Заместитель руководителя ЦЕАОИ РИСИ,
начальник сектора США
и стран Латинской Америки
Д.Н. Бурых

О ситуации в сфере информационной безопасности в БРИКС

(на примере Бразилии)

Тема безопасности информационного пространства прежде всего с точки зрения несанкционированного проникновения и получения доступа к критически важным сведениям, как коммерческого, так и государственного значения, становится крайне важным аспектом в общем спектре вопросов, связанных с государственным управлением.

Правительства стран БРИКС, особенно Китая, Индии и Российской Федерации уделяют этой проблеме первостепенное значение. Реализуется ряд мер, ориентированных на обеспечение безопасности кибер пространства в условиях кратно участившихся атак со стороны не столько кибер преступников, сколько около государственных и государственных структур. За примерами далеко ходить не нужно. Достаточно вспомнить громкие разоблачения бывшего сотрудника АНБ США Э. Сноудена, сделанные им в конце 2013 года.

Из пятерки стран БРИКС в наиболее уязвимом положении оказалась Бразилия, которая связана с Европой и Африкой через оптико-волоконные кабели, проложенные через атлантическое побережье США. Т.е., иными словами, вся структура бразильских электронных коммуникаций осуществляется через Соединенные Штаты и является, фактически, открытой для ее спецслужб. Подтверждением этому тезису служат разоблачения ранее упомянутого сотрудника АНБ, согласно которым спецслужбы США получили доступ к критически важной государственной и финансово-экономической информации латиноамериканского гиганта. В первую очередь это касается крупнейших бразильских государственных и частных компаний.

Какие последствия? Мощнейший за последнее десятилетие политический и экономический кризис. Одной из основных причин кризиса являются

«антикоррупционные» разоблачения вокруг крупнейшей нефтяной государственной компании Бразилии – «Петробраз».

В основе скандала лежит создание коррупционной схемы обогащения путем незаконного заключения подрядных договоров с данной госкомпанией. Ключевым моментом стали показания одного из высокопоставленных менеджеров «Петробраз» П. Косты (Paulo Roberto Costa) – директора по снабжению. В результате в скандальную историю оказались вовлечены более полусотни топ-менеджеров упомянутой компании, включая президента и связанных с ней крупнейших бразильских компаний и политиков.

По мнению ряда бразильских политиков, одной из причин возникновения нынешнего кризиса вокруг «Петробраз» является стремление США приостановить ослабление влияния на бразильский истеблишмент и восстановить тесный политический и экономический диалог с Бразилиа после охлаждения отношений, обусловленного фактором «Сноудена». При этом они обращают внимание на тот факт, что наиболее жесткую позицию в отношении вовлеченных в скандал топ-менеджеров бразильской компании занимает федеральный судья Серхио Фернандо Моро (Sérgio Fernando Moro). С.Моро, окончивший в 1995 году юридический факультет Федерального университета штата Парана и ставший федеральным судьей в 1996 году, прошел подготовку в Гарвардской школе права по программе «Противодействие отмыванию денежных средств» под эгидой Госдепартамента США. Подчеркивается также, что согласно данным, преданным огласке Э. Сноуденом, АНБ США получило незаконный доступ к информационным системам «Петробраз», включая конфиденциальную информацию, касающуюся контрактной деятельности бразильской компании. Именно эти данные, по словам политиков, были использованы для давления на основных фигурантов дела в целях получения признательных показаний, в том числе тех, которые не могли быть получены средствами электронной разведки.

Очевидным ответом бразильской стороны на ставшую очевидной серьезную угрозу своим информационным ресурсам стали планы госкомпании Телебраз по прокладке оптико-волокна по дну Атлантики в Европу и Африку из города Форталеза. Но до настоящего времени проект не реализуется.

Однако этот случай не первый в списке, свидетельствующем о кибер уязвимости Бразилии. Наиболее наглядным проявлением имеющихся проблем стала атака на сайты правительственных структур Бразилии в 2012 году. В результате их работа была заблокирована от нескольких часов до нескольких суток. Кроме того, атаке подверглись серверы администрации президента республики. Наибольшую опасность представляет ни сколько атаки на правительственные он-лайн порталы, сколько уязвимость серверов, которые могут содержать информацию конфиденциального и секретного характера. На данный момент, сведений об утечке подобного рода сведений в результате вмешательства извне не зафиксировано. Тем не менее, констатируется, что современный уровень информационной защиты не соответствует требованиям времени и требует принятия срочных соответствующих мер.

Еще одним из факторов уязвимости органов государственного управления Бразилии является коммуникационное оборудование. В основном бразильские госструктуры используют оборудование американской компании “Cisco Systems”. О тесном сотрудничестве этой фирмы с АНБ также говорил Э. Сноуден.

Чувствительным направлением в плане защищенности от кибер-угроз является банковский сектор страны. Банки Бразилии в полной мере ощутили на себе резкое увеличение количества интернет-мошенничеств, зафиксированных в 2011 году и начале нынешнего года. Только по официальным данным, предоставленным Федерацией банков Бразилии (Febraban), ущерб финансовых учреждений составил в первом квартале 2011 года 378 млн. долл. США, что на 36% больше, чем за аналогичный период 2010 года. В основном фиксируются попытки незаконного доступа к персональным счетам физических и юридических лиц через он-лайн банкинг, который получил широкое распространение в последнее время. Бразильские эксперты констатируют, что официальные данные об ущербе в финансовом секторе сильно занижены в связи с тем, что банки неохотно придают гласности подобного рода информацию. Поэтому реальный ущерб - гораздо больше и может составлять до 600 - 700 млн. долл. США в квартал. Согласно данным Лаборатории Касперского, Бразилия занимает первое место в мире по числу атак с помощью «троянских» программ с целью получения доступа к банковским счетам. В 2011 – 2012 годах атакам подверглись

практически все крупные банки страны, включая Центральный банк Бразилии. В числе пострадавших – Сити банк, HSBS, Itau, Bradesco, PanAmericano.

Представители бразильских правительственных структур, в частности, генерал Антонио Сантос Герра (Antonio Santos Guerra), директор Центра коммуникаций и электронной войны вооруженных сил Бразилии (Ccomgex), подтверждают, что за последнее время в стране резко увеличилось количество кибер-атак. В 2011 году было зафиксировано более 400 тыс. различного рода преступных деяний в сфере интернет-технологий. По уровню кибер-опасности Бразилия делит первое место с Мексикой в латиноамериканском регионе.

Принимая во внимание складывающуюся ситуацию в сфере интернет-безопасности правительство Бразилии вынуждено принимать срочные меры. В частности, было выделено дополнительное финансирование на закупку антивирусных программ и программного обеспечения-симулятора кибер-атак на сумму 3.3 млн. долл. США. Программное обеспечение предоставят бразильские компании DECATRON и BluePex до конца нынешнего года. Кроме того, дальнейшее развитие получат профильные структуры такие как, Ccomgex и его структурное подразделение – Центр защиты Вооруженных сил (CDCiber). Будут усиливаться подразделения Гражданской полиции Бразилии, специализирующиеся на борьбе с интернет-мошенничеством.

Выделено дополнительное бюджетное финансирование на 2012 год в размере 45 млн. долл. США для CDCiber с целью закупки дополнительного программного обеспечения, обучения персонала и техники. Планируется также принять меры институционального характера, в частности, Сенат страны пребывания рассматривает вопрос о существенном усилении уголовной ответственности за совершение компьютерных преступлений за счет увеличения сроков наказания и расширения трактовки подобного рода преступлений.

Вывод: кибер- и информационное пространство Бразилии столкнулись с крупнейшими за всю историю вызовами. Фактически бразильское киберпространство оказалось практически полностью транспаретным для

Соединенных Штатов. Для решения проблемы такого масштаба требуется принятие неординарных и, возможно, весьма затратных мер. Сотрудничество в рамках БРИКС – одна из альтернатив, тем более, что РФ, Китай и Индия располагают собственными разработками как программных, так и аппаратных средств для решения этого вопроса.