|  |  |
| --- | --- |
| **Пункт повестки дня: PL 2** | **Пересмотр 1Документа C23/93-R** |
| **14 июля 2023 года** |
| **Оригинал: английский** |
|  |  |
| Вклад Бразилии (Федеративной Республики) |
| ДАЛЬНЕЙШЕЕ РАЗВИТИЕ ГЛОБАЛЬНОЙ ПРОГРАММЫ КИБЕРБЕЗОПАСНОСТИ (ГПК) |
| **Назначение**Представить руководящие указания для успешной реализации Направления деятельности С5 ВВУИО (Укрепление доверия и безопасности при использовании ИКТ).**Необходимые действия Совета**Совету предлагается **принять** проект Решения, содержащийся в проекте Решения в Приложении.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Справочные материалы**[Резолюция 130](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-130-R.pdf) (Пересм. Бухарест, 2022 г.) Полномочной конференции – Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологийРекомендация 3 Рабочей группы пленарного заседания ПК-22 (пункт 1.8 [Документа PP-22/206](https://www.itu.int/md/S22-PP-C-0206/en)): Глобальная программа кибербезопасности[Резолюция 1332](https://www.itu.int/md/S19-CL-C-0137/en) (C11, последнее изменение C19) Совета − Роль МСЭ в выполнении решений ВВУИО и Повестки дня в области устойчивого развития на период до 2030 года |

Базовая информация

|  |
| --- |
| **Информация и контекст по пересмотренной версии 1: пересмотренная версия 1 данного вклада Бразилии является результатом корректировок и изменения формата на основании неофициальных вкладов, полученных Бразилией от различных Государств‑Членов после публикации Документа C23/93. Эта версия представляет собой результат усилий по достижению консенсуса**. |

Бразилия представила на Полномочной конференции МСЭ 2022 года (ПК-22) вклад, касающийся пересмотра Резолюции 130 об усилении роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий, в котором содержалось конкретное положение о привлечении членов МСЭ (Государств-Членов, Членов Секторов и Ассоциированных членов) к участию в процессе обновления структуры Глобальной программы кибербезопасности (ГПК) ([Документ PP-22/79(Add.1)](https://www.itu.int/md/S22-PP-C-0079/en)).

В процессе работы Конференции стало совершенно очевидно, что любые усилия, связанные с ГПК, вызывают разногласия среди членов. Было проведено несколько раундов переговоров и потрачено немало времени на обсуждение этого вопроса, при этом Бразилия последовательно отстаивала свою позицию о необходимости разработки на основе консенсуса базового документа в отношении ГПК, что стало бы первым шагом на пути к реализации инициатив МСЭ, связанных с кибербезопасностью. Эта позиция не была изолированным мнением Бразилии, многие другие страны также разделяют такой подход, хотя Бразилия признает, что ряд Государств-Членов выступают против.

На ПК-22 было принято решение утвердить следующую Рекомендацию Рабочей группы пленарного заседания (пункт 1.8 [Документа PP-22/206](https://www.itu.int/md/S22-PP-C-0206/en)):

|  |
| --- |
| РЕКОМЕНДАЦИЯ 3: ГЛОБАЛЬНАЯ ПРОГРАММА КИБЕРБЕЗОПАСНОСТИ (ГПК)РГ-ПЗ рекомендует Полномочной конференции предложить Совету рассмотреть предложения Государств-Членов, касающиеся ГПК, ее текущего использования и возможного будущего развития. ([Документ PP-22/188(Rev.1)](https://www.itu.int/md/S22-PP-C-0188/en)) |

Учитывая обсуждения, состоявшиеся в ходе ПК-22, и дополнительный обмен мнениями между делегатами, Бразилия предложила включить в повестку дня данной сессии Совета МСЭ один пункт, касающийся кибербезопасности в контексте Резолюции 130 (Пересм. Бухарест, 2022 г.).

Тем самым Бразилия стремится подтвердить важность продолжения и продвижения этих обсуждений, которые могут быть весьма полезными, особенно для развивающихся стран.

Бразилия отмечает и приветствует вклад, представленный на 30-м собрании Консультативной группы по развитию электросвязи (КГРЭ) Германией, Данией, Испанией, Литвой, Нидерландами, Польшей, Португалией, Румынией, Соединенным Королевством, Францией и Швецией и касающийся выполнения Резолюций МСЭ в поддержку кибербезопасности с предложением о проведении сравнительного анализа. Бразилия поддержала предложение в КГРЭ и считает, что это важный путь к повышению прозрачности и эффективности инициатив МСЭ-D, связанных с кибербезопасностью. Тем не менее, важно также подчеркнуть, что это предложение не препятствует разработке ГПК на уровне Совета. Бразилия рассматривает это как дополнительную инициативу, которая станет основой для возможного процесса дальнейшего развития ГПК.

Концепция

Учитывая вышеупомянутый контекст, Бразилия хотела бы представить свое предложение по будущему развитию ГПК, подтверждая, что дальнейшее развитие ГПК имеет первостепенное значение для работы МСЭ в области кибербезопасности, поскольку ГПК является структурой, которая служит методологической основой для Глобального индекса кибербезопасности (GCI).

Вопросник GCIv5 включает 84 вопроса по 19 показателям, относящимся к пяти направлениям ГПК (правовые меры, технические меры, организационные меры, меры по созданию потенциала и меры по сотрудничеству). GCIv5 (пятое издание GCI) находится в стадии реализации, и этот вопросник обсуждался в рамках работающей по переписке группы под руководством Бразилии в конце 2022 года (создана в рамках Вопроса 3/2 МСЭ-D – Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности).

В отношении вопросов, являющихся частью GCI, нет каких-либо публичных разногласий, что отражает консенсус относительно необходимости принятия конкретных мер по всем пяти направлениям для надлежащего решения проблем в области кибербезопасности, даже если эти меры затрагивают области, не входящие в мандат МСЭ (например, киберпреступность). Ни одно Государство-Член никогда публично не выступало против включения вопросов о киберпреступности в вопросник, ссылаясь на роль или мандат МСЭ.

Принимая во внимание тот факт, что вопросник GCI представляет собой список действий, которые должны быть предприняты в рамках каждого из пяти направлений (независимо от мандата МСЭ), и что нет никаких возражений со стороны членов относительно содержательного наполнения каждого направления, представляется закономерным, что этот механизм можно использовать для разработки структуры ГПК.

В связи с этим Бразилия предлагает разработать структуру ГПК, сохранив пять направлений и используя вопросник в качестве основы для этого процесса. Более того, помимо описания содержания каждого направления на основе вопросов вопросника, каждая тема должна содержать пояснение относительно мандата МСЭ по данному вопросу и деятельности/инициативам в этом отношении. В случае, если та или иная мера не входит в мандат МСЭ, в документе также следует указать организации/инициативы, которые могут оказать членам некоторую поддержку по данному конкретному вопросу.

Благодаря этому члены МСЭ не только получат более полное представление о потенциале, который необходимо развивать, и мерах, которые необходимо принять, но и смогут ознакомиться с мандатом МСЭ и с легкостью определить другие организации, которые могут оказать помощь и предоставить ресурсы в различных областях. Вся эта информация будет содержаться в одном сводном и согласованном документе.

Поэтому Бразилия предлагает Членам Совета МСЭ рассмотреть настоящий документ и Приложение к нему в качестве отправной точки для обсуждения дальнейшего развития ГПК.

**Приложение**: 1

ПРИЛОЖЕНИЕ

ПРОЕКТ НОВОГО РЕШЕНИЯ [...]

Информационный ресурс для помощи Государствам-Членам в наращивании их потенциала кибербезопасности и киберустойчивости

Совет МСЭ,

учитывая

*a)* Резолюцию 130 (Пересм. Бухарест, 2022 г.) об усилении роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий;

*b)* Резолюцию 45 (Пересм. Кигали, 2022 г.) ВКРЭ о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним;

*c)* Резолюцию 50 (Пересм. Женева, 2022 г.) ВАСЭ о кибербезопасности;

*d)* рекомендацию 3 Рабочей группы пленарного заседания Полномочной конференции 2022 года, в которой Совету предлагается рассмотреть предложения Государств-Членов относительно ГПК, ее текущего использования и возможного будущего развития,

напоминая,

*a)* что кибербезопасность является одним из основополагающих элементов обеспечения защиты инфраструктуры электросвязи/ИКТ и необходимым фундаментом социального и экономического развития;

*b)* что для того, чтобы воспользоваться огромными возможностями цифровых технологий, необходимо укреплять доверие и безопасность при использовании ИКТ;

*c)* что для увеличения возможности цифровых соединений требуется дополнительная работа с целью создания потенциала осведомленности о киберустойчивости и кибербезопасности, а также для решения проблемы цифровых разрывов,

решает поручить Генеральному секретарю в тесном сотрудничестве с Директорами трех Бюро

1 разработать информационный ресурс для Государств-Членов, который включал бы по каждому из направлений Глобальной программы кибербезопасности (ГПК):

a) примеры существующего передового опыта;

b) источники рекомендаций, помощи и руководящих указаний от МСЭ и других соответствующих организаций для укрепления кибербезопасности и киберустойчивости;

c) информацию о программах создания потенциала, обеспечиваемых МСЭ и другими соответствующими организациями;

2 поддерживать и регулярно обновлять данный ресурс, для учета новых проблем, новых направлений развития и новых касающихся МСЭ видов деятельности, а также новых видов деятельности под руководством других организаций, которые способны помочь Членам МСЭ укрепить их потенциал кибербезопасности и киберустойчивости.

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