|  |  |
| --- | --- |
| **СОВЕТ 2020 Женева, 9–19 июня 2020 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Документ C20/36-R** |
| **5 мая 2020 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря | |
| ОТЧЕТ, РАЗЪЯСНЯЮЩИЙ, как МСЭ в настоящее время использует структуру [Глобальной программы кибербезопасности](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (ГПК) | |

|  |
| --- |
| Резюме  В 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 (бывшего председателя HLEG) и при участии Государств-Членов был сформулирован для рассмотрения Советом проект руководящих указаний по использованию ГПК Союзом (см. С20/65).  Одновременно на рассмотрение Совета представляется настоящий отчет, разъясняющий, как МСЭ в настоящее время использует ГПК.  Необходимые действия  Совету предлагается **принять к сведению** настоящий отчет.  \_\_\_\_\_\_\_\_\_\_\_\_  Справочные материалы  [*Глобальная программа кибербезопасности (ГПК)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*;* [*Документ C20/65 Совета*](https://www.itu.int/md/S20-CL-C-0065/en) |

# 1 Введение

**1.1** Полномочная конференция МСЭ 2018 года, состоявшаяся в Дубае, приняла Резолюцию 130: "*Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий*".В Резолюции содержится, наряду с прочим, решение *использовать структуру* [*Глобальной программы кибербезопасности (ГПК*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*) 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 (HLEG), в котором отмечалось, что для более эффективного использования ГПК можно было бы разработать соответствующие руководящие указания[[2]](#footnote-2)2. 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 при поддержке Старшего судьи (в отставке) Штайна Шольберга (бывшего председателя HLEG) и при участии Государств-Членов был подготовлен проект таких руководящих указаний по использованию ГПК Союзом для рассмотрения и утверждения Советом[[4]](#footnote-4)4. Одновременно Генеральный секретарь подготовил для рассмотрения Советом данный отчет, разъясняющий, как МСЭ в настоящее время использует ГПК.

# 2 Базовая информация

**2.1** В соответствии с указанием Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и Полномочной конференции МСЭ, важнейшая роль МСЭ заключается в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).

**2.2** На ВВУИО главы государств и мировые лидеры поручили МСЭ роль содействующей организации по Направлению деятельности С5 "*Укрепление доверия и безопасности при использовании ИКТ*", в связи с чем в 2007 году МСЭ приступил к реализации ГПК в качестве основы для международного сотрудничества в этой области.

**2.3** Осуществление ГПК началось в 2007 году; она призвана способствовать сотрудничеству и эффективности, поощрению взаимодействия со всеми заинтересованными сторонами и между ними. Программа включает в себя пять направлений, или областей работы: правовые меры, технические и процедурные меры, организационные структуры, создание потенциала и международное сотрудничество.

**2.4** Впоследствии, в октябре 2007 года, была создана HLEG по ГПК под председательством Старшего судьи (в отставке) Штайна Шольберга для оказания помощи Генеральному секретарю МСЭ в разработке для Государств-Членов стратегических предложений по содействию кибербезопасности.

**2.5** HLEG состоит из независимой группы глобального уровня, которая объединяет почти 100 экспертов, представляющих различные заинтересованные стороны. Группа представила свои рекомендации Генеральному секретарю по всем пяти направлениям в Отчете председателя в августе 2008 года (Отчет HLEG 2008 г.)[[5]](#footnote-5)5.

**2.6** В 2008 году работа по направлениям ГПК стала крупным нововведением с точки зрения глобального подхода к решению вопросов кибербезопасности. С момента представления Отчета HLEG 2008 года прошло больше десяти лет. В целом весь мир признает, что ИКТ являются важнейшим инструментом достижения Целей устойчивого развития (ЦУР) ООН и что для выполнения ИКТ этой функции необходимо, чтобы все люди, где бы они ни находились, испытывали доверие и уверенность при их использовании. Таким образом, задача "*Укрепление доверия и безопасности при использовании ИКТ*" сегодня, как никогда, значима в контексте достижения ЦУР.

**2.7** Структура, которую обеспечивают пять направлений ГПК, получила высокую оценку сообщества членов МСЭ, выдержав проверку временем в целом, и по-прежнему является широкой основой для международного сотрудничества в области кибербезопасности на базе итоговых документов ВВУИО, в частности принципов, изложенных в Направлении деятельности С5. Вся работа МСЭ в этой области продолжает строиться вокруг пяти направлений ГПК.

**2.8** С момента начала осуществления ГПК МСЭ последовательно отчитывается перед Советом о своей деятельности по укреплению доверия и безопасности при использовании ИКТ, представляя ежегодный отчет, структурированный по пяти направлениям; это подчеркивает взаимодополняющий характер действующих программ работы МСЭ и облегчает осуществление деятельности БРЭ, БСЭ и БР в данной сфере.

**2.9** Подробная информация об этой деятельности содержится в документах [C08/33](https://www.itu.int/md/S08-CL-C-0033/en), [C09/50](https://www.itu.int/md/S09-CL-C-0050/en), [C10/12](https://www.itu.int/md/S10-CL-C-0012/en), [C11/54](https://www.itu.int/md/S11-CL-C-0054/en), [C12/29](https://www.itu.int/md/S12-CL-C-0029/en), [C13/23](https://www.itu.int/md/S13-CL-C-0023/en), [C14/23](https://www.itu.int/md/S14-CL-C-0023/en), [C15/18](https://www.itu.int/md/S15-CL-C-0018/en), [C16/18](https://www.itu.int/md/S16-CL-C-0018/en), [C17/18](https://www.itu.int/md/S17-CL-C-0018/en), [C18/18](https://www.itu.int/md/S18-CL-C-0018/en), [C19/18](https://www.itu.int/md/S19-CL-C-0018/en) и [C20/18](https://www.itu.int/md/S20-CL-C-0018/en). В следующих разделах приводятся некоторые примеры деятельности МСЭ согласно структуре ГПК.

# 3 Некоторые примеры деятельности МСЭ

**3.1** Как содействующая организация по Направлению деятельности С5 МСЭ использует структуру ГПК для объединения различных заинтересованных сторон в деле оказания странам помощи в преодолении рисков, связанных с ИКТ, и работает в тесном партнерстве с другими организациями по линии всех своих секторов и видов деятельности над укреплением доверия и уверенности при использовании ИКТ.

**3.2** В разделах ниже приводятся примеры деятельности МСЭ по каждому из пяти направлений, при том понимании, что между ними существует взаимозависимость. Это сделано для того, чтобы дать краткое представление о ряде видов деятельности, тогда как более подробные сведения включены в отдельные отчеты, представляемые Совету с 2008 года (см. п. 2.9 выше).

**3.3** В качестве примера сквозной инициативы, охватывающей все пять направлений ГПК, в отдельном разделе описывается [инициатива "Защита ребенка в онлайновой среде](https://www.itu.int/en/cop/Pages/default.aspx)".

## 3.4 Направление 1 ГПК: Правовые меры

a) Неотъемлемой составляющей любой национальной стратегии кибербезопасности является принятие соответствующего согласующегося с региональной и международной политикой и практикой законодательства против ненадлежащего использования ИКТ в преступных целях.

b) В области правовых мер МСЭ тесно сотрудничает с такими партнерами как УНП ООН и с другими экспертами. Союз также продолжает оказывать Государствам-Членам помощь в расширении их понимания правовых аспектов кибербезопасности, используя для этого [ресурсы МСЭ по законодательству в области киберпреступности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx), с тем чтобы содействовать согласованию их нормативно-правовых баз.

## 3.5 Направление 2 ГПК: Технические и процедурные меры

a) [Исследовательские комиссии МСЭ](https://www.itu.int/ru/mediacentre/backgrounders/Pages/itu-study-groups.aspx) представляют собой независимую глобальную платформу, позволяющую членам МСЭ собираться для совместной работы по стандартизации в области безопасности по ряду тем: архитектура и структура безопасности; безопасность приложений и услуг для существующих и возникающих технологий, таких как технологии распределенного реестра (одним из вариантов применения которых является блокчейн), облачные вычисления, большие данные, искусственный интеллект и машинное обучение, организация сетей с программируемыми параметрами, 5G, интернет вещей, интеллектуальные транспортные системы и "умные" электросети; базовые структуры безопасности, такие как PKI, управление определением личности и аутентификация; а также кибербезопасность (включая обмен информацией о киберугрозах).

b) [17-я Исследовательская комиссия МСЭ-T](https://www.itu.int/ru/ITU-T/studygroups/2013-2016/17/Pages/default.aspx) отвечает за вопросы укрепления доверия и безопасности в использовании ИКТ. К ним относится и исследование ряда технологий с точки зрения кибербезопасности. Это ведущая исследовательская комиссия по вопросам безопасности и по вопросам управления определением идентичности (IdM), которая по-прежнему играет полезную роль в проведении исследований и стандартизации в области кибербезопасности, борьбы со спамом, IdM, инфраструктуры открытых ключей (сертификатов X.509 МСЭ-Т), управления информационной безопасностью, повсеместно распространенных сенсорных сетей, телебиометрии, безопасности подвижной связи, безопасности виртуализации в интересах безопасности облачных вычислений, защиты информации, позволяющей установить личность, а также архитектуры безопасности и безопасности приложений, в сотрудничестве с внешними организациями по разработке стандартов. На сегодняшний день комиссия разработала более 200 стандартов. В настоящее время Исследовательская комиссия наряду с другими темами работает над вопросом обеспечения безопасности на квантовой основе и составила Рекомендации Х.1701 – спецификации для "Архитектуры генератора случайных чисел квантового шума".

c) Другие исследовательские комиссии, такие как ИК9, ИК13, ИК15 и ИК20 (IoT), также осуществляют разработку стандартов, связанных с безопасностью.

d) Вопросы безопасности и доверия являлись и являются неотъемлемой составляющей дискуссий во многих существующих и прежних оперативных группах МСЭ-Т, к числу которых относятся: 1) [*Оперативная группа МСЭ-Т по машинному обучению для будущих сетей, включая 5G (ОГ-ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx), 2) [*Оперативная группа МСЭ-Т "Технологии для Сети-2030 (ОГ-NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx), 3) [*Оперативная группа МСЭ-T по искусственному интеллекту для здравоохранения (ОГ-AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h), 4) [*Оперативная группа МСЭ-Т по мультимедиа в автотранспортных средствах (ОГ-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx), 5) [*Оперативная группа МСЭ-Т "ИИ для автономного и ассистированного вождения" (ОГ-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx), 6) [*Оперативная группа МСЭ-Т по квантовым информационным технологиям для сетей (ОГ-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx).

e) Продолжается работа МСЭ-R по стандартизации в области радиосвязи с учетом постоянного развития современных сетей электросвязи. МСЭ-R разработал четкие принципы безопасности для сетей IMT (3G, 4G и 5G) (Рекомендации МСЭ-R M.1078, M.1223, M.1457, M.1645, М.2012 и М.2083). Выпущены также Рекомендации по вопросам безопасности в архитектуре сетевого управления для цифровых спутниковых систем (Рекомендация МСЭ-R S.1250) и по повышению производительности протокола управления передачей по спутниковым сетям (Рекомендация МСЭ-R S.1711).

## 3.6 Направление 3 ГПК: Организационные структуры

a)Для уверенной борьбы с киберугрозами и киберинцидентами необходимы эффективные механизмы и институциональные структуры на национальном уровне. Отсутствие таких учреждений и недостаточный национальный потенциал являются настоящей проблемой для эффективного реагирования на кибератаки. Важную роль в решении этой проблемы играют национальные группы реагирования на компьютерные инциденты (CIRT).

b) МСЭ ведет работу с Государствами-Членами в целях создания потенциала на национальном и региональном уровнях, расширения возможностей и содействия созданию и усовершенствованию работы национальных CIRT. Союз провел технические оценки для определения готовности к [созданию CIRT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) в 76 странах и участвует в 20 проектах по их созданию; 14 из них успешно завершились созданием полноценно функционирующих национальных возможностей. Еще большее количество проектов осуществляется или планируется к осуществлению.

c) МСЭ проводит регулярные региональные и национальные учения – [тренировочные занятия по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) в целях укрепления способности стран реагировать на угрозы и расширения тем самым национального и международного сотрудничества Государств-Членов в деле борьбы с киберугрозами и кибератаками. На сегодняшний день МСЭ провел 28 тренировочных занятий по кибербезопасности с участием более 100 стран.

## 3.7 Направление ГПК 4: Создание потенциала

a) МСЭ провел для всех регионов МСЭ [региональные форумы по кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) с целью создания потенциала для различных программ и видов деятельности БРЭ, а также обеспечения рабочей платформы для сотрудничества на региональном и международном уровнях.

b) МСЭ оказывает Государствам-Членам содействие в разработке и усовершенствовании эффективных национальных стратегий кибербезопасности. [Руководство по разработке национальной стратегии кибербезопасности (NCS)](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-R.pdf), разработанное в рамках многостороннего процесса сотрудничества, представляет собой полезное практическое руководство и функциональный комплекс инструментов, который применяется странами во всех регионах при разработке и усовершенствовании национальных стратегий кибербезопасности. С момента его публикации в сентябре 2018 года национальные и региональные семинары-практикумы были организованы более чем в 20 странах, причем трем странам была оказана непосредственная помощь в разработке и пересмотре национальных стратегий кибербезопасности на основании Руководства.

c) МСЭ учредил [Глобальный индекс кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI), который является надежным средством оценки степени выполнения странами обязательств в области кибербезопасности на глобальном уровне, для повышения осведомленности о важности и различных аспектов данного вопроса. Уровень развития или участия каждой страны оценивается по пяти направлениям ГПК, которая служит общей базой и рамочной основой инициативы. GCI, опирающийся на многосторонний подход и инициативу, задействует потенциал и экспертные знания различных организаций в целях улучшения качества обследования, поощрения международного сотрудничества и обмена знаниями по этой теме. В настоящее время реализуется четвертая версия обследования на основе глобального индекса кибербезопасности.

## 3.8 Направление 5 ГПК: Международное сотрудничество

a) ГПК основана на международном сотрудничестве и направлена на объединение усилий всех соответствующих заинтересованных сторон в целях укрепления доверия и безопасности при использовании ИКТ.

b) МСЭ продолжает развивать и поддерживать отношения и партнерские связи с различными региональными/международными организациями и инициативами, в том числе со Всемирным экономическим форумом (ВЭФ), Инициативой Содружества по борьбе с киберпреступностью, ENISA, Интерполом, ЭКОВАС, Всемирным банком, FIRST и региональными ассоциациями CSIRT/CERT, такими как AP CERT, AFRICA CERT и OIC CERT. Эти партнерские связи способствуют расширению многостороннего сотрудничества в видах деятельности, общих для всех направлений ГПК.

c) Как содействующая организация по Направлению деятельности С5 ВВУИО МСЭ использует возможности процесса ВВУИО, включая ежегодный Форум ВВУИО, для содействия развитию многостороннего диалога. Каждый год в рамках [Форума ВВУИО](https://www.itu.int/net4/wsis/forum/2019/ru) МСЭ организует проведение Диалогов высокого уровня, собраний содействующих организаций по Направлению С5, а также тематических семинаров-практикумов по вопросам кибербезопасности.

d) С учетом большого значения работы по формированию в рамках ООН общего понимания нужд и потребностей, связанных с надлежащей организацией программ и инициатив, которые будут служить эффективным подспорьем для усилий, прилагаемых всеми заинтересованными сторонами, в 2010 году был сделан первый важный шаг на пути к улучшению внутренней координации между учреждениями ООН при оказании содействия государствам-членам в вопросах кибербезопасности. По просьбе Координационного совета руководителей системы ООН (КРС) МСЭ и УНП ООН в сотрудничестве с 33 другими учреждениями ООН в течение двух лет вели работу по созданию общей структуры ООН по кибербезопасности и киберпреступности, которая была утверждена КСР в ноябре 2013 года. С тех пор МСЭ продолжает вносить свой вклад в осуществление различных инициатив в этой сфере, нацеленных на улучшение внутренней координации и сотрудничества в системе ООН.

## 3.9 Инициатива "Защита ребенка в онлайновой среде"

a) МСЭ приступил к реализации инициативы "[Защита ребенка в онлайновой среде](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx)" как многостороннего мероприятия в рамках ГПК. Инициатива объединяет партнеров из всех секторов глобального сообщества для разработки стратегий кибербезопасности и содействия формированию безопасной онлайновой среды для детей во всем мире.

b) Ключевыми задачами СОР являются: а) определение рисков и уязвимости детей в киберпространстве; b) расширение осведомленности; с) разработка практических инструментов для содействия в минимизации рисков; и d) обмен знаниями и опытом.

c) COP осуществляется в рамках целостного подхода, направленного на поощрение безопасности ребенка в онлайновой среде, разработку стратегий, охватывающих пять направлений ГПК:

**• Правовые меры**: Важнейшим инструментом содействия формированию благоприятной и безопасной онлайновой среды для детей и молодежи является комплексная основа закона. В рамках COP отслеживаются подходы, которые принимают разные страны, имеющие разные правовые системы, и выпускаются руководящие указания в помощь Государствам-Членам при достижении поставленных ими целей.

**• Технические и процедурные меры**: В рамках COP разрабатываются ключевые рекомендации и стандарты в поддержку защиты ребенка в онлайновой среде всеми основными заинтересованными сторонами.

**• Организационные структуры**: COP содействует формированию типовых национальных структур, которые будут способствовать обеспечению благоприятной онлайновой среды для детей и молодежи. В рамках COP поощряется создание отделений COP на национальном уровне и разрабатывается набор показателей для оценки хода реализации инициатив по защите ребенка в онлайновой среде на всемирном, региональном и национальном уровнях.

**• Создание потенциала**: В рамках СОР оказывается содействие странам в развертывании национальных структур СОР и организуются стратегические мероприятия на региональном и глобальном уровнях в поддержку этих процессов.

**• Международное сотрудничество**: COP направлена на поощрение глобальной культуры "Цифрового гражданства" и стимулирование заключения соглашений о сотрудничестве для обмена информацией в целях устранения или смягчения рисков, которым подвергаются дети и молодые люди в онлайновой среде.

d) По различным направлениям ГПК осуществляется целый ряд видов деятельности; с момента объявления об инициативе подробная информация о них размещается на [вебсайте СOP](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx), а также включается в ежегодные отчеты Совету. К этим видам деятельности относятся разработка инструментов и ресурсов, таких как руководящие указания для детей, родителей и педагогов, представителей отрасли и директивных органов. Многосторонняя группа экспертов, в состав которой входят более 50 организаций и отдельных специалистов, приступила к пересмотру [Руководящих указаний по защите ребенка в онлайновой среде](https://www.itu.int/en/cop/Pages/guidelines.aspx), впервые изданных в 2009 году.

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

1. 1 Протокол семнадцатого пленарного заседания Полномочной конференции, Дубай, четверг, 15 ноября 2018 года. [↑](#footnote-ref-1)
2. 2 Передача Отчета бывшего председателя Группы экспертов высокого уровня по ГПК (C19/58), МСЭ, 8 мая 2019 года, <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, <https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)
4. 4 Размещено в онлайновом доступе для открытых консультаций с заинтересованными сторонами ВВУИО по адресу: <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. 5 Судья Штайн Шольберг: Отчет Председателя HLEG: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-5)