|  |  |
| --- | --- |
| **СОВЕТ 2019Женева, 10–20 июня 2019 года** | logo_R_ |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.5** | **Документ C19/58-R** |
| **6 мая 2019 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря |
| ПЕРЕДАЧА ОТЧЕТА БЫВШЕГО ПРЕДСЕДАТЕЛЯГРУППЫ ЭКСПЕРТОВ ВЫСОКОГО УРОВНЯ ПО ГПК |

|  |
| --- |
| РезюмеНа семнадцатом пленарном заседании ПК-18 **Генеральный секретарь** 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.Необходимые действияСовету предлагается **принять к сведению** настоящий отчет.\_\_\_\_\_\_\_\_\_\_\_\_Справочные материалы[Документ PP-18/174](https://www.itu.int/md/S18-PP-C-0174/en); [Документ C19/INF/9](http://www.itu.int/md/S19-CL-INF-0009/en) |

**Приложение:** 1

ПРИЛОЖЕНИЕ

**Отчет председателя, 2019 год**

**ПЕРЕСМОТРЕННЫЙ ОТЧЕТ БЫВШЕГО ПРЕДСЕДАТЕЛЯ ГРУППЫ ЭКСПЕРТОВ ВЫСОКОГО УРОВНЯ ПО ГПК**[[1]](#footnote-1)1

**Штайн Шольберг,
старший судья (в отставке)**

**Норвегия**

30 апреля 2019 года

**Кому:**

**Генеральному секретарю МСЭ Хоулиню Чжао**

# 1 Введение

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 ГПК для того, чтобы далее направлять работу Союза по укреплению доверия и безопасности при использовании ИКТ"*.*

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"[[2]](#footnote-2)2..

Базовая информация

Глобальная программа кибербезопасности (ГПК) составляет основу для международного сотрудничества, направленного на укрепление доверия и безопасности в информационном обществе. Цель ГПК − обеспечить взаимодействие и эффективность, стимулируя сотрудничество со всеми соответствующими заинтересованными сторонами и между ними и опираясь на существующие инициативы во избежание дублирования усилий.

Группа экспертов высокого уровня (HLEG) по ГПК создана в октябре 2007 года для оказания помощи Генеральному секретарю МСЭ в разработке для Государств-Членов стратегических предложений по содействию кибербезопасности. Функции председателя Группы выполнял судья Штайн Шольберг, Норвегия, имевший более чем 30-летний опыт работы в сфере законодательства о киберпреступности. Работа HLEG связана с ролью МСЭ, определенной Всемирной встречей по вопросам информационного общества (ВВУИО) как содействующей организации по ее Направлению деятельности C5 "Укрепление доверия и безопасности при использовании ИКТ". Основу этой работы составляет начатая в мае 2007 года Глобальная программа кибербезопасности, которая включает пять стратегических направлений: правовые меры, технические и процедурные меры, организационные структуры, создание потенциала и международное сотрудничество.

В состав HLEG вошли почти 100 независимых международных экспертов многих заинтересованных сторон со всего мира. Группа представила свои рекомендации Генеральному секретарю МСЭ по всем стратегическим направлениям в Отчете председателя в августе 2008 года[[3]](#footnote-3)3. Отчет направил судья Штайн Шольберг, как председатель HLEG по ГПК, и вступительное заявление к Отчету включало следующее:

*Кибератаки влекут за собой существенные затраты – в форме потери дохода, утраты конфиденциальных данных, повреждения оборудования, сбоев, вызываемых атаками "отказ в обслуживании", и выхода из строя сети. Увеличивающиеся киберугрозы создают опасность для будущего роста и потенциала сетевого информационного общества. Кроме того, киберпространство не имеет границ: за считанные минуты кибератаки могут нанести неизмеримый ущерб в разных странах. Кибератаки составляют глобальную проблему, и для борьбы с ними необходимо глобальное решение при участии всех заинтересованных сторон.*

С момента представления Отчета HLEG прошло более 10 лет. Настоящий отчет составлен по результатам анализа развития ситуации после 2008 года.

# 2 Сохраняющаяся актуальность и значимость ГПК

Основа, которую обеспечивают пять стратегических направлений ГПК, получила высокую оценку сообщества членов МСЭ, выдержав, в целом, проверку временем, и она по-прежнему является широкой основой для международного сотрудничества в области кибербезопасности на базе итоговых документов ВВУИО, в частности принципов, изложенных в Направлении деятельности С5. Соответствующие рекомендации, включенные в Отчет председателя HLEG 2008 года, актуальны сегодня также, как и в 2008 году (хотя следует признать, что ряд аспектов Отчета можно считать устаревшими или замещенными другими событиями).

За прошедшее с 2008 года время среда ИКТ безусловно кардинально изменилась, и теперь ИКТ − это движущие силы каждого сектора общества и, в частности, всей важнейшей инфраструктуры, которую страны используют в качестве основы своего бесперебойного функционирования. На наших глазах возникают и внедряются новые технологии, например широкое распространение интернета вещей, который соединит между собой десятки, если не сотни миллиардов новых устройств, влечет за собой значительное число новых потенциальных уязвимостей; появление искусственного интеллекта как инструмента использования потенциала данных, в особенности больших данных, для того чтобы люди могли принимать решения, используя всю имеющуюся информацию, а также для создания возможности принятия машинами автономных и так называемых интеллектуальных решений самостоятельно и без вмешательства человека, обусловливает проблемы конфиденциальности, безопасности и доверия применительно как к пользователям, так и к алгоритмам и инструментам; новые технологии и стандарты связи, как например, 5G, обеспечивающие связь со скоростью, многократно большей, чем достижимая сегодня; квантовые вычисления, которые предлагают вычислительное быстродействие, выходящее за пределы современных возможностей, открывают широкие перспективы, но и создают угрозы, в том числе для действующих в настоящее время криптографических алгоритмов. Мы наблюдали также появление новых технологий безопасности, таких как технологии распределенного реестра (наиболее популярной реализацией которых являются блокчейны), обеспечивающих существенно более эффективные средства защиты систем и связанных с ними данных. Кроме того, в настоящее время в мире растет число стран, которые все более активно переходят к внедрению систем цифровой идентификации.

Наряду с этим следует отметить явление, которое после 2008 года в значительной степени определило формат глобальной экосистемы ИКТ, − всемирное широкомасштабное распространение социальных сетей. Число пользователей ряда компаний превышает численность совокупного населения многих стран, например число пользователей Facebook превышает 2,3 млрд. (март 2019 г.). Социальные сети играют ключевую роль в соединении людей по всему миру, стирая географические границы и обеспечивая простой доступ к информации и возможностям в таких масштабах, которые прежде не существовали. Но они также вызвали серьезные проблемы доверия, связанные с конфиденциальностью и безопасностью пользователей и создаваемых ими данных, подлинностью и надежностью информации, доступной в социальных сетях, распространением контента, разжигающего ненависть, и т. д.

В целом ИКТ во всемирном масштабе признаны ключевым средством достижения Целей устойчивого развития, определенных Организацией Объединенных Наций, а для этого важно, чтобы люди, используя ИКТ, чувствовали доверие и уверенность.

Проводимая в рамках ГПК деятельность развивается, учитывая изменения среды ИКТ, в том числе деятельность, проводимая МСЭ[[4]](#footnote-4)4 в соответствии со своим мандатом и своей ролью содействующей организации по Направлению деятельности C5 ВВУИО.

ГПК эффективно содействует деятельности МСЭ по укреплению доверия и безопасности при использовании ИКТ. Руководствуясь своим мандатом и реализацией ГПК, МСЭ прилагает усилия к тому, чтобы объединить различные заинтересованные стороны для совместной работы по выполнению ряда важнейших инициатив, таких как помощь странам в определении своей национальной стратегии в области кибербезопасности, укреплении своей инфраструктуры путем разработки и внедрения международных стандартов безопасности, создании собственных групп реагирования на компьютерные инциденты, развертывании инициатив по защите ребенка в онлайновой среде, а также создании необходимого человеческого потенциала и приобретении требуемых навыков. В рамках ГПК начато выполнение различных инициатив с участием многих заинтересованных сторон, например инициативы "Защита ребенка в онлайновой среде".

# 3 Поиск общей позиции по кибербезопасности

Кибербезопасность составляет важную часть глобальной повестки дня глав государств и мировых лидеров, а также руководителей компаний частного сектора, международных организаций и организаций гражданского общества во всем мире. Как указано выше, в настоящее время выполняется несколько заслуживающих одобрения инициатив, предложенных разными группами заинтересованных сторон. Некоторые изменения, произошедшие после 2008 года на региональном и глобальном уровнях, отражены в [Документе INF/9](http://www.itu.int/md/S19-CL-INF-0009/en).

Однако несмотря на это, растет дефицит доверия в киберпространстве. Неоднократно отмечавшаяся задача, которая требует решения, заключается в необходимости обеспечить более высокий уровень согласованности и связанности инициатив, для того чтобы они оказывали максимальное воздействие. Это должно оставаться в центре внимания МСЭ, выполняющего функцию содействующей организации по Направлению деятельности C5 ВВУИО.

Направления и рекомендации ГПК, в особенности касающиеся международного сотрудничества, должны и далее использоваться Союзом в качестве основы, определяющей его соответствующие усилия по координации.

Для обеспечения большей ясности и эффективности при выполнении рекомендаций ГПК, принимая во внимание сложность вопросов, возникающих в связи с быстро меняющейся экосистемой ИКТ, может потребоваться дальнейшая разработка соответствующих руководящих принципов использования ГПК.

Как председатель HLEG 2008 года, я готов консультировать Генерального секретаря МСЭ по любой деятельности в этой области.

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

1. 1 Содержащаяся в настоящем Отчете информация была подготовлена и представлена председателем HLEG по ГПК на основе общедоступной информации. Мнения, выраженные в данной публикации, являются исключительно мнениями автора. [↑](#footnote-ref-1)
2. 2 Протокол семнадцатого пленарного заседания Полномочной конференции, Дубай, четверг, 15 ноября 2018 года. [↑](#footnote-ref-2)
3. 3 См.: Судья Штайн Шольберг, Норвегия, "Отчет председателя Группы экспертов высокого уровня" <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-3)
4. 4 См. ежегодный отчет Совету МСЭ о деятельности МСЭ по укреплению доверия и безопасности при использовании ИКТ. [↑](#footnote-ref-4)