semejantes conceptos sean adoptados en el marco de toda la región [11, pp. 37-56, 12].

Las concepciones de los países latinoamericanos respecto a la lucha contra los riesgos provenientes del ambiente

informativo, así como sus estrategias nacionales de seguridad cibernética iban formándose bajo influencia conceptual de los EE.UU. [13]. Pero, a diferencia de las estrategias norte-americanas, enfocadas al dominio geopolítico global, los conceptos latinoamericanos son de carácter defensivo, pues están orientadas justamente a contrarrestar amenazas potenciales [14].

En el marco de la región la OEA desempeña un papel importante prestando consultaría en esta esfera. En particular, su iniciativa "Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo" (CICTE) ya se ha convertido en el líder regional en cuanto a las iniciativas de investigación, al fortalecimiento del potencial técnico y elaboración de las políticas regionales comunes destinadas a resguardar la información [15]. Este proyecto tiene por objetivo elaborar conceptos, desarrollar el potencial (enseñanza y entrenamientos en el ámbito de la defensa cibernética), además de realizar investigaciones científicas y divulgar sus resultados [16, 17, pp. 14-25].

COLOMBIA

A fines de la primera década del siglo XXI, el gobierno colombiano intentó frenar el crecimiento de los delitos cibernéticos, que anualmente afectaban las compañías tanto colombianas como internacionales que operaban en el país, y definió el restablecimiento de la seguridad del espacio digital como una de sus tareas estratégicas [18, 19, pp. 12-24]. Colombia fue el primer país de América Latina en adoptar, en 2011, variante completa de la Estrategia nacional de seguridad cibernética. Transcurridos cinco años, en la primavera de 2016,

en este país suramericano fue adoptada una nueva versión de la estrategia que se denominó "Política Nacional de Seguridad Digital" [20]. El renovado plan cambió de manera patente los enfoques y conceptos del documento anterior, al incluir un apartado "gestión de riesgo" que pretende encontrar *equilibrio* entre la evaluación de las probables amenazas y los costes de su eliminación.

El proyecto tenía como objetivo principal disminuir la eficacia de las amenazas cibernéticas mediante el desarrollo del potencial de sus posibles víctimas, así como detectar oportunamente los riesgos para la seguridad informativa y saber manejarlos [21, pp. 22-36]. El rasgo distintivo de la estrategia fue la incorporación de los detalladamente elaborados cronograma de implementación y esquema de financiamiento [22].

El documento establece cinco ejes estratégicos: *el desarrollo coordinado* de todas las partes interesadas bajo la dirección del Estado; *elaboración de la base jurídica* de la seguridad informativa; *manejo sistematizado de los riesgos; formación de la cultura ciudadana en la esfera de la seguridad cibernética* por medio de acrecentar el nivel de los conocimientos de la sociedad en dicho ámbito; *desarrollo del potencial de todas las partes interesadas* en el manejo de los riesgos. Todo esto debe conducir al crecimiento paulatino de la economía nacional digital y a la prosperidad económica del país.

El plan comprende cinco tareas auxiliares:

Creación por el Estado del fundamento institucional para la seguridad cibernética. Con tal fin se procede a instituir el cargo de Coordinador Nacional para la Seguridad Informativa, que debe ser desempeñado por un funcionario del Departamento de Planificación Nacional. Entre sus funciones figuran la dirección

y monitoreo de la implementación de la estrategia, además de la distribución de los deberes entre todos los ministerios y órganos administrativos del poder en lo que la seguridad cibernética ataña. Ha sido creada la Comisión Nacional Digital y de Información Estatal que es la máxima instancia encargada de las tecnologías de información en el país.

Formación de condiciones adecuadas que permitan a todas las partes interesadas manejar los riesgos para la seguridad informativa dentro del marco de sus actividades económicas. El gobierno colombiano se encargará de asegurar el cumplimiento de esta tarea.

Desarrollo de la cooperación público-privada en el ámbito de información, tanto a nivel nacional como internacional.

Fortalecimiento de la defensa nacional y de la soberanía en el espacio informativo. Se trata de elaborar los métodos y medios ultramodernos en los ámbitos de prevención, detección, localización, reacción, recuperación y defensa, así como preservar la integridad y elevar el nivel de resistencia a los ataques cibernéticos contra los elementos de la infraestructura de importancia vital (su listado preciso no existe de momento). En el país ya ha sido creado el *Equipo de Seguridad Informática para la Reacción a Incidentes* (ESIRI), grupo de expertos en seguridad cibernética encargado de recoger la información sobre los incidentes cibernéticos para luego clasificarlos y neutralizarlos. El ESIRI actúa bajo la dirección de la Corporación Financiera Colombiana y de la Presidencia de la República [23]. Cabe destacar que los países latinoamericanos prefirieron seguir el ejemplo de los EE.UU., donde la creación de tales equipos es tradicionalmente financiada por entidades de Estado, y no él de la Unión Europea, donde la mayoría de los

ESIRI son creados por universidades y grandes TI compañías [24, 25].

La última tarea auxiliar fue la *creación de mecanismos permanentes* para el desarrollo de la cooperación en el campo de la seguridad de información a niveles tanto nacional como internacional. En este sentido, Colombia se dispone a sumarse a las convenciones internacionales sobre la seguridad informática y garantizar su cumplimiento.

Los organismos competentes, a cuyo cargo corre la implementación de este proyecto, son el Ministerio de Defensa Nacional, Departamento Nacional de Planeación y Ministerio de Tecnologías de la Información y Comunicaciones.

PANAMÁ

De conformidad con el Índice Nacional de Seguridad Cibernética (NCSI),[*] según los datos de 2019, Panamá devino uno de los países líderes en América Latina en cuanto al grado de preparación para contrarrestar los ciberataques. El país se destaca de entre los demás países de la región tanto por alto nivel de desarrollo de las tecnologías de información como por su afán de lograr una mayor integración en la industria de las innovaciones a escala global [26, pp. 37-42].

La estrategia panameña es muy breve y lacónica. Todo el plan estratégico cabe en 10 páginas. Ello se debe a que el país ya cuenta con una base jurídica bien detallada que regula la seguridad de información [27].

[*] El NCSI forma parte de la estrategia de la "e-Governance Academy", independiente organización no-lucrativa fundada en 2002 en el marco del Programa de Desarrollo de la ONU, Instituto de Sociedad Abierta y Gobierno de Estonia.

En la estrategia se podría destacar los siguientes momentos clave. En particular, el objetivo fundamental del Estado en materia de la seguridad cibernética es elevar el nivel de la cooperación entre la población, sector comercial y Estado [28].

Como se ha señalado arriba, este documento no especifica los principios básicos. Tampoco tiene indicadas tareas detalladas. Pero sí contiene enumerados seis "pilares" en los que se sustenta la política del Estado en este ámbito: *la protección de la vida privada y de los derechos fundamentales del ciudadano* en el ciberespacio*; prevención y represión de los delitos en el espacio cibernético; fortalecimiento de la seguridad cibernética de los elementos de la infraestructura de importancia vital del país,* lo que se logra mediante una colaboración más estrecha entre los sectores público y privado y por medio de ejercicios antiaverías masivos; *asistencia para desarrollar un clima empresarial estable y competitivo* en la esfera de la seguridad cibernética, para lo cual el Estado trazaría un plan de actividades a ser implementadas en conjunto con empresas públicas; *desarrollo de una cultura de seguridad de información;* así como *mejoramiento de la seguridad cibernética de los organismos de Estado* por medio de aumento de la celeridad de respuesta a los ataques hacker.

Las órganos oficiales de Panamá en este campo son la Dirección Estatal de Innovaciones, el Consejo Nacional de la Política Estatal para el Desarrollo de las Innovaciones y CSIRT Panamá [29].

PARAGUAY

Precisamente en Paraguay, en el período 2010-2014, hubo el mayor crecimiento de los usuarios de Internet en América Latina [30, pp. 102-114]. A raíz de tal circunstancia, la dirigencia del

país decidió fortalecer la seguridad de información adoptando, en 2017, la estrategia correspondiente [31].

A diferencia de las estrategias de la seguridad cibernética de la mayoría de los países de América Latina, en las cuales se define sólo un objetivo fundamental teniendo otras metas de carácter auxiliar, la versión paraguaya contiene 7 objetivos fundamentales divididos en 20 submetas.

Los objetivos principales consisten en: *propagar la cultura de la seguridad cibernética,* a la vez que *profundizar los conocimientos de la población* sobre el empleo seguro de las tecnologías de Internet; *promover los proyectos "Investigación, Diseños e Innovaciones"* intensificando la interacción entre los sectores estatal y privado, entre los ciudadanos y círculos académicos; *defender la infraestructura informativa de importancia vital* compartiendo los operadores de comunicaciones privados y el Estado la responsabilidad respecto a su seguridad; *reaccionar con la mayor eficacia a los incidentes cibernéticos* mediante la asignación de considerables recursos estatales al Centro de Monitoreo y Respuesta a los Ataques Informáticos de Paraguay CERT y PY); *financiar y proveer del equipo necesario* a todas las organizaciones encargadas de investigar los delitos cibernéticos; *impartir cursos de capacitación en los temas de las TI* para los funcionarios de las instituciones que administran la justicia, así como *robustecer la colaboración internacional* en los temas de la lucha contra los delitos cibernéticos; *crear una infraestructura de información* capaz de garantizar un espacio informativo seguro.

La estructura institucional de la seguridad cibernética consta del Coordinador Nacional, con la función de efectuar el monitoreo y control del cumplimiento de la estrategia, así como

de la Comisión Nacional para la Activación de la Colaboración en la Seguridad Cibernética.

COSTA RICA

Hoy día, Costa Rica es el segundo exportador de los *software* en América Latina después de Uruguay [32]. El mercado costarricense de *software* aporta más del 1,7% del PIB del país [33]. En Costa Rica hay más de 1500 empresas, cuyas actividades están ligadas a la elaboración de los programas informáticos, siendo los EE.UU. el comprador principal [34].

El país ya cuenta con experiencia en la creación de la base jurídica e institucional que coordina la labor de la industria de las TI. La Cámara de Tecnologías de Información y Comunicación (CAMTIC) fue creada todavía en el año 1998 como entidad no-lucrativa para representar y defender los intereses de la rama [35]. En 1999 se lanzó el proyecto "PRO-SOFTWARE" cuyo objetivo fundamental era crear condiciones favorables para las compañías que actúan en la rama de las TI. En 2003 fue adoptado el Plan Estratégico de Desarrollo de la Industria de Software [36].

El propósito primordial de la estrategia de la seguridad cibernética de Costa Rica es la elaboración de un sistema de medidas encaminadas a lograr utilización segura de las TI, desarrollar cooperación entre las numerosas partes interesadas y promover actividades educativas en la esfera de información [37].

Dicho propósito viene dividido en ocho submetas: *lograr la coordinación de las actuaciones de todos los agentes de la economía nacional; elevar el nivel de los conocimientos de la población* sobre la seguridad informativa; *desarrollar el*

potencial de Costa Rica en el terreno de la seguridad cibernética, incluyendo la realización de actividades educativas e informativas para los funcionarios públicos; *crear una eficiente base jurídica-normativa* en materia de la seguridad cibernética y las Tecnologías de Información y Comunicación (TIC); *alcanzar un nuevo nivel de resistencia de la infraestructura informativa de importancia vital contra los ataques cibernéticos; manejar los riesgos de información* elevando el grado de protección de las tecnologías de información empleadas por entidades públicas y grandes organizaciones privadas; *dinamizar la cooperación internacional; implementar gradualmente la Estrategia, ejercer control sobre su cumplimiento y evaluar los resultados obtenidos.*

El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el principal organismo responsable de las políticas en el campo de la seguridad cibernética. Adjunto al Ministerio se instituye el cargo de Coordinador Nacional con la función de evaluar el grado del cumplimiento de las tareas asignadas. El Centro de Reacción a los Incidentes de la Seguridad de Información, creado en 2012, se encarga de detectar, prevenir y eliminar las secuelas de los ataques cibernéticos. Ha sido constituido el Comité Consultivo, órgano especial conformado por representantes del MICITT, Poder Judicial, Superintendencia de Comunicaciones, sociedad civil, científicos y sector empresarial.

Es remarcable que la estrategia de la seguridad cibernética de Costa Rica no fija los plazos y fases de su realización; tampoco contiene un apartado que determine los recursos que hayan de asignarse para llevarla a la práctica.

CHILE

La rama de las tecnologías de información ocupa un lugar importante en la economía de Chile. Las compañías chilenas que operan en este sector, exportan en promedio US$340 millones al año, siendo los países de América Latina, los EE.UU. y Europa sus clientes principales [38]. En 2001 fue creada la Asociación Chilena de Empresas de Tecnologías de Información que promueve los intereses del sector. En 2005 quedó instituido el Consejo Nacional de Innovación para la Competitividad que se encarga de trazar las políticas de Estado en la esfera de las TI. Chile forma parte de los países más avanzados de América Latina en cuanto al índice de cobertura del Internet: superior al 70% de la población. Todo esto ha ido planteando la necesidad de elaborar la política nacional de seguridad cibernética [39, pp. 11-27].

En la estrategia de seguridad cibernética chilena están detalladamente descritos las prioridades a mediano y corto plazo, así como se enumeran las instituciones responsables de su implementación práctica [40].

El año 2022 se fija como el límite máximo para alcanzar los cinco objetivos fundamentales, cada uno de los cuales contiene submetas. Dichos objetivos consisten en *crear una infraestructura de las TIC* que sea apta para contrarrestar los ataques cibernéticos de distinto grado de complejidad; *garantizar los derechos humanos y las libertades civiles en el espacio cibernético; formar una cultura de seguridad cibernética en la sociedad* informando a los usuarios de las TIC tanto sobre los riesgos y amenazas como sobre la responsabilidad jurídica por los delitos cibernéticos; *ampliar la cooperación internacional en el campo de la seguridad*

cibernética; *ensanchar el mercado de la seguridad cibernética* de Chile en general.

La estructura institucional la encabeza el Comité Interdepartamental para la Seguridad Cibernética que coordina las actividades y evalúa los resultados alcanzados. La solución de las cuestiones técnicas, tales como el manejo de los incidentes cibernéticos, la tiene a su cargo el equipo nacional del CSIRT. Además, se planea crear a corto plazo el Consejo Consultivo como órgano especializado en el tema.

MÉXICO

La industria de las Tecnologías de Información y Comunicaciones desempeña un papel relevante en el desarrollo de la economía mexicana. La esfera de las TIC proporciona puestos laborales a más de 76 mil personas, mientras que su tasa de crecimiento en la última década sobrepasa lá del crecimiento económico de México [41]. México tampoco ha evitado el problema de la delincuencia cibernética: en los US$3 mil millones se estima el daño que éste le causa anualmente al país [42]. Justamente México ha sido la fuente principal de los envíos de las cartas *spam* en la región, además de ser el receptor del 53% de todos los programas virus que se lanzan en el mundo [43]. Esto ha llevado a que el Estado y el empresariado se han dado cuenta de lo importante que es el tema de la seguridad cibernética. Ya hacia 2019, México se tornó el líder regional por el índice de las inversiones en la industria de la seguridad digital [44].

De todos los países latinoamericanos mencionados en esta investigación, México ha sido el último en adoptar la estrategia nacional propia de la seguridad cibernética [45]. Dicho

documento le da prioridad al fortalecimiento de la seguridad informativa, lo que permitirá tanto a los ciudadanos como a las organizaciones públicas y privadas hacer uso responsable de las TIC para lograr las metas del desarrollo sostenible del país [46].

La variante mexicana de la estrategia establece ocho ejes fundamentales de las actividades[*]: *el desarrollo de la cultura de seguridad cibernética; incremento del potencial,* entendido como un conjunto de las actividades orientadas a desarrollar el capital humano, TI, recursos y organizaciones en el campo de la seguridad cibernética; *coordinación eficiente; aplicación del modelo trisectorial "*Investigaciónes-Diseños-Innovaciones" con el empleo de recursos presupuestarios; *la elaboración e introducción de los más novedosos estándares y reglamentos técnicos* que permitan adaptar las mejores soluciones aplicadas en el terreno de la seguridad cibernética; *la protección de la infraestructura de importancia vital; creación de la base jurídica y normativa; recopilación de la estadística y ejecución del monitoreo de las acciones encaminadas a lograr los objetivos fundamentales,* que permitan evaluar la eficacia de la Estrategia y determinar el grado de su influencia en el desarrollo.

La misión de implementar y renovar el proyecto, además de coordinar las labores gubernamentales en este ámbito, está asignada al Subcomité de Seguridad Cibernética, creado en octubre de 2017. El organismo se halla subordinado a la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) y está integrado por varias dependencias especializadas.

[*] Nota: en el documento se subraya que todas las actividades indicadas serán implementadas de conformidad con la "Ley de Seguridad Nacional" (aprobada el 31 de enero de 2005).

BRASIL

El sistema de la seguridad cibernética nacional de Brasil ha ido formándose bajo la influencia de diferentes factores. Entre ellos, el preocupante auge del número de los ataques *hacker*, sin que el país tenga la capacidad de hacerles frente, y el deseo de no quedarse a la zaga de las mayores potencias mundiales en la lucha contra las amenazas cibernéticas que hoy día se lleva a cabo [47]. Al mismo tiempo, en Brasil ha habido un considerable crecimiento del número de las personas que tienen acceso al Internet: hoy la red abarca a más del 70% de la población.

El diseño de la política en el ámbito de la defensa cibernética en Brasil se llevó a cabo en el contexto de las iniciativas que propugnaban la tarea de fortalecer el potencial de la defensa nacional. Dentro del gobierno federal se creó un sistema jerárquico de toma de las decisiones estratégicas, desde el Presidente de la República y la Agencia Brasileña de Inteligencia hasta el Gabinete de Seguridad Institucional de Presidencia de la República [48, pp. 10-15]. Los encargados de coordinar el plan de actividades en materia de la protección de información fueron el Centro de Defensa Cibernética y el Ministerio de Justicia que actúa en esa esfera por conducto de la policía federal. Sin embargo, no ha sido creada una agencia especializada que se ocupe de la implementación de la política estatal en cuanto a la seguridad cibernética [49, pp. 98-110].

La tarea principal de la política de seguridad cibernética de Brasil consiste en elevar el nivel de la protección de la infraestructura vitalmente importante y de los organismos del poder público [50, 51]. Entre sus objetivos básicos se puede mencionar él de incrementar el volumen de los recursos

presupuestarios para las tareas de la seguridad cibernética y él de conseguir un alto nivel de protección de las instituciones gubernamentales.

Dentro del sistema de las Fuerzas Armadas la jefatura en esta esfera le pertenece al Centro de Defensa Cibernética (Ciberdefensa) bajo cuyo mando se encuentran el Centro de Estudio, Respuesta y tratamiento de Incidentes de Seguridad, Servicio Federal de Procesamiento de Datos y varios centros de investigaciones creados adjunto al gobierno y a otros organismos del poder público [52, pp. 57-60, 53].

La política brasileña en este campo se basa en la "Estrategia de la Defensa Nacional" adoptada en 2008 y modernizada en 2012. Fue precisamente en dicho documento donde la seguridad cibernética pasó a calificarse como una de las tareas estratégicas de Brasil [54, pp. 13-25]. Las facultades en el campo de la defensa cibernética fueron delegadas al ejército. En 2012, el Ministerio de Defensa de Brasil adoptó la "Política de Seguridad Cibernética" en la que fijó los principios rectores, objetivos y actividades obligatorias.

En la "Estrategia para la Seguridad de Información y Comunicaciones y para la Seguridad Cibernética de la Gestión Pública Federal (2015-2018)" se definen los principales propósitos y tareas estratégicos para garantizar la seguridad de información, aunque se pasan por alto las cuestiones relacionadas con la defensa del país [55, pp. 110-121]. Se perfiló como la tarea prioritaria promocionar a Brasil como actor global en materia de la seguridad cibernética. Según lo planeado, este cometido sería cumplido mediante incremento acelerado de inversiones internas en las TI, creación de puestos de trabajo, así como establecimiento de relaciones de socios entre los sectores público y privado. Se propone adoptar en el futuro cercano la

estrategia nacional integral en el ámbito de la seguridad cibernética [56, 57].

A diferencia de otros países latinoamericanos analizados en el presente artículo, Brasil, por medio de su actual política de la seguridad cibernética, aspira a ser un importante actor internacional en este campo. A esta tarea el gobierno brasileño brinda atención especial [58, 59, 60, pp. 110-134].

* * *

Resumiendo cabe señalar que las élites políticas de los países latinoamericanos ya no pueden hacer caso omiso al hecho de que la cantidad de los delitos cibernéticos crece cada año. Ellas han tomado conciencia de la necesidad de adaptar estrategias claras y definidas, crear una infraestructura de seguridad cibernética, optimizar los recursos de la defensa cibernética, así como realizar labores coordinadas entre los organismos de Estado, sector privado y sociedad. Y a pesar de que en América Latina el nivel de la seguridad cibernética actualmente es bastante bajo, la región está en avance activo, creando gradualmente un ambiente informativo más coordinado y de mayor confianza, gestionado conjuntamente por todos los miembros de la sociedad.

Bibliografía References Библиография

1. América Latina registró en 2017 unos 677 millones de ataques informáticos. Available at: 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. Alexander, J. The civil sphere. New York, 2006, 791 p.

3. Ciberseguridad en Latam. Available at: https://www.forbes.com.mx/ciberseguridad-latam-mercado-millonario-insuficiente/(accessed 15.08.2019).

4. OEA: Ciberdelito. Available at: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16 (accessed 11.09.2019).

5. Finnemore M., Hollis Duncan B. Constructing Norms for Global Cybersecurity. *The American Journal of International Law*, 2016, vol. 110, num. 3, pp. 425-79.

6. ¿Hay que preocuparse por la ciberseguridad en América Latina? Available at: https://es.platinumplaycasino.com/blog/hay-que-preocuparse-por-la-ciberseguridad-en-america-latina/ (accessed 15.08.2019).

7. Informe Ciberseguridad 2016. Banco Interamericano de Desarrollo (BID). Organización de los Estados Americanos. Marzo 2016, 193 p.

8. Aranda Bustamante G., Riquelme Rivera J, Salinas Cañas S. La Ciberdefensa Como Parte de La Agenda de Integración Sudamericana. *Línea Sur*. Ecuador, 2015, vol. 9, pp. 100-116.

9. Balzacq Th., Dunn Cavelty M.A Theory of Actor-Network for Cyber-Security. *European Journal of International Security*, 2016, vol. 1, num. 2, pp. 176-198.

10. Hernández J.C. Estrategias nacionales de ciberseguridad en América Latina. Universidad de Granada. Análisis GESI, 2018, num. 8, pp. 54-69.

11. Betz D. J., Stevens T. Cyberspace and the State. Toward a Strategy. Cyber-Power, Routledge, London, 2011, 160 p.

12. Buchanan B. Cryptography and Sovereignty. *Survival*, 2016, vol. 58, num. 5, pp. 95-122.

13. Vargas R., Recalde I., Reyes, R. Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. *Revista Latinoamericana de Estudios de Seguridad*, 2016, num. 20, pp. 31-45.

14. Caro M. Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. España: Ministerio de Defensa. *Cuadernos de estrategia*, 2010, num. 147, pp. 49-82.

15. El programa de Ciberseguridad del CICTE. Available at: http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp (accessed 25.08.2019).

16. Torres M. Ciberguerra. Manual de Estudios Estratégicos y Seguridad Internacional. Madrid, 2013, pp. 329-348.

17. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. España: Ministerio de Defensa. *Cuadernos de estrategia*, 2010, num. 149, 352 p.

18. Ochoa P. Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL - RTE*, 2015, num. 28(3), pp. 1-17.

19. Requena Santos F. Redes sociales y sociedad civil. Madrid: Centro de Investigaciones Sociológicas, Colección Monografías, 2008, 183 p.

20. Política nacional de seguridad digital. Documento CONPES. Consejo nacional de política económica y social. República de Colombia. Bogotá, D.C. Borrador, num. 2, 2016, 95 p.

21. Политические конфликты в Латинской Америке: вызовы стабильности и новые возможности. Отв. ред. З.В. Ивановский. Москва, ИЛА РАН, 2017, 452 с. [Politicheskie konflikty v Latinskoy Amerike: vyzovy stabil'nosti i novye vozmozhnosti. [Political conflicts in Latin America: challenges to stability and new opportunities. Z.V. Iwanowski (ed.). Moscow, ILA RAN, 2017, 452 p. (In Russ.)].

22. Bernal P. Data Gathering, Surveillance and Human Rights: Recasting the Debate. *Journal of Cyber Policy*, Taylor and Francis Online, U.S., 2016, vol. 1, num. 2, pp. 243-64.

23. Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Available at: http://www.colcert.gov.co. (accessed 25.08.2019).

24. Campbell-Verduyn, M., Goguen, M. Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance. Campbell-Verduyn, M. Routledge. London, 2018, pp. 69-87.

25. Beveridge R., Kern K. The Energiewende in Germany: Background, Developments and Future Challenges. *Renewable Energy Law and Policy Review*. Berlin, 2013, vol. 4, num. 1, pp. 3-12.

26. Choucri N. Cyberpolitics in International Relations. *The MIT Press*, Cambridge, Massachusetts, 2012, 320 p.

27. Vila Seoane M. Digitalización, automatización y empresas transnacionales de seguridad privada en áreas con capacidad estatal limitada. *Revista de Relaciones Internacionales, Estrategia y Seguridad*. Bogotá, 2018, vol. 13, num. 2, pp. 17-21.

28. Estrategia nacional de seguridad cibernética y protección de infraestructuras críticas de Panamá. *Gaceta Oficial Digital*, Viernes 17 de mayo de 2013, num. 27289-A. Available at: https://sherloc.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf (accessed 15.08.2019).

29. OEA y Cisco unidos en la creación de Consejos de Innovación en Ciberseguridad en América Latina. Available at: https://digitalpolicylaw.com/oea-y-cisco-unidos-en-la-creacion-de-consejos-de-innovacion-en-ciberseguridad-en-america-latina/ (accessed 18.11.2019).

30. Bijker Wiebe E., Hughes Thomas P. The Social Construction of Technological Systems. *The MIT Press*. Cambridge, Massachussetts, 2012, 405 p.

31. Plan Nacional de Ciberseguridad de Paraguay. 2017. Available at: http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg (accessed 15.08.2019).

32. Vallés L. La ciberseguridad en el mundo actual. *TINO Revista informática – tecnológica*. La Habana, 2016, num. 50, pp. 585-620.

33. Por qué Uruguay es el principal exportador de software per cápita en América Latina. Available at: 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).

34. Borelli D. International Trading of Big Data. *Athens Journal of Law*. Athens, 2017, vol. 3, num. 1, pp. 21-30.

35. Chapron G. The environment needs cryptogovernance. *Nature*, Springer. Berlin, 2017, vol. 545, num. 7655, pp. 403-405.

36. Galán C. La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad*. Lima, 2016, num. 47, pp. 293-306.

37. Estrategia Nacional de Ciberseguridad de Costa Rica. 2017. Available at: https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf (accessed 15.08.2019).

38. Carlini A. Ciberseguridad: un nuevo desafío para la comunidad internacional. IEEE, Documento de opinión, 2016. Madrid, num. 67, pp. 1-16.

39. Ciberpolítica: las nuevas formas de acción y comunicación políticas. Valencia, España: Tirant Humanidades, 2013, 328 p.

40. Gobierno de Chile. Política Nacional de Ciberseguridad. 2017. Available at: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf (accessed 10.06.2019).

41. Carr M. Power Plays in Global internet Governance. Millennium: Journal of International Studies. Prague, 2014, vol. 43, num. 2, pp. 640-659.

42. La ciberseguridad en Mexico debe atenderse de forma prioritaria. Available at: https://elceo.com/tecnologia/la-ciberseguridad-en-mexico-debe-atenderse-de-forma-prioritaria-expertos/ (accessed 15.08.2019).

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

44. Rodríguez P. ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades*. Sevilla, 2016, num. 18(36), pp. 391-415.

45. Gobierno de México. Estrategia de Ciberseguridad. 2017. Available at: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (accessed 01.08.2019).

46. Deibert R. The Geopolitics of Cyberspace after Snowden. *Current History*. Philadelphia, PA, 2015, vol. 114, num. 768, pp. 9-15.

47. De Tomas S. Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. *Revista ICADE*. Madrid, 2014, num. 92, pp. 14-47.

48. Ibarra V., Nieves M. La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. *Memorias "VIII Congreso de Relaciones Internacionales"*. Universidad Nacional de La Plata, Argentina, 2016, 16 p.

49. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. España: Ministerio de Defensa. *Cuadernos de estrategia*. Madrid, 2010, num. 149, 352 p.

50. La política brasileña de ciberseguridad como estrategia de liderazgo regional. Luisa Cruz Lobato. *Revista Latinoamericana de Estudios de Seguridad*. Quito, 2017, num. 20, pp. 16-30.

51. Ablon L., Libicki M.C., Golay A.A. Markets for Cybercrime Toolsand Stolen Data: Hackers' Bazaar. *National Security Research Division*. Santa Monica, CA, 2014, num. 5, pp. 42-51.

52. Betz D.J., Stevens T. Cyberspace and the state: Toward a Strategy for Cyber-power. Adelphi, Routledge, London, 2011, 157 p.

53. Betz D.J., Stevens T. Analogical reasoning and cyber security. *Security Dialogue,* 2013, Thousand Oaks, CA, num. 1, pp.147-164.

54. Clarke R.A., Knake R.K. Cyber War: The Next Threat to National. Security and What To Do About It. New York, NY: Ecco, 2010, 51 p.

55. De Nardis L. Protocol Politics: The Globalization of Internet Governance. Cambridge: MIT Press, 2009, 288 p.

56. Deibert R.J., Rohozinski R. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*. Oxford, Oxford Press, 2010, num. 6, pp. 15-32.

57. Dunn Cavelty M., Jaeger M.D. (In)visible Ghosts in theMachine and the Powers that Bind: The Relational Securitization of Anonymous.

International Political Sociology. Oxford, Oxford Press, 2015, num. 1, pp. 176-194.

58. Dunn Cavelty M. The Normalization of Cyber-International Relations. *ATH Zurich,* CSS. Zurich, 2015, pp. 1-15.

59. Robles M. El ciberespacio: presupuestos para su ordenación jurídico-internacional. *Revista Chilena de Derecho y Ciencia Política.* Universidad Católica de Temuco, 2016, vol. 7, num. 1, pp. 17-32.

60. Blank L. R. Cyberwar versus Cyber Attack: The Role of Rethoric in the Application of Law to Activities in Cyberspace. En Ohlin J.D., Govern K, Finkelstein C. (ed.). Cyberwar. Law and Ethics for Virtual Conflicts. Oxford, Oxford University Press, 2015, 237 p.