|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **Всемирная конференция по развитию электросвязи 2017 года (ВКРЭ-17)**  **Буэнос-Айрес, Аргентина, 9–20 октября 2017 года** | C:\Users\murphy\Documents\WTDC17\bd_R_25Years_Horizontal-411959.jpg |
|  | |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | **Документ WTDC-17/36-R** |
|  | | **8 сентября 2017 года** |
|  | | **Оригинал: испанский** |
| Бразилия (Федеративная Республика), Мексика | | |
| ПРЕДЛОЖЕНИЯ ДЛЯ РАБОТЫ КОНФЕРЕНЦИИ | | |
|  | | |
|  | | |
| **Приоритетная область**: − Вопросы Исследовательских комиссий  **Резюме**  Изменение исследуемого Вопроса 3/2 МСЭ-D "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности"  **Ожидаемые результаты**  Бразилия и Мексика предлагают всем делегациям на ВКРЭ-17 рассмотреть настоящий документ при обсуждении пересмотра исследуемого Вопроса 3/2, в том что касается как его содержания, так и формулировок.  **Справочные документы**  Вопрос 3/2 | | |

2-я ИССЛЕДОВАТЕЛЬСКАЯ КОМИССИЯ

**MOD** B/MEX/36/1

Вопрос 3/2

Защищенность сетей информации и связи: передовой опыт   
по созданию культуры кибербезопасности

# 1 Изложение ситуации или проблемы

Использование электросвязи и информационно-коммуникационных технологий бесценно с точки зрения стимулирования развития и социально-экономического роста на глобальном уровне. Несмотря на все преимущества, возникающие благодаря использованию этих технологий, существуют также риски и угрозы в области безопасности. Управление операциями (от личных финансовых средств до бизнес-операций), национальной инфраструктурой, государственными услугами и услугами частного сектора все чаще осуществляется через ту или иную сеть информации и связи и становится, таким образом, более уязвимым по отношению к тем или иным формам атаки.

Для того чтобы укрепить доверие при использовании и применении электросвязи/ИКТ в отношении всех типов приложений и контента, особенно тех, которые характеризуются значительным положительным влиянием на социально-экономические аспекты всех субъектов и затрагивают неприкосновенность частной жизни, защиту личных данных, безопасность сетей и их фактических пользователей, необходимо тесное сотрудничество между национальными и зарубежными полномочными органами, отраслью, академическими организациями и пользователями.

С учетом вышесказанного, в современном мире обеспечение защиты сетей информации и связи и создание культуры кибербезопасности приобрели важнейшее значение вследствие многих причин, в том числе:

a) взрывного роста масштабов развертывания и использования информационно-коммуникационных технологий (ИКТ);

b) того, что кибербезопасность остается предметом всеобщей обеспокоенности и, таким образом, существует необходимость в оказании содействия странам, особенно развивающимся странам, в обеспечении защиты их сетей электросвязи/ИКТ от кибератак и киберугроз;

с) необходимости стремиться к обеспечению безопасности этих глобально сопряженных инфраструктур для реализации потенциала информационного общества;

d) необходимости национальных, региональных и международных действий, а также использования подхода с участием многих заинтересованных сторон для формирования глобальной культуры кибербезопасности, что предусматривает координацию на национальном уровне, соответствующую национальную правовую инфраструктуру, наличие средств слежения, оповещения и восстановления, партнерские отношения между правительством и отраслью, а также просветительскую работу с гражданским обществом и потребителями;

e) того, что в резолюции 57/239 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) "Создание глобальной культуры кибербезопасности" государствам-членам предлагается обеспечивать "развитие у себя в обществе культуры кибербезопасности при применении и использовании информационных технологий";

f)того, что в резолюциях 68/167, 69/166 и 71/199 ГА ООН "Право на неприкосновенность личной жизни в цифровой век" подтверждается, что те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, включая право на неприкосновенность личной жизни;

g) того, что передовой опыт в области обеспечения кибербезопасности должен защищать и уважать права на неприкосновенность частной жизни и свободу волеизъявления, содержащиеся в соответствующих частях Всеобщей декларации прав человека, Женевской декларации принципов, принятой Всемирной встречей на высшем уровне по вопросам информационного общества (ВВУИО), и других соответствующих международных документах о правах человека;

h) того, что в Женевской декларации принципов указывается, что "необходимо формировать, развивать и внедрять глобальную культуру кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями", а в Женевском плане действий поощряется обмен примерами передового опыта и принятие необходимых мер для защиты от спама на национальном и международном уровнях, в то время как в Тунисской программе для информационного общества подтверждается необходимость глобальной культуры кибербезопасности, в частности в Направлении деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ);

i) того, что в программе по выполнению решений ВВУИО и последующей деятельности в связи с ВВУИО, состоявшейся в Тунисе в 2005 году, МСЭ предлагается стать основной содействующей/ ведущей организацией для Направления деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ);

j) того, что в резолюции 70/125 Генеральной Ассамблеи Организации Объединенных Наций, которая представляет собой итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений ВВУИО, подтверждается, что укрепление доверия и повышение безопасности при использовании информационно-коммуникационных технологий должны быть приоритетом, особенно с учетом растущих проблем, в том числе неправомерного использования таких технологий для осуществления вредоносных действий, от преследований и правонарушений до террористической деятельности, и должны согласовываться с правами человека;

k) того, что, согласно Заявлению ВВУИО+10 о выполнении решений ВВУИО, правительства и все соответствующие заинтересованные стороны осознают потребность в более тесном сотрудничестве для решения проблем надежности, безопасности, неприкосновенности частной жизни и защиты личных данных, безопасности и доверия при использовании ИКТ;

l) того, что в Резолюции 45 (Пересм. Дубай, 2014 г.) ВКРЭ высказывается поддержка повышению кибербезопасности в заинтересованных Государствах − Членах Союза;

m) того, что в Резолюции 130 (Пересм. Пусан, 2014 г.) Полномочной конференции содержится решение продолжать содействие выработке общего понимания среди правительств и других заинтересованных сторон вопросов укрепления доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях;

n) того, что в Резолюции 50 (Пересм. Хаммамет, 2016 г.) ВАСЭ подчеркивается необходимость укреплять и защищать информационные системы и системы электросвязи от киберугроз и кибератак и продолжать содействовать сотрудничеству между соответствующими международными и региональными организациями с целью расширения обмена технической информацией в области безопасности информационных сетей и сетей электросвязи;

o) того, что в выводах и рекомендациях, содержащихся в заключительном отчете 2-й Исследовательской комиссии МСЭ-D по Вопросу 3/2, предлагается рассмотреть вопрос о проведении в следующем исследовательском периоде исследования, посвященного меняющимся и новым угрозам помимо спама и вредоносных программ;

p) того, что предпринимаются различные усилия, направленные на повышение безопасности сетей, такие как подготовка отчетов о передовом опыте в рамках МСЭ-D; работа, проводимая Секретариатом МСЭ в рамках Глобальной программы кибербезопасности (ГПК), а также Сектором развития электросвязи МСЭ в рамках его деятельности по созданию потенциала в соответствующей пересмотренной программе и в некоторых случаях экспертами со всего мира;

q) того, что перед правительствами стран, поставщиками услуг и конечными пользователями, особенно в наименее развитых странах (НРС), стоят специфические проблемы выработки политики безопасности и подходов, соответствующих условиям, сложившимся в этих странах;

r)того, что спам остается предметом обеспокоенности, хотя необходимо исследовать и меняющиеся и новые угрозы;

s) необходимости в упрощенных процедурах проверки на базовом уровне для тестирования безопасности сетей электросвязи в целях содействия культуре безопасности.

# 2 Вопрос или предмет для исследования

a) Укреплять целостность систем ИКТ, что важно для их непрерывного развития;

b) Обсудить подходы и передовой опыт в области оценки воздействия спама в рамках сети, а также меняющихся и новых угроз, и представить необходимые меры и руководящие указания, в частности методы смягчения последствий, законодательные рамки и регуляторные меры, которые могли бы использовать развивающиеся страны, учитывая существующие стандарты и имеющиеся инструменты;

с) Представить информацию о существующих в настоящее время проблемах в сфере кибербезопасности, с которыми сталкиваются поставщики услуг, регламентарные учреждения и другие соответствующие стороны;

d) Продолжать собирать примеры национального опыта, относящегося к кибербезопасности, неприкосновенности частной жизни и защиты ребенка в онлайновой среде в Государствах-Членах, а также выявлять и изучать общие темы в рамках этого опыта и разрабатывать, на основе этой информации, руководящие указания, которые позволят Государствам-Членам внедрять эффективные механизмы в области безопасности и неприкосновенности частной жизни в цифровой среде;

e) Анализировать проблемы в области кибербезопасности, которые стоят перед IoT, искусственным интеллектом и другими новыми технологиями, а также меры по решению этих проблем;

f) Обсуждать перспективы и передовой опыт в области защиты неприкосновенности частной жизни и личных данных;

g) Содействовать росту осведомленности и развитию потенциала среди пользователей в отношении защиты данных, неприкосновенности частной жизни и кибербезопасности;

h) Составить сборник по соответствующим текущим видам деятельности в сфере кибербезопасности, ведущимся Государствами-Членами, организациями, частным сектором и гражданским обществом на национальном, региональном и международном уровнях, в которых могли бы участвовать развивающиеся страны и все секторы, в том числе представить информацию, собранную в соответствии с пунктом с) выше;

i) Изучить особые потребности лиц с ограниченными возможностями при координации с другими соответствующими Вопросами;

j) Изучить методы и способы оказания помощи развивающимся странам в связи с появлением проблем, связанных с кибербезопасностью, уделяя особое внимание НРС;

k) Развивать сотрудничество между заинтересованными сторонами, с тем чтобы проводить специальные сессии, семинары и семинары-практикумы для совместного использования знаний, информации и передового опыта, касающихся эффективных, действенных и полезных мер и видов деятельности для повышения кибербезопасности, укрепления доверия и защиты данных и целостности сетей с учетом существующих и потенциальных рисков для ИКТ, используя результаты исследования, проведение которого должно быть в максимально возможной степени приурочено к собраниям 1‑й Исследовательской комиссии или собраниям Группы Докладчика по этому Вопросу;

l) Осуществлять деятельность в сотрудничестве с соответствующими исследовательскими комиссиями МСЭ-Т и другими организациями по разработке стандартов (ОРС), в зависимости от случая и с учетом информации и материалов, имеющихся в этих организациях;

m) Разработать руководящие указания для содействия внедрению на национальном, региональном и международном уровнях мер, направленных на борьбу с массовой рассылкой незапрашиваемых электронных сообщений;

n) Собирать национальный опыт, касающийся мер регулирования и/или стратегий, осуществляемых органами регулирования электросвязи в целях укрепления доверия и безопасности при использовании электросвязи/ИКТ.

# 3 Ожидаемые результаты

1) Отчеты для членов по вопросам, указанным в разделе 2 а)–n), выше. Такие отчеты будут отражать информацию о том, что защищенные сети информации и связи неразрывно связаны с построением информационного общества и с социально-экономическим развитием всех стран. Проблемы, относящиеся к кибербезопасности, включают возможность несанкционированного доступа к сетям ИКТ, их разрушения и изменения передаваемой по ним информации, а также противодействие распространению спама и борьбу со спамом. Однако последствия этого можно уменьшить путем повышения уровня осведомленности в вопросах кибербезопасности, создания эффективных партнерств государственного и частного секторов и совместного использования примеров передового опыта органами, ответственными за выработку политики, коммерческими предприятиями, а также путем сотрудничества с другими заинтересованными сторонами.

Кроме того, культура кибербезопасности может содействовать формированию доверия к таким сетям и уверенности в них, стимулировать безопасное использование, обеспечить защиту данных и неприкосновенность частной жизни, расширяя при этом доступ и торговлю, а также содействовать странам в более эффективном получении преимуществ информационного общества в области социально-экономического развития.

2) Учебные материалы для использования во время практикумов, семинаров и т. д.

3) Получение знаний, информации и передового опыта, касающихся эффективных, действенных и полезных мер и видов деятельности для обеспечения кибербезопасности в развивающихся странах.

4) Рекомендации, упрощающие для Государств-Членов внедрение соответствующих мер, направленных на укрепление доверия и безопасности при использовании ИКТ.

# 4 График

Предлагаемая продолжительность данного исследования – четыре года, при этом предварительные отчеты о ходе работы должны представляться через 12, 24 и 36 месяцев.

# 5 Авторы предложения/спонсоры

1-я Исследовательская комиссия МСЭ-D, арабские государства, Межамериканское предложение, Япония, Исламская Республика Иран.

# 6 Источники используемых в работе материалов

a) Государства-Члены и Члены Сектора.

b) Соответствующая работа исследовательских комиссий МСЭ-Т и МСЭ-R.

c) Соответствующие результаты работы международных и региональных организаций.

d) Соответствующие неправительственные организации, занимающиеся вопросами кибербезопасности и культуры безопасности.

e) Обследования, онлайновые ресурсы.

f) Эксперты в области кибербезопасности.

g) Глобальный индекс кибербезопасности (GSI).

h) Другие источники, в случае необходимости.

# 7 Целевая аудитория

|  |  |  |
| --- | --- | --- |
| Целевая аудитория | Развитые  страны | Развивающиеся  страны[[1]](#footnote-1)1 |
| Органы, определяющие политику в области электросвязи | Да | Да |
| Регуляторные органы в области электросвязи | Да | Да |
| Поставщики услуг/операторы | Да | Да |
| Производители | Да | Да |
| Академические организации | Да | Да |

a) Целевая аудитория

Национальные органы, определяющие политику в области электросвязи, Члены Сектора и другие заинтересованные стороны, занимающиеся деятельностью в сфере кибербезопасности или отвечающие за нее, в особенности из развивающихся стран.

b) Предлагаемые методы реализации результатов

Целью программы исследований является сбор информации и передового опыта. Предполагается, что она будет по своей сути информативна и может использоваться для повышения осведомленности Государств – Членов Союза и Членов Сектора в вопросах кибербезопасности, а также для привлечения внимания к имеющимся информации, инструментам и передовому опыту; результаты программы могут использоваться в сочетании с организуемыми БРЭ специальными сессиями, семинарами и практикумами.

# 8 Предлагаемые методы рассмотрения данного Вопроса или предмета

Вопрос будет рассматриваться в рамках той или иной исследовательской комиссии в течение четырехгодичного периода (с представлением промежуточных результатов) под руководством Докладчика и заместителей Докладчика. Это позволит Государствам-Членам и Членам Сектора поделиться опытом и уроками в области кибербезопасности.

# 9 Координация

Необходима координация с МСЭ-Т, в частности с 17-й Исследовательской комиссией, занимающейся вопросами безопасности и отвечающей за укрепление доверия и безопасности при использовании информационно-коммуникационных технологий, а также другими соответствующими организациями, в том числе FIRST, ИМПАКТ, APCERT, ОАГ, СИКТЕ, ОЭСР, АТЭС, RIR, НПО, M3AAWG, UCENET и другими. Учитывая существующий уровень технических знаний по данному вопросу в этих группах, все документы (вопросники, промежуточные отчеты, проекты заключительных отчетов и т. п.) следует направлять 17-й Исследовательской комиссии для замечаний и вкладов до представления исследовательской комиссии МСЭ‑D полного состава для замечаний и утверждения.

# 10 Связь с Программой БРЭ

Программа БРЭ в рамках Намеченного результата деятельности 3.1 Задачи 3 должна способствовать обмену информацией и использовать результаты, в зависимости от случая, для достижения программных целей и удовлетворения потребностей Государств-Членов.

# 11 Другая соответствующая информация

–

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 1 К ним относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой. [↑](#footnote-ref-1)