|  |  |
| --- | --- |
| **СОВЕТ 2021Виртуальные консультации Советников, 8–18 июня 2021 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.04** | **Документ C21/82-R** |
| **25 мая 2021 года** |
| **Оригинал: английский** |
| Записка Генерального секретаря |
| вклад ОТ австралии, канады, чешской Республики, Франции, румынии, соединенного королевства великобритании и северной ирландии |
| руководящиЕ указаниЯ по использованию Глобальной программы кибербезопасности |

Имею честь передать Государствам − Членам Совета вклад, представленный **Австралией, Канадой, Чешской Республикой, Францией, Румынией, Соединенным Королевством Великобритании и Северной Ирландии**.

 Хоулинь ЧЖАО
 Генеральный секретарь

Вклад от Австралии, Канады, Чешской Республики, Франции, Румынии, Соединенного Королевства Великобритании и Северной Ирландии

руководящиЕ указаниЯ по использованию Глобальной программы кибербезопасности

|  |
| --- |
| РезюмеПо нашему мнению, руководящие указания по использованию Глобальной программы кибербезопасности (ГПК) должны представлять собой краткий и очень целенаправленный справочный документ, в котором учитываются текущая работа МСЭ по вопросам кибербезопасности, отраженная в частности в Резолюции 130 Полномочной конференции, Резолюции 50 ВАСЭ и Резолюции 45 ВКРЭ, работа ИК17 МСЭ-T, а также некоторые другие инициатив и программы, осуществляемые Сектором развития электросвязи.Необходимые действияНастоящий документ **представляется** для рассмотрения Советом.\_\_\_\_\_\_\_\_\_\_\_\_Справочные материалы[*https://www.itu.int/en/action/cybersecurity/Pages/default.aspx*](https://www.itu.int/en/action/cybersecurity/Pages/default.aspx)*[Документ C21/36](https://www.itu.int/md/S21-CL-C-0036/en)* |

# 1 Введение

Мы высоко ценим возможность представить дополнительные замечания по проекту руководящих указаний по использованию ГПК и признаем, что были предприняты значительные усилия для разработки существующего проекта руководящих указаний, представленного Генеральным секретарем для рассмотрения Советом.

Мы признаем, что ГПК является важной основой, включающей пять направлений: правовые меры, технические и процедурные меры, организационные структуры, создание потенциала и международное сотрудничество, то есть по сути является справочным документом для сотрудничества и взаимодействия между всеми и со всеми соответствующими заинтересованными сторонами, с упором на существующие инициативы во избежание дублирования усилий.

Кроме того, мы хотели бы обратить внимание на тот факт, что МСЭ уже использует ГПК эффективным и действенным образом в интересах всех своих Членов, как это отражено во вкладе Генерального секретаря Совету.

Признавая мандат, текущую деятельность и программы Союза в области кибербезопасности, а также необходимость четкого понимания МСЭ и его Членами целей, целевой аудитории и задачи руководящих указаний, хотели бы предложить, чтобы эти руководящие указания представляли собой краткий и очень целенаправленный справочный документ, ограниченный следующими оптимизированными видами деятельности для каждого из направлений ГПК.

Направление 1: Правовые меры

a) МСЭ следует продолжать усилия в рамках своего мандата, направленные на содействие многосторонним обсуждениям и сотрудничеству по проблемам, связанным с кибербезопасностью, и в частности, на укрепление отношений со всеми заинтересованными сторонами в целях оказания помощи Государствам-Членам в этой области.

b) МСЭ следует продолжать сотрудничество с соответствующими партнерами, в рамках своего мандата, по разработке и поддержанию ресурсов по законодательству в области кибербезопасности в целях оказания помощи Государствам-Членам в обеспечении понимания ими правовых аспектов кибербезопасности, а также содействовать обмену опытом и знаниями между Государствами-Членами с тем, чтобы поддержать их усилия по разработке рамочных основ в этой области.

c) МСЭ, в сотрудничестве со всеми заинтересованными сторонами, следует работать в целях достижения более четкого общего понимания термина "возникающие технологии", возможностей и проблем, создаваемых такими технологиями, и содействовать обмену исследованиями конкретных ситуаций и примерами передового опыта по любым правовым мерам, которые могут быть применимы на национальном, региональном и международном уровнях.

d) МСЭ следует продолжать укреплять программу защиты ребенка в онлайновой среде как платформу для работы с партнерами и заинтересованными сторонами по содействию обмену знаниями, информацией, видами деятельности, включая меры, способные облегчить и поддержать деятельность стран по решению этой острейшей проблемы.

Направление 2: Технические и процедурные меры

a) Исследовательским комиссиям МСЭ следует в рамках своих конкретных мандатов и основных сфер компетенции уделять особое внимание дополнительному разъяснению того, что подразумевается под возникающими технологиями, чтобы изучить и предложить надлежащие руководящие указания по кибербезопасности для использования таких технологий и рекомендовать Государствам-Членам своевременно и в добровольном порядке применять их.

b) Следует создать механизм тесного сотрудничества между различными исследовательскими комиссиями МСЭ-Т в изучении вопросов, связанных с кибербезопасностью, при координирующей/ведущей роли ИК17.

c) Следует поощрять тесную координацию и сотрудничество МСЭ с ОРС под руководством частного сектора в целях поддержания сквозной безопасности продукции в отношении различных приложений и услуг на протяжении всего жизненного цикла продуктов.

d) МСЭ следует продолжать свои усилия в направлении разработки добровольных рекомендаций по техническим мерам для обеспечения кибербезопасности в областях, относящихся к его мандату, стимулируя своих членов к более активному участию в соответствующей деятельности МСЭ по стандартизации и в рамках стратегических партнерств и консультаций с ОРС под руководством частного сектора.

Направление 3: Организационные структуры

a) МСЭ следует продолжать оказывать развивающимся странам, наименее развитым странам и малым островным развивающимся государствам (СИДС) содействие в проектировании и создании национальных CIRT и других соответствующих технических подразделений / организаций.

b) Чтобы избежать дублирования усилий, МСЭ следует продолжать поощрять открытое и всеохватывающее взаимодействие между различными национальными, региональными или международными организациями, работающими над созданием устойчивых национальных организационных структур.

c) МСЭ следует поддерживать усилия по оценке выполнения Государствами-Членами своих обязательств, применяя такие инструменты, как Глобальный индекс кибербезопасности (GCI).

d) Что касается национальных структур, в частности, и по просьбе Государств-Членов, МСЭ следует оказывать им содействие в разработке стратегий для общегосударственных координационных механизмов с целью совершенствования согласованного межотраслевого процесса реализации национальных усилий в области кибербезопасности.

Направление 4: Создание потенциала

a) Продолжать поощрение открытого и всеобъемлющего взаимодействия и координации между различными национальными, региональными и международными организациями, которые участвуют в работе по созданию потенциала в области кибербезопасности, того чтобы обеспечить результативность и не допускать дублирования усилий.

b) Продолжать оказывать поддержку развивающимся странам, наименее развитым странам и СИДС в их усилиях по созданию потенциала в области кибербезопасности при содействии национальных и международных сообществ, участвующих в работе по созданию потенциала в области кибербезопасности.

c) Продолжать оказывать содействие развивающимся странам, наименее развитым странам и СИДС в разработке национальных стратегий, планов, политики и механизмов реагирования на инциденты в области кибербезопасности при поддержке заинтересованных партнеров и сообществ, занимающихся вопросами укрепления потенциала.

d) Стимулировать и поощрять обмен передовым опытом между Государствами-Членами, чтобы помочь странам, не имеющим достаточного опыта в этой сфере, укрепить свое положение с точки зрения кибербезопасности и сократить разрыв в развитии потенциала.

e) Продолжать развивать деятельность по созданию потенциала с учетом необходимости приобретения новых навыков для адаптации к возможностям и проблемам, связанным с возникающими технологиями.

f) Продолжать уделять особое внимание потребностям наиболее уязвимых групп населения, таких как женщины, дети, лица с ограниченными возможностями, лица с особыми потребностями и люди с ограниченными в связи с возрастом возможностями, в рамках усилий по созданию потенциала.

g) Продолжать использовать Глобальный индекс кибербезопасности (GCI) в качестве инструмента для создания потенциала и повышения осведомленности.

h) Продолжать содействовать определению заинтересованными сторонами направлений научно-исследовательской деятельности, связанных с кибербезопасностью, особенно в сфере возникающих технологий, используя возможности членства в МСЭ представителей частного сектора и академических организаций.

i) Распространять инструменты, ресурсы и передовой опыт среди Государств-Членов, отраслевых организаций и других заинтересованных сторон, чтобы поддержать их усилия, направленные на создание потенциала ММСП, в целях укрепления их уверенности и доверия при использовании ИКТ, и продолжать содействовать развитию культуры кибербезопасности.

Направление 5: Международное сотрудничество

a) МСЭ следует продолжать играть лидирующую роль в областях, относящихся к его мандату, чтобы содействовать сотрудничеству, диалогу и координации между всеми государствами, а также представителями частного сектора и другими заинтересованными сторонами по вопросам глобальной кибербезопасности.

b) Помимо того, что следует и дальше поощрять проведение двусторонних и многосторонних обсуждений между ключевыми игроками, учитывая глобальный характер кибербезопасности, необходимо также способствовать организации более широких дискуссий с привлечением большего числа участников, включая частный сектор, академические организации, гражданское общество и другие заинтересованные стороны.

c) МСЭ следует продолжать изучение инновационных, гибких и оперативных механизмов для создания партнерских связей с учетом стремительного развития сектора технологий и многообразия появляющихся новых структур, особенно стартапов и ММСП.

d) МСЭ следует продолжать взаимодействовать с другими ключевыми учреждениями системы ООН, чтобы оказывать поддержку внутренним усилиям Секретариата ООН и оптимизировать свои программы и виды деятельности в области кибербезопасности, с тем чтобы более эффективным образом служить мировому сообществу.

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