Макарычева Анна Владимировна

Московский государственный институт

международных отношений (университет)

Министерства иностранных дел Российской Федерации

аспирант кафедры мировых политических процессов; помощник директора Центра информационной безопасности и научно-технологической политики МГИМО МИД России

[makarycheva.a.v@my.mgimo.ru](mailto:makarycheva.a.v@my.mgimo.ru)

**Информационная безопасность в Латинской Америке: пути адаптации к новым угрозам**

* Информационная безопасность в современном мире становится той темой, которая затрагивает всё большее число государств и регионов, неизбежно привлекая внимание своей масштабностью и многоплановостью. Латинская Америка не стала исключением, напротив, современные вызовы безопасности в лице информационных угроз вызывают всё большую обеспокоенность в регионе, а также осознание того, что вновь и вновь возникающие проблемы необходимо решать. Главный вопрос заключается в путях и методах решения этих проблем.
* Для того чтобы понимать, в какой степени то или иное региональное государство подготовлено к отражению возможных нападений в Интернет-пространстве, можно условно разделить все страны Латинской Америки на две группы: к первой группе будут относиться те государства, у которых есть национальная программа в области информационной безопасности, ко второй – те, которые по ряду причин пока не успели её выработать.
* Важно отметить, что, как и развитие сети Интернет, так и тем более отражение новых угроз, возникающих на пространстве этой сети происходит в Латинской Америке крайне неравномерными темпами, что, в свою очередь, напрямую сказывается на безопасности региона в целом. Так, больше половины стран на сегодняшний день не обладают даже национальными программами по отражению угроз в информационной сфере, что тормозит и общерегиональные инициативы.
* Представляется целесообразным изучить систему мер противодействия информационным угрозам одного из государств с национальной программой, а также одного из тех, где она отсутствует, и сопоставить эти методы, понять, как два типа региональных государств адаптируются к новым реалиям, как решают новые проблемы на различных уровнях.
* В качестве яркого примера государства не только с созданной, но и с качественно проработанной национальной программой, можно привести Бразилию. В этом региональном государстве уже на современном этапе в рамках противодействия киберпреступности ведётся скоординированная работа воздушных, морских сил и армии, осуществляющих свою деятельность в рамках Управления по защите от киберугроз. Такие совместные действия позволяют выработать более отлаженные механизмы по предотвращению новых вызовов и по борьбе с ними. Подобное совмещение усилий является в Бразилии одним из первых прецедентов такой тесной взаимосвязи, которая в дальнейшем будет только расширяться.
* В качестве примера государства, которое ещё не выработало национальной стратегии в области противодействия информационным угрозам, приведём Парагвай. Эта региональная страна с ноября 2014 года постепенно, при содействии Организации американских государств, занимается выработкой национальной стратегии, при этом в Парагвае уже была создана Группа реагирования на инциденты в области информационной безопасности. Кроме того, ведётся активная работа и по совершенствованию законодательства в соответствующей области.
* Так или иначе, обе группы государств осознают необходимость скоординированных действий как на страновом, так и на региональном и глобальном уровнях, однако на данном этапе сильно различаются и степень развития информационных технологий в государствах региона, и их методы урегулирования новых угроз. Именно по этой причине представляется целесообразным проанализировать те направления, по которым движутся государства в стремлении обеспечить свою безопасность и выработать соответствующие рекомендации.