Россия, США и безопасность киберпространства: путь к сотрудничеству

Основные положения

В двустороннем порядке России и Соединенным Штатам не удалось достичь взаимопонимания по большей части аспектов кибербезопасности. Несмотря на декларацию 1998 года о заинтересованности в совместном руководстве глобального реагирования на проблемы кибербезопасности, стороны чаще действовали как противники на страже собственных тайн национальной безопасности, а не как союзники, приверженные защите общих интересов в условиях глобальной цифровой экономики и мира социальных сетей.

Существуют убедительные исторические прецеденты, позволяющие предположить, что можно преодолеть российские и американские сомнения, в основе которых кроется конфиденциальность вопросов национальной безопасности. Так, невзирая на секретность определенной информации, в процессе подготовки к переходу в новое тысячелетие в 2000 году (так называемая проблема Y2K) под нависшей глобальной угрозой большинство стран предпочли сотрудничество. В сфере крайне засекреченных процедур пуска и предупреждения для баллистических ракет, Россией и Соединенными Штатами были утверждены меры совместного мониторинга, подразумевающие высокую степень присутствия на местах. Другой свежий пример – договоренность двух стран о новой системе кодирования для 40-летней прямой телефонной связи между Кремлем и Белым Домом. Более того, банки России и США уже сотрудничают по вопросам безопасных цифровых коммуникаций при осуществлении международных денежных переводов в ошеломляюще крупных размерах.

Проблемы кибербезопасности рассматриваются с различных точек зрения: если в США основное внимание уделяется правоохранительной деятельности в пределах страны, а международное сотрудничество – дело добровольное, то Россия стремится к разработке обязательных международных систем. Стороны также руководствуются совершенно разными философиями: Россия склоняется к социальному контролю интернета, чего США по большей части не поддерживают.

Несмотря на подобные разногласия, в декабре 2009 года на заседании Комитета ООН по вопросам разоружения и международной безопасности Соединенные Штаты и Россия договорились о начале переговоров в сфере укрепления безопасности интернета и ограничения использования киберпространства в военных целях. Если ранее в течение нескольких лет США отклоняли российские инициативы в области кибербезопасности, теперь было принято однозначное решение коренным образом изменить политику: огласив задачи обеспечения кибербезопасности 29 мая 2009 г., администрация Президента Обамы продемонстрировала решимость вывести вопрос на новый уровень. За такими заявлениями могут последовать новые двусторонние договоренности.

Предлагаемый документ в общих чертах представляет аргументы в защиту мер по более быстрому продвижению российско-американского сотрудничества в сфере обеспечения кибер- или информационной — более предпочтительный в России термин —

безопасности. Авторы также призывают две стороны приступить к реализации официально заявленного в декабре 2009 года начала новых консультаций по вопросам кибербезопасности в рамках резолюции Генеральной Ассамблеи ООН. С целью изучения сложностей и путей их преодоления, данный документ рассматривает четыре возможных сферы сотрудничества: инфраструктуру открытых ключей; быстрое реагирование на киберпреступления; обсуждения Организацией по безопасности и сотрудничеству в Европе (ОБСЕ) законов ведения кибервойны; а также сотрудничество между НАТО и Россией по вопросам кибербезопасности.

Рекомендации

Приведенные ниже рекомендации были разработаны на основе открыто заявленного обеими сторонами намерения сотрудничества. Сторонам предлагается возглавить перемены в каждой из четырех вышеперечисленных сфер, а правительствам – выступить с совместным предложением каждой инициативы в рамках соответствующей международной площадки (одной из которых может стать Международный союз электросвязи), возглавить необходимые рабочие группы, а также вовлечь прочие заинтересованные стороны в дискуссию с целью создания атмосферы доверия для более глубокого сотрудничества. Затем необходимы двусторонние переговоры по существу конкретных вопросов сотрудничества, обсуждение которых в открытом международном формате не представляется возможным из соображений государственной тайны.

1. Инфраструктура открытых ключей: в рамках Международного союза электросвязи (МСЭ) России и США следует выступить в защиту идеи обязательного многостороннего соглашения по инфраструктуре открытых ключей (PKI) с целью продвижения на международном уровне «экосистемы» достоверной идентичности. За основу можно взять «совместную оценку стратегии» российскими и американскими экспертами.

2. Ликвидация последствий киберпреступлений: России и Соединенным Штатам необходимо расширить существующую инфраструктуру круглосуточной Сети координационных пунктов по борьбе с высокотехнологичной преступностью под эгидой «Группы восьми», в том числе поддержку глобальной программы развития потенциала охраны правопорядка и расследования киберпреступлений для всех стран, подсоединенных к интернету.

3. Международное киберправо: России и Соединенным Штатам необходимо провести совместную оценку политики юридических аспектов регламентации наступательных и оборонительных мер в рамках противодействия киберпреступности, особенно в сфере критической инфраструктуры и «правил применения силы». Выбор площадки для обсуждения данных вопросов представляет определенные трудности, но лучшим вариантом в скудном списке представляется ОБСЕ.

4. Военные учения и обмены между НАТО и Россией в сфере кибербезопасности: на политическом уровне НАТО и России необходимо взять обязательства в

определенные сроки (например, в течение двух лет) провести совместную оценку составляющих кибербезопасности и путей ее обеспечения. В рамках научного сотрудничества между НАТО и Россией, России и Соединенным Штатам необходимо включиться в двустороннее наблюдение за моделированием кибератак и участие в нем. Вместе с партнерами из НАТО обоим государствам следует разработать методики и стандарты оценки уязвимости и классификации объектов критической инфраструктуры.