ЗАМЕСТИТЕЛЬ МИНИСТРА
ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

DEPUTY MINISTER
OF DIGITAL DEVELOPMENT, COMMUNICATIONS AND MASS MEDIA
OF THE RUSSIAN FEDERATION

Пресненская наб., д.10, стр. 2, Москва, 125039
Юридический адрес: Тверская, 7, Москва

Presnenskaya Embankment 10, building 2,
Moscow, 125039, Russian Federation
Legal address:7, Tverskaya str., Moscow

№ ММ-П16-116-87 «10» 01.2020

Уважаемый господин Генеральный секретарь!

В соответствии с циркулярным письмом Международного союза электросвязи (МСЭ) от 15 октября 2019 г. № CL-19/47, касающимся разработки проекта руководящих указаний по использованию структуры Глобальной программы кибербезопасности МСЭ, направляем вклад администрации связи Российской Федерации по данному вопросу.

Пользуюсь случаем, чтобы выразить Вашему Превосходительству уверения в своем глубоком уважении.

Приложение: вклад администрации связи России на 3 л. в 1 экз.

М.В. Мамонов

ЕГО ПРЕВОСХОДИТЕЛЬСТВУ
господину ХОУЛИНЮ ЧЖАО,
ГЕНЕРАЛЬНОМУ СЕКРЕТАРЮ
МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ

г. Женева

Вклад администрации связи Российской Федерации в проект руководящих указаний по использованию структуры Глобальной программы кибербезопасности МСЭ

Интернет становится неотъемлемой частью современного общества, продвигая конечного пользователя в авангард связи. Мошенничество, воровство и подделки существуют в онлайновой среде точно так же, как они существуют в среде офлайн. Доступны все виды информации, причем в разных форматах. Но в какой мере эта информация подлинная? Не является ли информация неточной или ложной, или не является ли контент вредоносным? Для того чтобы пользователи могли получить доступ ко всем открываемым Интернетом возможностям, решающее значение имеет доверие к инфраструктуре.

Именно поэтому мировые лидеры в ходе второго этапа Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) в Тунисе в ноябре 2005 года доверили МСЭ руководящую роль в координации международных усилий, направленных на содействие реализации программы кибербезопасности. Глобальная программа кибербезопасности (ГПК) МСЭ, объявленная 17 мая 2007 года Генеральным секретарем МСЭ д-ром Хамадуном И. Туре, является основой для международного сотрудничества в целях укрепления доверия и безопасности в информационном обществе.

В продолжение развития ГПК администрация связи Российской Федерации предлагает интенсифицировать работу в рамках этой программы с участием Исследовательских комиссий и Рабочих групп совета МСЭ в двух стратегических областях работы:

1) Правовые меры;

2) Технические и процедурные меры.

1. Правовые меры

Создание соответствующей правовой инфраструктуры является неотъемлемым компонентом любой национальной стратегии в области кибербезопасности. В рамках Дохинского плана действий (ДПД) 2006 года Бюро развития электросвязи (БРЭ) МСЭ оказывает содействие Государствам-Членам в понимании правовых аспектов кибербезопасности в целях согласования их нормативно-правовых баз. БРЭ опубликовало «Комплект материалов по законодательству в области киберпреступности», разработанный группой экспертов с тем, чтобы предоставить Государствам-Членам типовые тексты законов и справочный материал для содействия в согласовании законов и процессуальных норм в области киберпреступности. БРЭ разработало также вспомогательный документ под названием «Кибербезопасность: роль и обязанности эффективного регуляторного

органа» для представления его на Глобальном симпозиуме для регуляторных органов, который состоялся в ноябре 2009 года в г. Бейруте (Ливан).

В продолжение вышеуказанной работы в рамках ГПК Российская Федерация предлагает организовать дальнейшую проработку вопросов создания норм международного регулирования и гармонизации национальных норм на базе Рабочей группы Совета МСЭ по вопросам международной государственной политики, касающейся Интернета.

В частности, Государства-Члены МСЭ могут:

- провести анализ влияния новых технологий в электросвязи/ИКТ и развития Интернета на актуальные вопросы в области государственной политики, роль государств, бизнеса и гражданского общества с точки зрения аспектов кибербезопасности;
- обсудить практику государственного нормативного управления, индустриального регулирования и саморегулирования вопросов кибербезопасности в Интернете в разных странах, особенности работы операторов и сервис-провайдеров в условиях такого регулирования, принимая во внимание информацию и материалы, подготовленные в рамках ГПК;
- провести обмен передовым опытом по аспектам правового регулирования кибербезопасности в развивающихся странах с учётом опыта развитых стран с учетом международной работы, проделанной в рамках ГПК;
- представить предложения по сотрудничеству на международном уровне, направленные на оценку востребованности заинтересованными сторонами необходимости разработки международных политик в области кибербезопасности, и предложения по организации процесса дальнейшей разработки таковых международных политик в рамках МСЭ.

2. Технические и процедурные меры

Работа МСЭ в области безопасности охватывает широкий спектр угроз - от сетевых атак, отказа в обслуживании, хищения идентификационных данных, несанкционированного извлечения информации, телебиометрической аутентификации до обеспечения безопасности электросвязи в случае чрезвычайных ситуаций, возникающих на разных участках сети или в области сервисных услуг.

Органы по разработке стандартов должны играть активную роль при решении вопросов уязвимости систем безопасности в сетевых протоколах. Сектор стандартизации электросвязи МСЭ (МСЭ–Т) занимает уникальное

положение в области стандартизации в силу того, что его деятельность объединяет частный сектор и правительства в целях координации работы и содействия гармонизации политики и стандартов безопасности в международном масштабе. Поэтому в рамках деятельности МСЭ рассматриваются аспекты безопасности в архитектуре СПП, вопросы качества обслуживания, управления сетями, мобильности, выставления счетов и оплаты, так как в каждом из этих элементов есть уязвимости и потенциальный риск возникновения инцидентов в области кибербезопасности. Кроме того, в настоящее время МСЭ исследует новые области обеспечения безопасности, связанные с "облачными вычислениями" и "умными" электросетями.

Все исследовательские комиссии МСЭ проводят деятельность, связанную с обеспечением безопасности, и рассматривают вопросы безопасности как часть своей работы. Российская Федерация в рамках программы ГПК предлагает организовать взаимодействие между ИК в МСЭ для обеспечения сквозной безопасности во всех элементах цепочки предоставления ИКТ-услуг. К сожалению, сегодня нишевый подход к обеспечению безопасности приводит:

- к возникновению проблем с безопасностью именно на стыке отдельных фрагментов инфраструктуры и сервисной экосистемы;

- к разному пониманию и как следствие уровню реализации мер по обеспечению кибербезопасности в отдельных фрагментах инфраструктуры и сервисной экосистемы.

Целью дальнейшего развития ГПК в области технических и процедурных мер должна быть реализация концепции «secure by default», обеспечивающей максимальную и сквозную безопасность для разных технологий и протоколов с едиными высокими требованиями.

Но помимо МСЭ также существуют и другие стандартизирующие организации и индустриальные объединения, разрабатывающие технические требования к системам безопасности для передачи данных и требования к безопасности для протоколов уровня веб-услуг и приложений. Кроме того, существуют интернет-гиганты, реализующие свои проприетарные технические разработки.

В этой связи ГПК могла бы выступить связующим звеном для реализации единых стандартов, обеспечивающих нормы безопасности для поставщиков услуг и предприятий, гарантируя при этом взаимодействие цифровых продуктов и реализуя требования госполитик, в частности для того, чтобы идентификационные данные пользователей, обменивающихся информацией через IP-носитель, надлежащим образом аутентифицировались и авторизовались.