ВОПРОС 3/2

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

1 Изложение ситуации или проблемы

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;

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

d) расширяющегося признания на национальном, региональном и международном уровнях необходимости в разработке и содействии распространению примеров передового опыта, стандартов и технических руководств, а также процедур для снижения уязвимости сетей на базе ИКТ и числа угроз для таких сетей;

e) необходимости национальных действий, регионального и международного сотрудничества для формирования глобальной культуры кибербезопасности, что включает координацию на национальном уровне, соответствующую национальную правовую инфраструктуру, наличие средств слежения, оповещения и восстановления, партнерские отношения между правительством/отраслью, а также просветительскую работу с гражданским обществом и потребителями;

f) потребности в подходе, предусматривающем участие многих заинтересованных сторон, в целях эффективного использования всего диапазона имеющихся инструментов для укрепления доверия при использовании сетей на базе ИКТ;

g) 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";

h) того, что в резолюции 68/167 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;

i) 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;

j) 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);

k) 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), и что МСЭ-Т, МСЭ-R, МСЭ-D и Генеральный секретариат, исходя из этой ответственности и во исполнение соответствующих Резолюций, принятых Всемирными конференциями по развитию электросвязи (ВКРЭ) (Доха, 2006 г., и Хайдарабад, 2010 г.), Полномочными конференциями (Анталия, 2006 г., и Гвадалахара, 2010 г.) и Всемирными ассамблеями по стандартизации электросвязи (Йоханнесбург, 2008 г., и Дубай, 2012 г.), провели многочисленные исследования в целях повышения кибербезопасности;

l) того что в итоговых документах ВВУИО (оба этапа: Женева, 2003 г., и Тунис, 2005 г.), содержится призыв к укреплению доверия и безопасности при использовании ИКТ;

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

n) того, что в соответствии со своим мандатом МСЭ-D должен объединять Государства-Члены, Членов Сектора и других экспертов в целях обмена знаниями и опытом в области защиты сетей на базе ИКТ;

o) результатов работы по Вопросу 22-1/1 в прошедшем исследовательском периоде, которые включают многочисленные отчеты и вклады со всего мира;

p) того, что предпринимаются различные усилия, направленные на повышение безопасности сетей, включающие работу Государств-Членов и Членов Сектора в рамках деятельности МСЭ-Т по разработке стандартов и работу по подготовке отчетов о передовом опыте в рамках МСЭ-D; работу, проводимую 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 для Государств-Членов и операторов инфраструктуры были бы полезны дополнительные отчеты, в которых подробно описывались бы различные ресурсы, стратегии и инструментарий, которые можно было бы использовать для формирования

доверия при использовании сетей на базе ИКТ, а также роль международного сотрудничества в этом отношении;

s) того, что спам остается предметом обеспокоенности;

t) изменяющихся методик тестирования общих критериев для сетей электросвязи;

u) 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) Обсудить подходы и передовой опыт в области оценки воздействия спама в рамках сети и представить необходимые меры, в частности методы смягчения последствий, которые могли бы использовать развивающиеся страны, учитывая существующие стандарты и имеющиеся инструменты.

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

c) Продолжать собирать примеры национального опыта, относящегося к кибербезопасности, в Государствах-Членах, а также выявлять и изучать общие темы в рамках этого опыта.

d) Продолжать анализировать результаты обследования осведомленности в вопросах кибербезопасности, проведенного в прошедшем исследовательском периоде, и опубликовать обновленные результаты обследования для измерения динамики с течением времени.

e) 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 c) выше.

f) Изучить особые потребности лиц с ограниченными возможностями при координации с другими соответствующими Вопросами.

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

h) Продолжать собирать примеры национального опыта и национальных потребностей в области защиты ребенка в онлайновой среде, при координации с другими соответствующими видами деятельности.

i) 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, используя результаты исследования, проведение которых должно быть в максимально возможной степени приурочено к собраниям 1-й Исследовательской комиссии или собраниям Группы Докладчика по этому Вопросу.

j) Собрать некоторые примеры национального опыта и потребностей в отношении общих критериев и тестирования безопасности, которые будут способствовать разработке общей основы и руководящих указаний, которые могли бы ускорить тестирование безопасности

оборудования электросвязи, 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.

3 Ожидаемые результаты

1) Отчеты для членов по вопросам, указанным в разделе 2 a)–j), 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 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, Исламская Республика Иран, Япония.

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) Другие источники, в случае необходимости.

7 Целевая аудитория

Целевая аудитория	Развитые страны	Развивающиеся страны[1]
Органы, определяющие политику в области электросвязи	Да	Да
Регуляторные органы в области электросвязи	Да	Да
Поставщики услуг/операторы	Да	Да
Производители	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

Координация с МСЭ-Т, в частности с ИК17 или ее преемницей, Вопросом 20 МСЭ-D о лицах с ограниченными возможностями, а также другими соответствующими организациями, в том числе FIRST, ИМПАКТ, APCERT, СИКТЕ ОАГ, ОЭСР, RIR, группами сетевых операторов (NOG), M3AAWG 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 им для замечаний и вкладов до представления исследовательской комиссии МСЭ-D полного состава для замечаний и утверждения.

---

[1] К ним относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой.

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

–