Доклад

Коданевой С.И., к.ю.н., доцента, в.н.с. Института научной информации по общественным наукам РАН

Актуальные вопросы согласования подходов России и стран Латинской Америки к регулированию кибербезопасности»

На Кутафинских чтениях 2025 г.

Регион Латинской Америки и Карибского бассейна является одним из самых быстрорастущих в мире по уровню цифровизации и внедрению новых технологий. В регионе активно распространяются системы e-government и разрабатываются соответствующие национальные стратегии цифрового правительства. Не менее активно в регионе развивается e-commerce: по прогнозам экспертов, в Бразилии, Мексике и Аргентине объем рынка электронной коммерции вырастет к 2027 году на 58%, 52% и 90% соответственно. На 2024 год основная доля рынка e-commerce приходится на Бразилию (29%) и Мексику (26%).

Наиболее развитыми по уровню цифровизации можно считать Аргентину, Уругвай, Чили, Коста-Рику, Колумбию, а менее развитыми – Доминиканскую Республику, Парагвай, Боливию, Гватемалу, Гондурас и Венесуэлу.

Однако вместе со стремительным внедрением новых технологий возрастают и риски кибератак. Цифровизация открывает новые возможности для киберпреступников, стремящихся воспользоваться уязвимостями в системах безопасности.

Наибольшему числу кибератак в странах Латинской Америки и Карибского бассейна в 2023–2024 годах подверглись госучреждения (21%) и финансовые организации (13%): они представляют наибольший интерес для киберпреступников ввиду хранения ценной информации и реализации критически важных процессов.

Основными последствиями успешных кибератак на организации, как и в прошлом году, остаются утечка конфиденциальной информации (53%) и нарушение деятельности (35%). Больше половины от общего объема похищенных у организаций данных составили персональные и учетные данные (32% и 21% соответственно). Кибератаки на частные лица приводили к утечке конфиденциальной информации в 72% случаев и к прямым финансовым потерям в 19% случаев.

В числе пяти самых атакуемых стран Латинской Америки и Карибского бассейна — Бразилия (19%), Мексика (16%), Колумбия, Чили и Аргентина.

Кибербезопасность в бразильском законодательстве - это сложная и развивающаяся область, основу которой составляют Marco Civil da Internet (Гражданский кодекс интернета Марко часто называют «Конституцией бразильского Интернета») и Генеральный закон о защите данных, а также принятые в соответствии с ними подзаконные нормативные акты.

Marco Civil da Internet (Закон № 12,965/2014) устанавливает принципы, гарантии, права и обязанности в отношении использования Интернета в Бразилии. Хотя он не является исключительно законом о кибербезопасности, он устанавливает основополагающие принципы:

- Сетевой нейтралитет: предотвращает дискриминацию интернет-провайдеров в отношении контента или услуг, что является основополагающим принципом безопасности и справедливости.

- Конфиденциальность и защита данных: устанавливает защиту конфиденциальности и персональных данных в качестве ключевого принципа.

- Хранение данных: требует, чтобы журналы подключений (записи о подключении пользователя к Интернету) хранились провайдерами в течение одного года. Журналы приложений (записи о действиях пользователя в рамках определенного приложения или сервиса) должны храниться в течение шести месяцев. Это имеет решающее значение для судебных споров.

- Ответственность интернет-приложений: устанавливает, что платформы не несут ответственности за контент третьих лиц, за исключением случаев, когда они не выполняют судебный приказ об его удалении. Это создает основу для борьбы с вредоносным контентом.

- Безопасность и стандарты: обязывает организации, которые собирают и хранят данные, обеспечивать безопасность и конфиденциальность в соответствии с установленными техническими стандартами.

Генеральный закон о защите данных (Закон № 13,709/2018) в основном дублирует Регламент о защите персональных данных ЕС, поэтому он заложил правовую основу регулирования кибербезопасности: принцип безопасности данных (статья 6);требование обеспечения безопасности (статья 46);требование об уведомлении уполномоченного органа о нарушении конфиденциальности данных (статья 48); а также требование к операторам данных соответствовать принципам безопасности, т.е. внедрять надежные программы и политики в области кибербезопасности.

Также в Бразилии в 2020 году была разработана национальная стратегия кибербезопасности (E-Ciber), а в соответствии с законом о кибербезопасности (Lei de Segurança Cibernética - Закон № 13,709/2021) в 2023 году были созданы

национальная политика кибербезопасности (PNCiber) и национальный комитет по кибербезопасности (CTIR Gov).

Помимо этого, вопросы кибербезопасности регулируются отраслевым законодательством, в частности, Законом о киберпреступлениях № 12 737/2012 (Закон Каролины Дикманн), актами ЦБ Бразилии, законодательством о критически важной инфраструктуре, актами Национального агентства по надзору в сфере здравоохранения.

Все организации в Бразилии обязаны принимать меры по кибербезопасности, разрабатывать планы обнаружения инцидентов, реагирования на них и восстановления после них, уведомлять уполномоченные органы и субъектов персональных данных об утечках и т.д.

Таким образом, за последнее десятилетие бразильское законодательство в области кибербезопасности значительно усовершенствовалось. От основополагающего подхода, основанного на принципах (Marco Civil), оно перешло к детальному, основанному на правах человека режиму защиты данных (LGPD) в сочетании с отраслевым регулированием.

Регулирование кибербезопасности в Мексике представляет собой сложную и динамично развивающуюся систему, характеризующуюся многоуровневой правовой базой. Единого всеобъемлющего закона не существует. Основы кибербезопасности, часто называемые «Киберсегуридад» в контексте национальной безопасности, изложены в Законе о национальной безопасности (Ley de Seguridad Nacional), который рассматривает кибербезопасность через призму национальной безопасности. Это дает властям полномочия предотвращать кибератаки, направленные на критически важные объекты инфраструктуры страны, которая понимается довольно широко и включает энергетику, финансы, транспорт и телекоммуникации.

Федеральный закон о защите персональных данных и имущества физических лиц (LFPDPPP) является наиболее важным законом для организаций частного сектора, касающимся безопасности данных. В целом регулирование схоже с европейским: закреплен принцип безопасности (статья 19), подход, основанный на рисках и требование уведомлять уполномоченный орган об инцидентах.

Закон о внутренней безопасности также затрагивает вопросы кибербезопасности, особенно в контексте защиты критически важной инфраструктуры. Он координирует действия различных государственных органов (таких как Министерство национальной обороны - SEDENA и Министерство военно-морского флота - SEMAR) по защите стратегических объектов от киберугроз.

Помимо этого, существует отраслевое регулирование: статьи в Уголовном кодексе, акты Национальной комиссии по банковским операциям и ценным бумагам, национальные стандарты (NOM-151-SCFI-2016 - этот стандарт касается сохранения учетных сообщений и имеет отношение к сохранению и целостности данных). Правительство уже много лет работает над более общим документом о кибербезопасности, но его принятие еще не завершено.

Организации в Мексике имеют следующие обязанности: принимать меры по обеспечению кибербезопасности, проводить оценку рисков, разрабатывать план реагирования на инциденты, сообщать об утечках данных, соблюдать отраслевые правила, особенно в сфере финансов, здравоохранения и телекоммуникаций, придерживайтесь более строгих протоколов кибербезопасности и обязательств по отчетности.

Подход Мексики к законодательству о кибербезопасности является фрагментарным, но надежным. Он опирается на систему национальной безопасности, закон о защите данных, в основе которого лежит принцип безопасности, уголовные наказания и очень подробные правила для таких важных секторов, как финансы. Наблюдается тенденция к усилению регулирования и более строгому обеспечению соблюдения, особенно со стороны отраслевых органов.

По результатам исследования российского объединения программных разработчиков «Руссофт», которое было проведено в 2023 году, только 5,9% (порядка 300 из более чем 5 тыс. российских IT-компаний) в ближайшие годы планируют попытаться выйти на латиноамериканский рынок. Причины: юридические сложности (законодательная специфика отдельных стран региона и антироссийскими санкциями, которые поддержали некоторые латиноамериканские страны), экономические проблемы (открытие и содержание дополнительных офисов в регионе), организационные трудности (например, сложность осуществления максимально эффективного управленческого контроля в виду географической отдаленности России и стран Латинской Америки) и пр. Наиболее активно они представлены в Бразилии.

Продукция российских производителей для многих латиноамериканских потребителей цифровых технологий может быть более привлекательна по сравнению с производителями других стран по ряду обстоятельств. В первую очередь это оптимальное соотношение цены и качества по сравнению с конкурентами. Во-вторых, нельзя не учитывать и тот факт, что сегодня ряд стран Латинской Америки (например, Куба, Никарагуа, Венесуэла и пр.) стремятся к цифровому суверенитету (прежде всего от США) и опасаются определенных цифровых угроз, в том числе вмешательства посредством информационных технологий в социально-политические и экономические

процессы со стороны внешних акторов. В-третьих, ряд российских IT-компаний имеют сильную репутацию в отдельных сегментах мирового рынка информационных технологий (в первую очередь компания «Лаборатория Касперского»).

У России и стран Латинской Америки есть потенциал для сотрудничества в области кибербезопасности, но для этого требуется сближение законодательства, выработка единых подходов к регулированию как требований к кибербезопасности, так и деятельности компаний, предоставляющих соответствующие услуги. Так, уже сегодня можно выделить определенное сходство в подходах.

1. Важность защиты критически важных объектов инфраструктуры (существует всеобщее признание того, что определенные сектора настолько жизненно важны, что киберинциденты на них представляет угрозу национальной безопасности, поэтому законодательство всех стран направлено на защиту такой инфраструктуры, хотя масштабы регулирования и конкретные обязательства различаются).

2. Рост числа обязательных отчетов об инцидентах (переход от добровольного обмена информацией к обязательному своевременному сообщению о значительных инцидентах в настоящее время является глобальным трендом даже в таких странах как США).

. Влияние системы NIST (хотя эта система стандартизации и является рекомендательной и добровольной в США, но де-факто она стала глобальным стандартом кибербезопасности).

. Слияние защиты данных и кибербезопасности (принятие GDPR стало поворотным моментом в правовых подходах к кибербезопасности – все больше стран мира рассматривают данную область через призму защиты персональных данных).

Основу для сотрудничества в области кибербезопасности должны составлять такие принципы как:

1. Регулирование, основанное на оценке рисков: требования должны быть пропорциональны ущербу, который может нанести инцидент в области кибербезопасности. Возлагать одинаковое бремя на международный банк и мелкого розничного продавца неэффективно. Поэтому правовое регулирование, как правило, направлено на операторов критически важной информационной инфраструктуры или «основных услуг» (организации в таких секторах, как энергетика, водоснабжение, финансы, здравоохранение и транспорт, где последствия сбоя могут иметь опасные последствия для всего общества, влечь существенный экономический ущерб).

2. Технологическая нейтральность: нормативные акты содержат только требования к результату принимаемых мер (например, «обеспечивать безопасность»), но не используемым для этого технологиям (например, «использовать шифрование AES-256»). Этот принцип отражает то, что технологии очень быстро развиваются и устаревают, поэтому технологическая нейтральность правового регулирования позволяет организациям адаптировать свои средства защиты к возникающим угрозам и инновациям.

3. Отказ от чрезмерно детализированного регулирования и фрагментации: чрезмерно подробные правила могут быть негибкими и не учитывать уникальный контекст организации. Более того, когда разные страны принимают совершенно разные требования, это создает дополнительную нагрузку на транснациональные корпорации, вынужденные подстраиваться под множество национальных правопорядков. Соответственно, некоторые страны предпочитают закреплять только общие положения и принципы, которые могут способствовать международной гармонизации правового регулирования. Хотя, как было показано выше, этот принцип не является универсальным, поскольку такие страны как Китай и Россия, напротив, стремятся защитить свой киберсуверенитет в т.ч. посредством детализации и фрагментации правового пространства.

4. Акцент на передовых практиках, а не на наказаниях: эффективное правовое регулирование нацеливает организации внедрять самые современные и передовые подходы к информационной безопасности, используя для этого различные меры стимулирования. Например, Закон США об обмене информацией о кибербезопасности 2015 г. предоставляет юридические убежища компаниям, делящимся с органами власти данными о киберугрозах, тем самым укрепляя коллективную защиту.