|  |  |
| --- | --- |
| **СОВЕТ 2022Женева, 21–31 марта 2022 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Пересмотр 1Документа C22/32-R** |
| **15 марта 2022 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря |
| ПРОЕКТ руководящиХ указаниЙ по использованию мсэ Глобальной программы кибербезопасности |

|  |
| --- |
| РезюмеВ ходе своей сессии 2019 года Совет поручил Генеральному секретарю одновременно представить на следующей сессии Совета 1) отчет, разъясняющий, как МСЭ в настоящее время использует структуру [Глобальной программы кибербезопасности](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (ГПК), и 2) соответствующие руководящие указания по использованию структуры ГПК Союзом, разработанные при участии Государств-Членов, – на рассмотрение и утверждение Советом ([C19/117](https://www.itu.int/md/S19-CL-C-0117/en), [C19/58](https://www.itu.int/md/S19-CL-C-0058/en)).В соответствии с этими поручениями при поддержке Старшего судьи (в отставке) Штайна Шольберга (бывший председатель HLEG), проф. Соланж Гернаути и г‑на Нобору Накатани, а также при участии Государств-Членов и других заинтересованных сторон был сформулирован проект руководящих указаний, который вместе с отчетом секретариата (C21/36), был представлен виртуальным консультациям Советников 2021 года (C21/VCC-1) для рассмотрения и утверждения (C21/71).После C21/VCC-1 Государства – Члены Совета приняли к сведению отчет секретариата и в отношении проекта руководящих указаний приняли решение по переписке поручить секретариату провести дальнейшие консультации с Государствами – Членами Совета с учетом полученных вкладов и замечаний, представленных на этом собрании. Секретариат представит пересмотренный документ для рассмотрения и утверждения на следующей сессии Совета.Соответственно, были проведены дополнительные консультации с Государствами – Членами Совета, и с учетом полученных вкладов был разработан следующий пересмотренный проект руководящих указаний, а также вспомогательный информационный документ ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)). Важно отметить, что эта деятельность не направлена на пересмотр ГПК и что этот вопрос не будет затрагиваться в ее рамках.Необходимые действияНастоящий документ представляется Совету для **рассмотрения** и **утверждения** в установленном порядке.***Примечание. – Этот проект руководящих указаний был обновлен для отражения обсуждений, проведенных Государствами – Членами Совета 14 марта по нерешенным пунктам, помещенным в квадратные скобки в Документе 32. В настоящей версии документа в квадратных скобках остаются два пункта.***\_\_\_\_\_\_\_\_\_\_\_\_Справочные материалы*Резолюция* [*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-R.pdf) *(Пересм. Дубай, 2018 г.) Полномочной конференции**[Глобальная программа кибербезопасности (ГПК)](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx),* [*Документ C21/36 Совета*](https://www.itu.int/md/S21-CL-C-0036/en)*, Документы* [*C21/36*](https://www.itu.int/md/S21-CL-C-0036/en)*,* [*C21/71*](https://www.itu.int/md/S21-CL-C-0071/en)*,* [*C19/117*](https://www.itu.int/md/S19-CL-C-0117/en)*,* [*C19/58*](https://www.itu.int/md/S19-CL-C-0058/en)*,* [*C22/INF/8*](https://www.itu.int/md/S22-CL-INF-0008/en) *Совета* |

Раздел 1. Введение

**1.1** Полномочная конференция МСЭ 2018 года, состоявшаяся в Дубае, приняла [Резолюцию 130](https://www.itu.int/en/council/Documents/basic-texts/RES-130-R.pdf): "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий".В Резолюции содержится, наряду с прочим, решение *использовать структуру ГПК для того, чтобы далее направлять работу Союза по укреплению доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).*

**1.2** На пленарном заседании непосредственно перед принятием Резолюции 130 Генеральный секретарь МСЭ "с удовлетворением отметил, что в ходе обсуждения проекта резолюции значимость ГПК получила широкое признание. Он обратился к пленарному заседанию с призывом согласиться с сохранением пункта 12.1 раздела решает, который позволит МСЭ использовать ГПК в качестве руководящих указаний в своей работе по вопросам укрепления доверия и безопасности при использовании ИКТ. В связи с этим он проконсультируется с Советом и бывшим председателем Группы экспертов высокого уровня по ГПК судьей Штайном Шольбергом"[[1]](#footnote-1)1.

**1.3** На сессии Совета МСЭ 2019 года был представлен отчет бывшего председателя Группы экспертов высокого уровня по [ГПК](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (HLEG), в котором отмечалось, что для более эффективного использования Глобальной программы кибербезопасности можно было бы разработать соответствующие руководящие указания[[2]](#footnote-2)2. На этом собрании Совет поручил Генеральному секретарю одновременно представить на следующей сессии Совета 1) отчет, разъясняющий, как МСЭ в настоящее время использует структуру ГПК, и 2) соответствующие руководящие указания по использованию ГПК Союзом, разработанные при участии Государств-Членов, – на рассмотрение и утверждение Советом[[3]](#footnote-3)3.

**1.4** В соответствии с этими поручениями процесс разработки проекта руководящих указаний был описан в Циркулярном письме ([CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)), и 23 апреля 2020 года и 1 марта 2021 года были проведены две открытые консультации с участием всех заинтересованных сторон ВВУИО в целях получения замечаний по проекту руководящих указаний (открытые консультации). На собрании присутствовали более 160 участников, которые представили свои замечания по каждому разделу проекта руководящих указаний. Все замечания, полученные от участников в письменном виде до или после открытых консультаций, были опубликованы на [веб-сайте](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) ГПК.

**1.5** С учетом полученных вкладов секретариатом был разработан отчет, разъясняющий, как МСЭ в настоящее время использует структуру ГПК ([отчет секретариата](https://www.itu.int/md/S21-CL-C-0036/en)), и при поддержке Старшего судьи (в отставке) Штайна Шольберга (бывший председатель HLEG) и участии Государств-Членов был подготовлен проект руководящих указаний по использованию ГПК ([проект руководящих указаний](https://www.itu.int/md/S21-CL-C-0071/en)) для рассмотрения и утверждения Советом. Генеральный секретарь также выражает благодарность профессору Соланж Гернаути (Швейцарская консультативно-исследовательская группа по кибербезопасности, Лозаннский университет) за консультации и вклад по разделам, посвященным направлениям 2 и 4 ГПК, а также г-ну Нобору Накатани (бывший Исполнительный директор Глобального комплекса Интерпола по инновациям) – за консультации и вклад по разделу, посвященному направлению 3 ГПК. Важно отметить, что эта деятельность не направлена на пересмотр ГПК и этот вопрос не будет затрагиваться в ее рамках.

**1.6** Из-за пандемии COVID-19 презентация этих документов была перенесена на виртуальные консультации Советников (VCC) 2021 года, которые проходили с 8 по 18 июня 2021 года. После VCC 2021 года Государства – Члены Совета приняли к сведению отчет секретариата и приняли решение по переписке в отношении проекта руководящих указаний "поручить секретариату провести дальнейшие консультации с Государствами – Членами Совета с учетом полученных вкладов и замечаний, представленных на этом собрании. Секретариату следует представить пересмотренный Документ [71](https://www.itu.int/md/S21-CL-C-0071/en) для рассмотрения и утверждения на следующей сессии Совета".

**1.7** Соответственно, с Государствами – Членами Совета были проведены дополнительные консультации, и с учетом полученных вкладов были подготовлены два документа:

a) информационный документ ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)) в котором представлена базовая информация, меняющаяся среда и контекст разработки настоящего проекта руководящих указаний; и

b) настоящий проект руководящих указаний, изложенных ниже, которые были разработаны для рассмотрения и утверждения Советом в 2022 году.

При разработке этих документов учитывались рекомендации, изложенные в Отчете HLEG 2008 года, осуществлявшаяся впоследствии деятельность МСЭ, события, произошедшие в соответствующей сфере после 2008 года, а также [вклады, представленные Государствами-Членами и другими заинтересованными сторонами](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) (в соответствии с Циркулярными письмами ([CL-20/18](https://www.itu.int/md/S20-SG-CIR-0018/en) и [CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en))).

**1.8** В то время как пять направлений, безусловно, взаимосвязаны между собой, в каждом разделе рассматривается отдельное направление ГПК и предлагаются конкретные руководящие указания по его использованию. Раздел 2 посвящен правовым мерам. В разделе 3 освещаются технические и процедурные меры. В разделе 4 рассматриваются вопросы создания потенциала. Раздел 5 охватывает организационные структуры, а раздел 6 – международное сотрудничество. В разделе 7 содержатся некоторые общие сквозные руководящие указания по использованию структуры ГПК.

Раздел 2. Направление 1 − Правовые меры

**2** С учетом стремительного развития технологий меры, принимаемые организациями и странами, должны также претерпевать изменения, чтобы поспевать за темпами этого развития. Это обусловливает возникновение в рамках проблемы кибербезопасности новых сложностей, которые требуют тщательного рассмотрения с различных точек зрения. В связи с этим ниже приводятся предлагаемые руководящие указания по использованию МСЭ направления 1 в рамках своего мандата:

**a)** МСЭ следует продолжать усилия, направленные на содействие многосторонним обсуждениям и сотрудничеству для решения проблемы кибербезопасности 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, чтобы содействовать разработке и поддержанию ресурсов по кибербезопасности и законодательства в области киберпреступности в целях оказания помощи Государствам-Членам в понимании правовых аспектов кибербезопасности, [включая [существующие] соответствующие международные системы], а также содействовать обмену опытом и знаниями среди Государств-Членов, с тем чтобы поддержать их усилия по разработке рамочных основ в этой области.

**c)** МСЭ, в сотрудничестве со всеми соответствующими заинтересованными сторонами, следует содействовать более глубокому пониманию правовых проблем кибербезопасности и рисков, создаваемых возникающими технологиями, и поощрять обмен исследованиями конкретных ситуаций и примерами передового опыта 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 и направлениями деятельности (в том числе связанными с правовыми мерами) в целях облегчения и поддержки деятельности стран по решению этой острейшей проблемы.

Раздел 3. Направление 2 − Технические и процедурные меры

**3** Рекомендации, касающиеся направления 2 в Отчете HLEG 2008 года, остаются действительными. В свете вышеизложенного для направления 2 предлагаются следующие руководящие указания:

**a)** Исследовательским комиссиям МСЭ следует сосредоточить внимание на возникающих технологиях, связанных с электросвязью/ИКТ, с тем чтобы продумывать и предлагать руководящие указания и рекомендации по кибербезопасности в целях укрепления доверия и безопасности при использовании таких технологий и своевременно рекомендовать Государствам-Членам добровольно 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, для того чтобы поддерживать сквозную безопасность на максимально возможном уровне на всем протяжении процесса стандартизации всех компонентов и интерфейсов продукции ИКТ.

**c)** Следует поощрять тесную координацию и сотрудничество МСЭ с другими ОРС на основе взаимности в целях поддержания сквозной безопасности продукции в отношении различных приложений и услуг на протяжении всего жизненного цикла продуктов.

**d)** МСЭ следует продолжать работу по распространению глобальных стандартов в области безопасности ИКТ, а также работать с другими организациями по стандартизации и отраслевыми группами, с тем чтобы они представили свои стандарты по техническим и процедурным мерам МСЭ-Т и МСЭ-R для принятия в качестве Рекомендаций МСЭ-Т и МСЭ-R.

**e)** МСЭ следует продолжать свои усилия в том, что касается разработки рекомендаций по техническим и процедурным мерам обеспечения кибербезопасности в областях, входящих в его мандат, стимулирования своих членов к более активному участию в соответствующей деятельности МСЭ по стандартизации и в рамках стратегических партнерств и консультаций с университетами и ОРС.

**f)** МСЭ следует продолжать настоятельно рекомендовать своим Членам инициировать/заключать соглашения о взаимной сертификации в целях формирования согласованных стандартов кибербезопасности.

Раздел 4. Руководящие указания по использованию направления 3 – Организационные структуры

**4** При том понимании, что рекомендации, изложенные в Отчете HLEG 2008 года, оказались полезны в качестве ориентира для усилий МСЭ по направлению 3 и по-прежнему сохраняют свою актуальность, предлагаются следующие руководящие указания, касающиеся в частности работы Бюро развития электросвязи МСЭ (БРЭ), которые могли бы способствовать наращиванию усилий в этом отношении:

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

**b)** Во избежание дублирования усилий МСЭ следует продолжать поощрять открытое и всеохватное взаимодействие, а также координацию, в рамках своего мандата, между различными национальными, региональными или международными организациями, работающими над созданием устойчивых национальных организационных структур.

**c)** МСЭ следует наращивать усилия по оценке выполнения Государствами-Членами своих обязательств, применяя такие инструменты как Глобальный индекс кибербезопасности (GCI), в целях продвижения кибербезопасности как межотраслевого фактора, способствующего их усилиям в области цифровой трансформации.

**d)** По просьбе Государств-Членов, МСЭ следует оказывать, в частности, национальным структурам содействие в разработке стратегий общегосударственных координационных механизмов для налаживания комплексного межотраслевого процесса осуществления национальных мер кибербезопасности.

**e)** МСЭ следует продолжать содействовать расширению сотрудничества между организационными структурами по вопросам кибербезопасности на региональном и глобальном уровнях при помощи таких мероприятий, как тренировочные занятия по кибербезопасности и другие.

Раздел 5. Руководящие указания по использованию направления 4 – Создание потенциала

**5** В свете вышесказанного ГПК и рекомендации по этому направлению, представленные в Отчете HLEG 2008 года, по-прежнему служат надежной основой, способствующей укреплению и продвижению междисциплинарного подхода к вопросам создания потенциала. С учетом этого МСЭ предлагается силами своего Бюро развития электросвязи (БРЭ):

**a)** Продолжать поощрение более открытого и всеобъемлющего взаимодействия и координации между различными национальными, региональными и международными организациями, которые участвуют в работе по созданию потенциала в области кибербезопасности, для того чтобы обеспечивать 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 в сотрудничестве с заинтересованными партнерами и сообществами, занимающимися вопросами укрепления потенциала.

Продолжать усилия по созданию потенциала для преодоления разрыва в стандартизации, в том числе путем оказания странам технической помощи по их просьбе.

**d)** Усиливать и поощрять обмен передовым опытом между Государствами-Членами, чтобы помочь странам, не имеющим достаточного опыта в области кибербезопасности, укрепить свое положение в этой сфере 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 в области кибербезопасности. Для этого необходимо развивать более тесное взаимодействие с академическими организациями, частным сектором и Государствами-Членами.

**f)** Продолжать уделять особое внимание потребностям более уязвимых групп населения, таких как женщины, дети, лица с ограниченными возможностями, лица с особыми потребностями, а также лица с ограниченными возможностями возрастного характера, в рамках усилий по созданию потенциала.

**g)** Продолжать развивать и укреплять применение Глобального индекса кибербезопасности (GCI) в качестве инструмента для создания потенциала и повышения осведомленности.

**h)** Продолжать поддерживать Государства-Члены программами по созданию потенциала для молодежи в системах начального, среднего и высшего образования, а также профессионального обучения для взрослых, с тем чтобы способствовать подготовке большего числа специалистов по вопросам кибербезопасности во всем мире и повысить осведомленность в области кибербезопасности

**i)** Продолжать содействовать определению направлений научно-исследовательской деятельности, связанных с кибербезопасностью, между заинтересованными сторонами, особенно в сфере возникающих технологий, используя возможности организаций частного сектора и академических организаций, являющихся членами МСЭ.

**j)** 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 укреплении уверенности и доверия при использовании ИКТ, а также продолжать содействовать развитию культуры кибербезопасности.

Раздел 6. Руководящие указания по использованию направления 5 − Международное сотрудничество

**6** Организация Объединенных Наций играет уникальную роль в содействии сотрудничеству, диалогу и координации между всеми государствами, а также представителями частного сектора и другими заинтересованными сторонами по вопросам глобальной кибербезопасности. Учитывая сквозной характер этого направления и многообразие форматов сотрудничества и партнерства в различных Секторах МСЭ, всем Секторам МСЭ важно работать в тесном взаимодействии и координировать свои усилия как на внутреннем, так и на внешнем уровне, используя эффективные механизмы межсекторальной координации и назначенных координаторов. В этом контексте рекомендации, содержащиеся в Отчете HLEG 2008 года, по-прежнему сохраняют свою актуальность, а на основании информации, представленной в вышеприведенном разделе, предлагаются следующие дополнительные руководящие указания по использованию МСЭ направления 5 в рамках своего мандата:

**a)** Учитывая свое положение в системе ООН как специализированного учреждения в области ИКТ и единственной содействующей организацией по Направлению деятельности C5 ("Укрепление доверия и безопасности при использовании ИКТ"), МСЭ должен продолжать играть ведущую роль в соответствующих вопросах.

**b)** На основаниипроцесса ВВУИО, в том числе его составляющих, связанных с Направлением деятельности 5, и принимая во внимание усилия Группы высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, МСЭ следует содействовать укреплению посреднических усилий, направленных на объединение различных участников, в том числе на Форуме ВВУИО и ФУИ.

**c)** [Следует и дальше поощрять проведение двусторонних и многосторонних обсуждений между ключевыми участниками; вместе с тем, учитывая глобальный характер кибербезопасности, также необходимо способствовать организации более широких дискуссий с привлечением большего числа участников, включая частный сектор, органы системы ООН, академические организации, гражданское общество и другие заинтересованные стороны, с тем чтобы обеспечить [глобальное] общее понимание кибербезопасности с целью смягчения последствий связанных с этим проблем. В этом отношении МСЭ следует играть посредническую роль и совместно с партнерами содействовать объединению всех заинтересованных сторон в рамках более широкого глобального контекста Организации Объединенных Наций.]

**d)** 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.

**e)** МСЭ следует продолжать взаимодействовать с другими ключевыми учреждениями системы ООН, чтобы поддерживать внутренние усилия Секретариата ООН по согласованию и оптимизации своих программ и видов деятельности в области кибербезопасности, с тем чтобы более эффективным образом служить мировому сообществу.

Раздел 7. Общие руководящие указания для всей структуры ГПК

**7** В процессе разработки руководящих указаний по использованию ГПК появилось несколько широких сквозных руководящих указаний, которые применимы и актуальны для всех аспектов работы МСЭ и для всех пяти направлений ГПК. Ниже представлены общие руководящие указания, которые составлены с учетом тесной взаимосвязи между направлениями и необходимости выработки МСЭ и его членами целостной и всеобъемлющей концепции деятельности в области кибербезопасности:

**a)** Учитывая увеличение числа заинтересованных сторон, организаций, партнерств и различных площадок, занимающихся вопросами кибербезопасности и способствующих достижению прогресса в его различных аспектах, МСЭ следует продолжать укреплять и наращивать сотрудничество и взаимодействие ради общего блага всех заинтересованных сторон, расширяя обмен знаниями, информацией и экспертным опытом и не допуская дублирования усилий.

**b)** МСЭ следует взять на себя функции хранения информации по различным глобальным видам деятельности, инициативам и проектам, посвященным тем или иным аспектам кибербезопасности, которые осуществляются другими заинтересованными сторонами и организациями, работающими в этой сфере и возможно имеющими главный мандат, роль и/или обязанности в отношении этих конкретных аспектов, с тем чтобы у международного сообщества был удобный доступ ко всем таким ресурсам.

**c)** Вся работа, которая осуществляется МСЭ в рамках ГПК, должна опираться на четкий анализ потребностей и целей его членов с использованием таких инструментов, как GCI, преследуемых ими целей и результатов, которые необходимо достичь, и соответствовать показателям и измерениям, разработанным специально для этой цели.

**d)** МСЭ следует и далее следить за событиями в области разработки и использования новых и возникающих ИКТ, с тем чтобы ориентировать Государства-Члены и заинтересованные стороны в отношении аспектов безопасности этих технологий в областях, относящихся к его мандату, и, в соответствующих случаях, их возможного применения в целях противодействия киберугрозам.

**e)** Поскольку вопросы кибербезопасности по определению имеют международный и межотраслевой характер, МСЭ следует содействовать осуществлению видов деятельности, инициатив и проектов, которые могут помочь Государствам-Членам в укреплении общегосударственного подхода к решению этого вопроса.

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

1. 1 Протокол семнадцатого пленарного заседания Полномочной конференции, Дубай, четверг, 15 ноября 2018 года, размещен по адресу: <https://www.itu.int/md/S18-PP-C-0174/en>. [↑](#footnote-ref-1)
2. 2 Передача Отчета бывшего председателя Группы экспертов высокого уровня по ГПК (C19/58), МСЭ, 8 мая 2019 года, размещено по адресу: <https://www.itu.int/md/S19-CL-C-0058/en>. [↑](#footnote-ref-2)
3. 3 Краткий отчет о шестом пленарном заседании (C19/117), МСЭ, 20 июня 2019 года, размещен по адресу: <https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)