|  |  |
| --- | --- |
| **СОВЕТ 2021 Виртуальные консультации Советников, 8–18 июня 2021 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Документ C21/71-R** |
| **22 апреля 2021 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря | |
| руководящиЕ указаниЯ по использованию Глобальной программы кибербезопасности | |

|  |
| --- |
| 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 (бывший председатель HLEG), проф.а Соланж Гернаути и г‑на Нобору Накатани, и при участии Государств-Членов и других заинтересованных сторон был сформулирован проект руководящих указаний для рассмотрения и утверждения Советом. Важно отметить, что эта деятельность не направлена на пересмотр ГПК и этот вопрос не будет затрагиваться в ее рамках.  В соответствии с процессом разработки проекта руководящих указаний, описанным в Циркулярном письме ([CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)), 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. Предыдущий вариант этого документа был первоначально подготовлен в качестве Документа [C20/65](https://www.itu.int/md/S20-CL-C-0065/en) для представления на сессии Совета 2020 года, но не рассматривался.  Необходимые действия  Настоящий документ представляется Совету для **рассмотрения** и **утверждения** в установленном порядке.  \_\_\_\_\_\_\_\_\_\_\_\_  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)* |

**Содержание**

Стр.

[**Раздел 1 − Введение**  **3**](#_Toc41467783)

[Базовая информация 4](#_Toc41467784)

[Контекст 4](#_Toc41467785)

[Сохраняющаяся актуальность и применимость ГПК как глобальной основы действий 7](#_Toc41467786)

[**Раздел 2 − Направление 1: Правовые меры**  **8**](#_Toc41467787)

[Введение 8](#_Toc41467788)

[Изменения в правовой сфере после 2008 года 9](#_Toc41467789)

[Руководящие указания по использованию направления 1 − Правовые меры 11](#_Toc41467792)

[**Раздел 3 − Направление 2: Технические и процедурные меры**  **13**](#_Toc41467793)

[Введение 13](#_Toc41467794)

[Изменение ситуации в области технических и процедурных мер с 2008 года 13](#_Toc41467795)

[Руководящие указания по использованию направления 2 – Технические и процедурные меры 14](#_Toc41467797)

[**Раздел 4 − Направление 3: Организационные структуры** **15**](#_Toc41467798)

[Введение 15](#_Toc41467799)

[Изменение ситуации с организационными структурами с 2008 года 16](#_Toc41467800)

[Руководящие указания по использованию направления 3 – Организационные структуры 17](#_Toc41467801)

[**Раздел 5 − Направление 4: Создание потенциала** **18**](#_Toc41467802)

[Введение 18](#_Toc41467803)

[Изменение ситуации в области создания потенциала с 2008 года 18](#_Toc41467804)

[Руководящие указания по использованию направления 4 – Создание потенциала 19](#_Toc41467805)

[Раздел 6 − Направление 5: Международное сотрудничество 21](#_Toc41467806)

[Введение 21](#_Toc41467807)

[Изменение условий международного сотрудничества с 2008 года 21](#_Toc41467808)

[Руководящие указания по использованию направления 5 − Международное сотрудничество 23](#_Toc41467812)

[**Раздел 7 − Общие руководящие указания для всей структуры ГПК** **24**](#_Toc41467813)

# Раздел 1 Введение

**1.1** Полномочная конференция МСЭ 2018 года, состоявшаяся в Дубае, приняла [Резолюцию 130](https://www.itu.int/en/action/cybersecurity/PublishingImages/Lists/resolutions/AllItems/Res%20130.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).

**1.3** 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). 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).

**1.4** В соответствии с этими поручениями при поддержке Старшего судьи (в отставке) Штайна Шольберга (бывший председатель HLEG) и участии Государств-Членов был подготовлен проект таких руководящих указаний по использованию ГПК Союзом для рассмотрения и утверждения Советом[[4]](#footnote-4). 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.

**1.5** В соответствии с процессом разработки проекта руководящих указаний, описанным в Циркулярном письме ([CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)), 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.

Базовая информация

**1.6** 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).

**1.7** На ВВУИО в 2005 году главы государств и мировые лидеры поручили МСЭ роль содействующей организации по Направлению деятельности С5 "*Укрепление доверия и безопасности при использовании ИКТ*"[[5]](#footnote-5), в связи с чем в 2007 году МСЭ приступил к реализации ГПК в качестве основы для международного сотрудничества в этой области.

**1.8** ГПК включает в себя пять направлений, или областей работы: правовые меры, технические и процедурные меры, организационные структуры, создание потенциала и международное сотрудничество. Она призвана обеспечивать многостороннее взаимодействие и эффективность, стимулируя сотрудничество со всеми и между всеми соответствующими заинтересованными сторонам и опираясь на существующие инициативы во избежание дублирования усилий.

**1.9** Впоследствии, в октябре 2007 года, была создана HLEG по ГПК для оказания помощи Генеральному секретарю МСЭ в разработке для Государств-Членов стратегических предложений по содействию кибербезопасности. Функции председателя Группы выполнял Старший судья (в отставке) Штайн Шольберг.

**1.10** В состав HLEG вошли почти 100 независимых международных экспертов со всего мира, представляющих различные заинтересованные стороны. Группа представила свои рекомендации Генеральному секретарю по всем пяти направлениям в Отчете председателя в августе 2008 года (Отчет HLEG 2008 года)[[6]](#footnote-6). В этом отчете председатель HLEG подчеркнул, что:

*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*.

**1.11** В 2008 году работа по пяти 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.

Контекст

**1.12** Основа, которую обеспечивают пять направлений ГПК, получила высокую оценку сообщества членов МСЭ, выдержав, в целом, проверку временем. Программа 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 HLEG 2008 года, остаются актуальными и сегодня[[7]](#footnote-7), за исключением ряда конкретных аспектов, которые можно считать устаревшими или замещенными другими событиями.

**1.13** За прошедшее с 2008 года время среда ИКТ, безусловно, кардинально изменилась, и сегодня ИКТ − это опора каждого сектора общества и подавляющей части всех объектов критической инфраструктуры[[8]](#footnote-8). Для современного мира характерны высокие темпы появления и внедрения новых технологий в качестве примеров можно привести:

• широкое распространение интернета вещей, который соединяет между собой десятки, если не сотни миллиардов новых устройств, что влечет за собой значительное число новых потенциальных уязвимостей;

• развитие искусственного интеллекта как инструмента использования потенциала данных, в особенности больших данных, который позволяет людям принимать решения с учетом всей имеющейся информации, а машинам – принимать автономные и так называемые интеллектуальные решения без вмешательства человека, что обусловливает появление проблем безопасности и доверия, а также соблюдения прав человека;

• новые технологии и стандарты связи, например 5G, обеспечивающие связь со скоростью, многократно большей, чем достижимая сегодня;

• квантовые вычисления, которые обеспечивают вычислительное быстродействие, выходящее за пределы современных возможностей, и открывают широкие перспективы, но одновременно создают угрозы, в том числе для действующих в настоящее время криптографических алгоритмов; и

• новые технологии безопасности, такие как технологии распределенного реестра (популярной реализацией которых являются блокчейны), обеспечивающие существенно более эффективные средства защиты систем и связанных с ними данных. Помимо этого, в мире растет число стран, которые уже активно переходят к внедрению систем цифровой идентичности.

**1.14** Наряду с этим с 2008 года на формат глобальной экосистемы ИКТ в значительной степени повлияло всемирное широкомасштабное распространение социальных сетей. Число пользователей некоторых социальных сетей превышает численность совокупного населения многих стран, например число активных пользователей Facebook в 2020 году составляло в месяц почти 2,8 млрд. человек[[9]](#footnote-9). 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 и с такой скоростью, которые прежде не были возможны. Но они также вызвали серьезные проблемы доверия, связанные с конфиденциальностью и безопасностью пользователей и генерируемых ими данных, подлинностью и надежностью информации, доступной в социальных сетях, распространением контента, разжигающего ненависть, и т. д.[[10]](#footnote-10)

**1.15** Кроме того, ряд других факторов, таких как появление даркнета, продолжает вызывать во всем мире растущую обеспокоенность в связи с преступной деятельностью в киберпространстве, в частности в том, что касается доступа к вредоносным инструментам, услугам и контенту.

**1.16** Ввиду этих обстоятельств все большее признание среди всех заинтересованных сторон, включая правительства, получает факт многообразия срочных действий, которые необходимо предпринять для повышения уровня кибербезопасности, начиная от защиты критической инфраструктуры и заканчивая обеспечением конфиденциальности пользователей. Будучи вопросом, представляющим потенциальную угрозу национальной безопасности всех стран, кибербезопасность находит отражение в повестках дня самых высоких политических уровней в правительствах, которые направляют все больше ресурсов на управление и административные меры для обеспечения "общегосударственного" реагирования в целях укрепления национальной киберустойчивости.

**1.17** Пандемия коронавирусной инфекции COVID-19 лишь в очередной раз продемонстрировала, что ИКТ играют центральную роль в работе систем здравоохранения и безопасности и обеспечении поступательного развития экономики и общества наших стран. Услуги и инфраструктура ИКТ – будь то телеработа, электронная коммерция, телемедицина или дистанционное обучение – обеспечивают бесперебойный доступ к удовлетворению важнейших потребностей. На фоне кризиса, вызванного коронавирусом COVID-19, также обострилась потребность в реагировании на быстро изменяющиеся критические угрозы кибербезопасности, обусловленные высокой степенью зависимости общества от ИКТ.

**1.18** На протяжении последнего десятилетия эволюция каждого из пяти направлений в структуре ГПК шла по своему особому пути.

**1.19** По состоянию на 2020 год более 125 стран подписали и/или ратифицировали те или иные конвенции, декларации, руководящие указания или соглашения по кибербезопасности и борьбе с киберпреступностью, такие как [Конвенция Совета Европы о киберпреступности 2001 года](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185) (Будапештская Конвенция), [Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности](http://eng.sectsco.org/documents/) (2009 г.) и [Конвенция Африканского союза о кибербезопасности и защите личных данных (2014 г.)](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).

**1.20** В соответствии с резолюциями ГА ООН Группа правительственных экспертов (ГПЭ)[[11]](#footnote-11) и Рабочая группа открытого состава (РГОС)[[12]](#footnote-12) изучили некоторые вопросы, касающиеся использования ИКТ в контексте международной безопасности, включая, *среди прочего*, поощрение ответственного поведения государств в киберпространстве, применимость международного права в киберпространстве, формирование потенциала и необходимость реализации и дальнейшего развития мер по укреплению доверия в киберпространстве.

**1.21** Инновационные ИКТ, такие как облачные вычисления, сети с программируемыми параметрами (SDN), виртуализация сетевых функций (NFV), 5G, большие данные, ИИ и т. п., стирают границы между рынками и странами, делая экосистему кибербезопасности все более динамичной и сложной. Появление новых технологий и коммерческих субъектов может привести к возникновению новых факторов уязвимости и угроз, особенно с учетом того, что в частном секторе приоритетное внимание нередко уделяется вопросам показателей деловой эффективности, доли рынка и издержек в ущерб инвестициям в безопасность на этапе проектирования. Есть целый ряд вопросов, вызывающих серьезные трудности при работе над такими технологиями, например поиск способов сокращения числа уязвимостей и их устранения за счет проектируемой безопасности (поскольку продукты становятся уязвимыми начиная уже непосредственно с этапа проектирования), укрепление доверия к продуктам и услугам на протяжении всего их жизненного цикла при помощи схем, протоколов и стандартов аккредитации и законное использование генерируемых пользователями данных при одновременной защите их конфиденциальности. Сокращения числа уязвимостей и уменьшения их влияния можно добиться за счет процессов стандартизации и периодической сертификации/аккредитации, поскольку они содействуют развитию культуры проектируемой безопасности и в то же время укрепляют доверие и уверенность при использовании таких технологий. Однако стандартизация в области безопасности, то есть разработка технических и процедурных мер для обеспечения безопасности, по-прежнему остается труднодостижимой целью, так как для этого требуется, соответственно, высокий уровень технологического развития отрасли, технически компетентные регуляторные органы и эффективные правоохранительные органы.

**1.22** Для решения проблемы кибербезопасности был создан ряд национальных, региональных и международных организаций. В качестве некоторых примеров национальных и региональных инициатив можно привести AFRIPOL, AMERIPOL, GCCPOL, Центр кибербезопасности для Океании (OCSC), Австралийский центр кибербезопасности (ACSC), Европейский центр по вопросам киберпреступности (ЕС3), Российский национальный координационный центр по компьютерным инцидентам и индийский Центр координации по вопросам киберпреступности (I4C). Что касается международных организаций, к числу недавно созданных структур относятся Глобальный центр развития потенциала в области безопасности (GCSCC), Глобальный форум по киберкомпетентности (GFCE), Глобальный комплекс Интерпола по инновациям (IGCI), Глобальный центр по вопросам кибербезопасности ВЭФ, Программа кибербезопасности межамериканского комитета по борьбе с терроризмом (СИКТЕ) Организации американских государств (ОАГ), Экономическое сообщество западноафриканских государств (ЭКОВАС)), Сообщество по вопросам развития юга Африки (САДК) и другие.

**1.23** Кроме того, нехватка навыков и компетенций в техническом, правовом, организационном и людском аспектах кибербезопасности может также оказывать негативное влияние на жизненно важные национальные инфраструктуры. В настоящее время многие конечные пользователи ИКТ, по всей вероятности, не осознают проблемы кибербезопасности в полной мере или не обладают необходимыми навыками или инструментами для эффективной защиты своих данных, конфиденциальности и активов, при этом особому риску подвергаются наиболее уязвимые группы, включая женщин и детей. Развитие навыков и компетенций и принятие мер, которые будут способствовать формированию эффективной культуры кибербезопасности, по-прежнему представляют собой одну из важнейших задач.

Сохраняющаяся актуальность и применимость ГПК как глобальной основы действий

**1.24** Ведущаяся на основе структуры ГПК деятельность, в том числе деятельность, проводимая МСЭ в соответствии с его мандатом и ролью содействующей организации по Направлению деятельности C5 ВВУИО, развивается с учетом изменения среды ИКТ.

**1.25** ГПК служит эффективным подспорьем для деятельности МСЭ по укреплению доверия и безопасности при использовании ИКТ. ГПК как структура применима на глобальном, региональном и национальном уровнях, и ее следует продолжать применять соответствующим образом. Руководствуясь своим мандатом и структурой ГПК, МСЭ прилагает усилия к тому, чтобы объединить различные заинтересованные стороны для совместной работы по осуществлению ряда инициатив, включая помощь Государствам-Членам в: определении своей национальной стратегии в области кибербезопасности, укреплении своей инфраструктуры путем разработки и внедрения международных стандартов безопасности, создании групп реагирования на компьютерные инциденты, развертывании инициатив по защите ребенка в онлайновой среде, а также создании необходимого человеческого потенциала и формировании требуемых навыков. В рамках ГПК осуществляются разнообразные инициативы с участием многих заинтересованных сторон, такие как инициатива по защите ребенка в онлайновой среде[[13]](#footnote-13).

**1.26** В последующих разделах представлены дальнейшие руководящие указания, направленные на повышение эффективности усилий по использованию ГПК. При разработке этих руководящих указаний 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))).

**1.27** 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

Введение

**2.1** Правовой аспект кибербезопасности является одним из ключевых факторов, содействующих укреплению доверия при использовании ИКТ.

**2.2** Как отмечалось в Отчете HLEG 2008 года, направление 1 ГПК призвано содействовать сотрудничеству и служить стратегическим руководством Генеральному секретарю МСЭ в вопросах принятия законодательных мер в ответ на видоизменяющиеся правовые проблемы в области кибербезопасности, включая вопрос о том, как добиться согласованности законодательных мер по борьбе с преступлениями, совершаемыми посредством ИКТ, на международном уровне. В ходе обсуждений было отмечено, что МСЭ мог бы сформулировать стратегии для разработки типового законодательства по борьбе с киберпреступностью в качестве руководящих указаний. В Отчете также рекомендовались соответствующие региональные инициативы, которые можно было бы использовать как основу.

Изменения в правовой сфере после 2008 года

**2.3** Начиная с 2008 года региональные организации разработали целый ряд конвенций, деклараций, соглашений и руководящих указаний в области кибербезопасности. Как отмечалось выше, многие страны подписали и/или ратифицировали те или иные конвенции, декларации, руководящие указания или соглашения по кибербезопасности и борьбе с киберпреступностью, что привело к фрагментации и отсутствию согласованности на международном уровне.

**2.4** В рамках системы ООН, как упоминалось ранее в разделе 1, Генеральная Ассамблея ООН установила два процесса для обсуждения вопроса безопасности при использовании ИКТ - Группу правительственных экспертов (ГПЭ) и Рабочую группу открытого состава (РГОС). После 2004 года Генеральная Ассамблея ООН создала шесть ГПЭ для обсуждения угроз, связанных с использованием ИКТ в контексте международной безопасности, а также вопроса о том, как устранить эти угрозы. Последней из них является [Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности](https://www.un.org/disarmament/group-of-governmental-experts/) (2019–2021 гг.) ([резолюция 73/266](https://dig.watch/instruments/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international)). В своих выводах ГПЭ (2014–2015 гг.) согласилась, что существующие обязательства в соответствии с нормами международного права применимы к использованию ИКТ государствами, и государства должны соблюдать свои обязательства уважать и защищать права человека и основные свободы. В 2018 году [была создана РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности](https://www.un.org/disarmament/open-ended-working-group/) (резолюция 73/27), в которую вошли все заинтересованные государства, для обсуждения следующих вопросов: существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению; дальнейшая выработка правил, норм и принципов ответственного поведения государств; как международное право применяется к использованию ИКТ государствами; меры укрепления доверия; а также возможность организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций. В марте 2021 года РГОС (2019−2021 гг.) приняла путем консенсуса свой [заключительный основной доклад](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf), в котором вновь подтверждалось, что международное право, и в частности Устав ООН, применимы в киберпространстве и далее рекомендовала, чтобы государства поддержали усилия по созданию потенциала в области международного, национального законодательства и политики, поскольку это позволит всем государствам содействовать формированию общего понимания того, как международное право применяется к использованию ИКТ государствами. Ожидается, что РГОС продолжит свою работу, поскольку в соответствии с резолюцией 75/240 создана Рабочая группа открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий (2021−2025 гг.).

**2.5** В рамках системы ООН было также предпринято несколько инициатив и начато несколько процессов, чтобы помочь выявить и устранить юридические проблемы, связанные с кибербезопасностью во всем мире. Так например, Генеральной Ассамблеей ООН в этом отношении было принято несколько резолюций, например, [резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 года о](https://undocs.org/pdf?symbol=en/A/RES/74/247) *[противодействии использованию информационно-коммуникационных технологий в преступных целях](https://undocs.org/pdf?symbol=en/A/RES/74/247)* [(резолюция 74/247)](https://undocs.org/pdf?symbol=en/A/RES/74/247), в которой содержится решение учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

**2.6** С учетом изложенного выше, государства, участвующие в работе этих различных форумов, изучают в настоящее время необходимость продолжения сотрудничества и взаимодействия с другими заинтересованными сторонами в целях поиска общей платформы для достижения взаимопонимания, толкования и уважения международного права в контексте киберпространства, в частности путем содействия более широкому обмену информацией и передовым опытом.

Правовые меры и новые технологии

**2.7** Некоторые эксперты считают, что в отношении новых технологий и методов, используемых в целях совершения преступных действий в киберпространстве, должно применяться уголовное законодательство[[14]](#footnote-14). Многие страны уже приняли либо готовятся к принятию новых законов, касающихся некоторых видов таких преступлений. Важно, чтобы любые соответствующие правовые средства, разработанные в этом отношении, согласовывались с обязательствами стран в области прав человека. Ниже приведен ряд примеров новых и возникающих технологий и тенденций, которые потенциально могут оказать влияние на правовые меры.

**a) Глобальные кибератаки**

Глобальные кибератаки на критические информационно-коммуникационные инфраструктуры стали угрозой для международной и национальной безопасности. Таким глобальным кибератакам подвергаются и правительства, международные организации и частные учреждения, что обуславливает необходимость разработки надежной национальной правовой основы для решения этой проблемы.

**b) Преступные действия в социальных сетях**

Звучат призывы к принятию мер по борьбе с противоправными действиями, такими как агрессивные высказывания, в социальных сетях. Появляются новые инициативы, направленные на решение этих проблем; одна из них – [Глобальный интернет-форум по борьбе с терроризмом](https://www.gifct.org/about/), представляющий собой партнерство между ООН и технологическими компаниями Facebook, Microsoft, Twitter, и YouTube.

**c) Интернет вещей (IoT)**

"Умные" технологии меняют уклад жизни, взаимодействия и работы людей во всем мире[[15]](#footnote-15). Существует немало свежих примеров веб-атак на элементы инфраструктуры интернета по всему миру, совершенных в последнее время бот-сетями, состоящими из скомпрометированных устройств, подключенных к сети, начиная от веб-камер и заканчивая маршрутизаторами. С появлением новых технологий, таких как 5G, и повсеместным распространением связанных между собой устройств, риски с высокой долей вероятности будут возрастать.

**d) Искусственный интеллект (ИИ)**

Прозрачность алгоритмов, включая возможность отслеживания выполняемых действий, является очень важным фактором для обеспечения подотчетности и ответственности за решения, принимаемые частично или полностью автоматизированными системами, и, как следствие, для обеспечения доверия при использовании приложений и услуг ИКТ. Эксперты отмечают, что в случае с некоторыми методами ИИ, такими как глубокое обучение, сделать прозрачным процесс получения результата проблематично. По мере того как автоматизированные процессы принятия решений получают все более широкое применение в потребительских и бизнес-приложениях и услугах, необходимость обеспечения большей ясности правовых аспектов, касающихся подотчетности и ответственности за анализ, производимый такими процессами, и принимаемые в результате решения, будет становиться все более очевидной[[16]](#footnote-16).

**e) Сексуальное насилие над детьми и сексуальная эксплуатация детей в онлайновой среде**

В 1989 году была принята [Конвенция Организации Объединенных Наций о правах ребенка](https://www.ohchr.org/en/professionalinterest/pages/crc.aspx). Статья 34 Конвенции обязывает государства-участники принимать надлежащие меры по защите детей от всех форм сексуальной эксплуатации и насилия. В 2002 году вступил в силу [Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии](https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx). С ростом популярности интернета и социальных сетей сексуальное насилие над детьми в интернете стало более распространенным. Эксперты призывают к применению комплексного подхода для противодействия такому насилию[[17]](#footnote-17). Сюда относятся меры по предотвращению создания веб-сайтов с контентом, содержащим сцены сексуального насилия над детьми, и ограничению доступа к ним, включая блокировку, фильтрацию или иные подобные технологии. В марте 2021 года Комитет по правам ребенка принял свое [замечание общего прядка № 25 (2021 г.) о правах детей в связи с цифровой средой](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en), в котором он разъясняет, каким образом государствам-участникам следует осуществлять Конвенцию применительно к цифровой среде, и дает руководящие указания относительно соответствующих законодательных, политических и других мер.

2.8 Процессуальные нормы – Общие принципы

Принятие процессуальных норм, определяющих полномочия и устанавливающих процедуры по преследованию за преступные действия в киберпространстве, считается одной из важнейших правовых мер, необходимых для предотвращения и расследования киберпреступлений и уголовного преследования за них, а также для обеспечения кибербезопасности во всем мире. Тем не менее некоторые эксперты отмечают, что такие полномочия и процедуры могут также требоваться для преследования за иные уголовные преступления, совершаемые при помощи компьютерных систем, и можно было бы предусмотреть соответствующее регулирование для сбора доказательств в электронной форме по всем уголовным преступлениям[[18]](#footnote-18). Все процессуальные нормы должны соответствовать обязательствам и стандартам, предусмотренным в рамках международного права прав человека. В связи с этим, принимая во внимание тот факт, что в отношении киберпространства действует принцип государственного суверенитета, были сформулированы просьбы и рассмотрен вопрос о внедрении механизмов, которые могли бы обеспечить возможность законного доступа к контенту, обмен которым осуществляется с использованием средств связи со сквозным шифрованием, при одновременном обеспечении защиты основных прав и безопасности граждан[[19]](#footnote-19). Некоторые заинтересованные стороны предупредили, что такие механизмы могут ослабить безопасность интернета и подвергнуть значительным рискам мировую экономику и критически важные услуги, от которых она во многом зависит, а также жизнь граждан.

**2.9** С учетом вышеупомянутых разделов,совершенно понятно, что странам следует продолжать принимать соответствующие правовые меры по защите своих критических информационно-коммуникационных инфраструктур (и любых связанных с ними объектов, систем или их частей), которые имеют ключевое значение для поддержания жизненно важных общественных функций, таких как обеспечение здоровья, безопасности, охраны и социально-экономического благополучия людей, и по предотвращению любых сбоев в работе или повреждений, которые могут привести к значительным последствиям для этих критических инфраструктур или к нарушению их функционирования.

Руководящие указания по использованию направления 1 − Правовые меры

**2.10** Как отмечалось выше, все пять направлений ГПК взаимосвязаны между собой, при этом направление, касающееся правовых мер, является сквозным и затрагивает все остальные направления.

**2.11** C начала реализации ГПК основные усилия МСЭ были сосредоточены на тех областях кибербезопасности, которые входят в его непосредственный мандат и компетенцию, в частности на технической сфере и сфере развития, и не затрагивали вопросы применения Государствами-Членами правовых и политических принципов, связанных с национальной обороной, национальной безопасностью, контентом и киберпреступностью, на которые распространяются их суверенные права. Таким образом, деятельность МСЭ в рамках направления 1 заключается главным образом в налаживании, с использованием таких механизмов, как МоВ, сотрудничества с другими соответствующими международными организациями и заинтересованными сторонами (например, с Интерполом и УНП ООН), мандат которых в большей степени относится к этим вопросам и позволяет оказывать странам соответствующее содействие. Так, например, для помощи Государствам-Членам в понимании правовых аспектов кибербезопасности были созданы такие инструменты, как [ресурсы МСЭ по законодательству в области киберпреступности](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html) и [хранилище данных по киберпреступности УНП ООН](https://sherloc.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo). Также была проведена работа по оказанию содействия Государствам-Членам в Карибском бассейне, Африке к югу от Сахары и на островах Тихого океана в согласовании нормативных положений и законодательства в области ИКТ, в том числе нормативно-правовых баз по борьбе с киберпреступностью.

|  |
| --- |
| **2.12** 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 данном контексте ниже приводятся предлагаемые руководящие указания по использованию направления 1:  **a)** МСЭ следует продолжать усилия, направленные на содействие многосторонним обсуждениям и сотрудничеству по вопросам, связанным с решением проблемы кибербезопасности, и, в частности, на укрепление отношений с партнерами и другими заинтересованными сторонами в целях оказания помощи Государствам-Членам в этой области.  **b)** МСЭ следует продолжать сотрудничество с партнерами, в рамках своего мандата, по разработке и поддержанию ресурсов, таких как ресурсы по законодательству в области киберпреступности, в целях оказания помощи Государствам-Членам в понимании правовых аспектов кибербезопасности, а также содействовать обмену опытом и знаниями среди Государств-Членов с тем, чтобы поддержать их усилия по разработке рамочных основ, включая законодательство, в этой области.  **c)** МСЭ, в сотрудничестве с соответствующими партнерами, следует содействовать более глубокому пониманию проблем кибербезопасности и рисков, создаваемых возникающими технологиями, в контексте существующих правовых мер, и поощрять обмен исследованиями конкретных ситуаций и примерами передового опыта на национальном, региональном и международном уровнях.  **d)** Соответствующим заинтересованным сторонам также необходимо принять соответствующие правовые меры для реализации эффективных программ по предотвращению или запрещению распространения онлайновых материалов, связанных с сексуальным насилием над детьми и сексуальной эксплуатацией детей, включая принятие превентивных мер по обнаружению, пресечению деятельности и ликвидации сетей, организаций или структур, используемых для производства и/или распространения онлайновых материалов, связанных с сексуальным насилием над детьми и сексуальной эксплуатацией детей, и создать механизмы для выявления преступников и привлечения их к ответственности, а также выявления и защиты жертв. В связи с этим МСЭ следует продолжать укреплять программу защиты ребенка в онлайновой среде как платформу для работы с партнерами и заинтересованными сторонами по содействию обмену знаниями, информацией, опытом и результатами во всех аспектах, включая правовые меры, в целях облегчения и поддержки деятельности стран по решению этой острейшей проблемы. |

# Раздел 3 Направление 2: Технические и процедурные меры

Введение

**3.1** ГПК служит в качестве руководства при разработке и осуществлении различных инициатив, способствуя содержательному диалогу на международном, региональном и национальном уровнях. Потребность в эффективных и результативных мерах кибербезопасности, будь то на стратегическом или оперативном уровне, должна обеспечиваться в рамках согласованного подхода, разработка которого по-прежнему представляет собой серьезную трудность.

**3.2** Сегодня может показаться, что аспекты, определенные направлениями 1, 3, 4 и 5 ГПК, приобретают все большее значение в области виртуальной дипломатии и международного диалога и часто превалируют над направлением 2. Тем не менее технические вопросы нередко могут лежать в основе всех других направлений. Преодоление киберрисков путем применения технических и процедурных (например, административных, эксплуатационных или управленческих) мер по-прежнему является важной задачей, в особенности в контексте критических инфраструктур. С учетом своей устоявшейся роли как специализированного учреждения ООН и всемирной организации по разработке стандартов (ОРС) МСЭ располагает всеми возможностями для успешной разработки стандартов и технических мер в области безопасности.

Изменение ситуации в области технических и процедурных мер с 2008 года

**3.3** Технологии (существующие и возникающие) и основанные на них цифровые практические методы постоянно развиваются. Этот динамично меняющийся технический аспект является независимым от других направлений ГПК и развивается главным образом самостоятельно, лишь до определенной степени учитывая потребности и последствия для тематики четырех других направлений.

**3.4** Для функционирования всей инфраструктуры, приложений и услуг необходимо разработать и внедрить стандарты. Кроме того, важно, чтобы при разработке стандартов учитывались также соответствующие обязательства в области прав человека.

**3.5** МСЭ со своими членами, представляющими различные заинтересованные стороны, является уникальной глобальной площадкой для разработки глобальных стандартов в сфере ИКТ для добровольного принятия в Государствах – Членах МСЭ. Ведущей исследовательской комиссией по выработке стандартов в области безопасности внутри МСЭ является ИК17 МСЭ-Т; она опубликовала более 200 стандартов по безопасности. В настоящий момент ИК работает над различными вопросами, касающимися возникающих технологий, включая безопасность финансовых технологий, IoT (в том числе безопасность промышленного интернета)и технологий интеллектуальных транспортных систем, технологии распределенного реестра, квантовое распределение ключей, машинное обучение для борьбы со спамом, безопасность сетей 5G, периферийные вычисления, защиту информации, позволяющей установить личность, многосторонние вычисления, а также разрабатывает руководящие указания по созданию, эксплуатации и автоматизации центров киберзащиты и ряд других документов. Выполняя рекомендации, содержащиеся в Отчете HLEG 2008 года о "сотрудничестве" (например, пп. 2.1, 2.6, 2.7, 2.10, 2.12, 2.16), ИК17 пополняет и обслуживает открытую для всеобщего пользования базу данных по стандартам безопасности ИКТ[[20]](#footnote-20), насчитывающую 2600 действующих и разрабатываемых стандартов безопасности ИКТ от 13 ключевых ОРС, в том числе 3GPP, ATIS, ЕТСИ, IEEE, IETF, ОТК 1 ИСО/МЭК, МСЭ, OASIS, OneM2M и др.

**3.6** Хотя основной исследовательской комиссией по стандартам безопасности остается ИК17 МСЭ-Т, большинство других исследовательских комиссий, если не все, также работают над аспектами, связанными с безопасностью в соответствующих областях исследований, как, например, ИК20 – в области IoT и его приложений (включая "умные" города и сообщества), ИК13 – в области сетей последующих поколений или ИК16 – в области кодирования, систем и приложений мультимедиа и другие. Различные оперативные группы по возникающим технологиям, таким как ИИ для здравоохранения, машинное обучение и 5G, технологии распределенного реестра, квантовые информационные технологии для сетей и другие, также работают над решением задач, связанных с безопасностью. Большую роль играет установление тесного сотрудничества между различными группами при координирующей/ведущей роли ИК17; это позволяет поддерживать сквозную безопасность на максимально высоком уровне на протяжении всего процесса стандартизации цикла разработки продуктов/услуг ИКТ.

Распространение инициатив в области стандартизации и необходимость более широкого сотрудничества

**3.7** Международная стандартизация по вопросам кибербезопасности представляет собой непростую задачу вследствие широкого круга технологий и появления всевозможных игроков в различных секторах; с особыми трудностями сталкиваются развивающиеся страны, которые часто испытывают нехватку технических навыков и оперативных возможностей для обеспечения кибербезопасности.

**3.8** В этом отношении особую актуальность сегодня приобретает Рекомендация 2.1, содержащаяся в Отчете HLEG 2008 года: "*Что касается возможностей наращивания взаимодействия со сторонами, работающими над вопросами кибербезопасности за пределами МСЭ, Союзу следует взаимодействовать с существующими внешними центрами в целях выявления, поощрения и облегчения внедрения усовершенствованных процедур и технических мер в области обеспечения безопасности*"[[21]](#footnote-21).

**3.9** Далее, согласно Рекомендации 2.2 Отчета HLEG 2008 года, МСЭ определяется как "глобальный центр повышения квалификации"[[22]](#footnote-22) в целях продвижения международного процесса стандартизации и стандартов, связанных с техническими и процедурными мерами. Для этого необходимо стимулировать передовые в техническом отношении страны и их частный сектор к участию в деятельности МСЭ и сотрудничеству в целях разработки технических и процедурных стандартов, в том числе связанных с безопасностью.

**3.10** Важно продолжать укреплять координацию и сотрудничество с другими ОРС на основе взаимности, для того чтобы обеспечить сквозную безопасность, безопасность при проектировании, оценку рисков и совместимость на протяжении всего жизненного цикла продукта.

**3.11** В Отчете HLEG 2008 года подчеркивается важность "*ключевых мер по устранению уязвимости программных продуктов, схем, протоколов и стандартов аккредитации*"[[23]](#footnote-23). В этом плане МСЭ следует продолжать адаптировать свою работу с учетом новых технологий и потребностей. Для каждой из этих технологий/сфер необходимо учитывать следующие потребности:

• необходимость обеспечить безопасность при проектировании/по умолчанию в каждом элементе и интерфейсе разнородной экосистемы ИКТ на этапе проектирования;

• необходимость разработки адекватных параметров для определения уровня безопасности на этапе реализации;

• необходимость периодического проведения процесса (процессов) оценки и сертификации для подтверждения уровня безопасности набора данных/продукта/системы/услуги на протяжении жизненного цикла после развертывания.

Руководящие указания по использованию направления 2 – Технические и процедурные меры

|  |
| --- |
| **3.12** 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, с тем чтобы продумывать и формулировать руководящие указания по безопасности для использования соответствующих технологий и своевременно рекомендовать Государствам-Членам добровольно применять их для противодействия меняющимся и расширяющимся киберугрозам.  **b)** Следует создать механизм тесного сотрудничества между различными исследовательскими комиссиями МСЭ-Т в изучении вопросов, связанных с безопасностью, 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. Другим организациям по стандартизации и отраслевым группам предлагается представить свои стандарты по техническим и процедурным мерам МСЭ-Т для принятия в качестве Рекомендаций МСЭ-Т.  **e)** МСЭ следует продолжать свои усилия по превращению в "глобальный центр повышения квалификации" в том, что касается разработки рекомендаций по техническим и процедурным мерам обеспечения кибербезопасности в областях, входящих в его мандат (как указано в Отчете HLEG 2008 г.), посредством, в том числе, стимулирования своих членов к более активному участию в соответствующей деятельности МСЭ по стандартизации и в рамках стратегических партнерств.  **f)** МСЭ следует продолжать настоятельно рекомендовать своим Членам инициировать/заключать соглашения о взаимной сертификации в целях формирования на глобальном уровне международных систем сертификации в области кибербезопасности, основанных на согласованных стандартах. |

# Раздел 4 Направление 3: Организационные структуры

Введение

**4.1** Организационные структуры, осуществляющие координацию на национальном, региональном и международном уровнях, могут быть проанализированы на основании критерия целей, в которых они сотрудничают: стратегических либо оперативных. Организации со стратегической структурой уделяют больше внимания вопросам налаживания взаимодействия, чем вопросам проведения совместных операций в случае киберинцидента. С другой стороны, при оперативной структуре организации формируют связные системы обмена информацией для быстрого обмена в целях оперативного реагирования на киберинциденты. Проведение подобного различия может быть полезно при сопоставлении различных организационных структур по всему миру.

**4.2** Для надежной подготовки к киберугрозам и инцидентам и реагирования на них необходимы эффективные механизмы и институциональные структуры на национальном уровне. Отсутствие таких учреждений и недостаточный национальный потенциал затрудняют адекватное и эффективное реагирование на кибератаки. Решающую роль в повышении готовности и устойчивости на национальном уровне играют национальные группы реагирования на компьютерные инциденты (CIRT).

Изменение ситуации с организационными структурами с 2008 года

**4.3** В последнее десятилетие в работе по направлению 3 достигнут значительный прогресс. В целях решения проблемы кибербезопасности было учреждено множество национальных, региональных и международных организаций.

**4.4** В качестве примеров национальных и региональных инициатив можно привести AFRIPOL, AMERIPOL, GCCPOL, Центр кибербезопасности для Океании (OCSC), Австралийский центр кибербезопасности (ACSC), Европейский центр по вопросам киберпреступности (ЕС3), индийские Центр координации по вопросам киберпреступности (I4C) и Портал для направления сообщений о киберпреступлениях, японские Национальный центр по вопросам готовности к инцидентам и Центр по вопросам стратегии в области кибербезопасности и контроля киберпреступности (JC3), Национальное агентство кибербезопасности Малайзии (NACSA), Национальное агентство кибербезопасности Франции (ANSSI), Национальный центр кибербезопасности Литвы (NCSC), Международную координационную группу по вопросам киберпреступности Соединенных Штатов (IC4), Российский национальный координационный центр по компьютерным инцидентам, а также Консультационный координационный центр Организации Договора о коллективной безопасности по вопросам реагирования на компьютерные инциденты (ККЦ ОДКБ), учрежденные ОАГ Секретариат межамериканского комитета по борьбе с терроризмом (СИКТЕ) и Программу в области кибербезопасности, а также Национальное управление кибербезопасности Саудовской Аравии (NCA) и Национальное управление кибербезопасности Руанды.

**4.5** Несмотря на рост инвестиций Государств-Членов в CIRT и независимый региональный и международных охват национальных CIRT, в 85 странах национальные CIRT все еще не созданы; такая ситуация вызывает серьезную обеспокоенность, поскольку киберугрозы имеют глобальный характер[[24]](#footnote-24).

**4.6** МСЭ, действуя через свое Бюро развития электросвязи, ведет работу с Государствами-Членами, партнерами и региональными/международными организациями в целях создания потенциала на национальном и региональном уровнях, расширения возможностей и содействия созданию и усовершенствованию работы национальных CIRT. На сегодняшний день МСЭ провел более 80 оценок готовности с целью помочь странам определить степень национальной готовности в области кибербезопасности и потенциала по реагированию на инциденты[[25]](#footnote-25). МСЭ оказывает содействие в учреждении/оптимизации работы 22 национальных проектов CIRT соответствующим Государствам-Членам[[26]](#footnote-26). В целях проведения указанных оценок стран МСЭ сотрудничает с такими партнерами как Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Глобальный центр развития потенциала в области кибербезопасности и другие.

**4.7** Что касается международных организаций, то примеры некоторых реализуемых инициатив приведены в перечне здесь:

• [Глобальный центр развития потенциала в области безопасности](https://www.oxfordmartin.ox.ac.uk/cyber-security/) (GCSCC) – это международный центр исследований по вопросам эффективного и результативного создания потенциала; центр сотрудничал с МСЭ в составлении [Руководства по разработке национальной стратегии кибербезопасности (NCS)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx), которое в настоящее время используется как источник практических занятий по вопросам NCS и руководство по изучению передового опыта для стран в целях разработки эффективных национальных стратегических рамок в области кибербезопасности.

• [Глобальный форум по киберкомпетентности](https://www.thegfce.com/) (GFCE), учрежденный в 2015 году, призван обеспечивать обмен передовым опытом и предоставление экспертных знаний в области создания потенциала странам, международным организациям и частному сектору. GFCE и МСЭ являются соучредителями [инициативы "](https://cybilportal.org/projects/csirt-maturity-initiative-3/)CSIRT Maturity" и сотрудничают в разработке таких мер в области кибербезопасности как "[Комплекс инструментов по борьбе с киберпреступностью](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf)".

• [Глобальный комплекс Интерпола по инновациям](https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors) (IGCI), открытие которого состоялось в Сингапуре в 2015 году, оказывает национальным правоохранительным органам специализированную оперативную поддержку и организует для них подготовку, необходимую с учетом меняющихся реалий преступности. В 2018 году МСЭ и Интерпол подписали соглашение о сотрудничестве, предполагающее установление официальной основы их взаимовыгодного взаимодействия в рамках соответствующих мандатов и ресурсов в деле укрепления доверия и безопасности при использовании ИКТ.

• В 2018 году ВЭФ инициировал учреждение нового [Глобального центра по вопросам кибербезопасности](https://www.weforum.org/centre-for-cybersecurity/) с целью создать глобальную платформу для сотрудничества правительств, делового сообщества, экспертов и правоохранительных органов в борьбе с вызовами кибербезопасности. В том же году МСЭ и ВЭФ договорились о сотрудничестве в продвижении проектов по укреплению кибербезопасности и инициатив по смягчению киберугроз, а также о поиске дальнейших возможностей сотрудничества в целях укрепления кибербезопасности.

Руководящие указания по использованию направления 3 – Организационные структуры

|  |
| --- |
| **4.8** 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 содействие в создании национальных CIRT и других соответствующих технических подразделений/организаций.  **b)** МСЭ следует уделять первоочередное внимание странам, где еще не развернуты надлежащие организационные структуры по вопросам кибербезопасности.  **c)** МСЭ следует поощрять более открытое и всеохватное взаимодействие, а также координацию между различными национальными, региональными или международными организациями, работающими над созданием устойчивых национальных организационных структур, с тем чтобы обеспечить эффективное содействие и избежать дублирования усилий.  **d)** МСЭ следует наращивать усилия по оценке выполнения Государствами-Членами своих обязательств, применяя такие инструменты как Глобальный индекс кибербезопасности, в целях продвижения кибербезопасности как межотраслевого фактора, способствующего их усилиям в области цифровой трансформации.  **e)** Что касается национальных структур в частности, МСЭ следует оказывать Государствам-Членам содействие в принятии стратегий по выработке общегосударственных координационных механизмов для налаживания комплексного межотраслевого процесса осуществления национальных мер кибербезопасности.  **f)** 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 Направление 4: Создание потенциала

Введение

**5.1** Большое значение имеют развитие и распространение среди всех заинтересованных сторон соответствующих навыков, культуры кибербезопасности и передового опыта.

**5.2** Все страны и все организации сталкиваются с потребностью в достаточных и необходимых людских ресурсах и навыках, для того чтобы:

• осуществлять стратегические и оперативные меры кибербезопасности;

• проводить национальные оценки рисков в области кибербезопасности;

• осуществлять управление в кризисных ситуациях, связанных с возникновением инцидентов в сфере кибербезопасности;

• повышать надежность цифровых инфраструктур и услуг и способность к их восстановлению; и

• вырабатывать согласованные процессы, навыки и практические методы.

**5.3** Важно также отметить, что ввиду стремительного прогресса в области ИКТ и существующих проблем доступа и установления соединений конечные пользователи – в частности такие категории населения как женщины, дети, пожилые люди, лица с ограниченными возможностями и особыми потребностями – могут быть более уязвимы перед угрозами и инцидентами в сфере кибербезопасности. Поэтому наряду с мерами по повышению осведомленности об угрозах кибербезопасности, связанных с уязвимостью конечных пользователей, ключевое значение для снижения рисков кибербезопасности для общества в целом имеют образовательные программы по вопросам кибербезопасности.

Изменение ситуации в области создания потенциала с 2008 года

**5.4** Поскольку кибербезопасность имеет глобальное измерение и затрагивает широкий круг проблем – таких как надлежащее и ненадлежащее использование ИКТ, технические меры, экономические, правовые и политические вопросы, - важное значение для повышения уровня понимания каждого участника в цепочке обеспечения кибербезопасности имеет формирование глобальной культуры кибербезопасности. Одна из основных трудностей при формировании культуры кибербезопасности состоит в том, чтобы правильно определить, что относится к глобальным и международным проблемам, а что – к конкретным потребностям на местном уровне, поскольку культуры опираются главным образом на местные и временные факторы. Международные технические стандарты могут помочь в выявлении ключевых проблем глобального и общего характера, связанных с техническим и процедурным аспектом культуры кибербезопасности.

**5.5** Для защиты цифровой инфраструктуры большое значение имеют коллективные меры реагирования. Их актуальность возрастает, поскольку технологические изменения направлены на достижение более широкой и постоянной взаимосвязанности на основе ИКТ[[27]](#footnote-27). Все, что может быть подключено, может быть скомпрометировано. Кроме того, из-за уменьшения размеров компонентов вследствие использования нанотехнологий, включая различные виды автономных и интеллектуальных чипов, такие чипы теперь применяются в технологиях, затрагивающих все сферы нашей деятельности.

**5.6** ГПК служит инновационной и эффективной междисциплинарной базой для деятельности по созданию потенциала, с опорой на которую соответствующие участники могут продолжать разрабатывать глобальные, конкретные, поддающиеся планированию решения в целях эффективного взаимодействия. Структура ГПК хорошо зарекомендовала себя как средство поддержки выполнения задачи по построению открытого для всех и безопасного информационного общества.

**5.7** Рекомендации, содержащиеся в Отчете HLEG 2008 года по этому вопросу, сохраняют свою актуальность сегодня. С учетом проделанной МСЭ работы, в частности с момента первого издания в 2006 году [Руководства по кибербезопасности для развивающихся стран](https://www.itu.int/pub/D-STR-SECU-2006), и на основе структуры ГПК и Отчета HLEG 2008 года в Государствах-Членах ведется обширная работа по созданию потенциала, в том числе мероприятия по подготовке, повышению осведомленности, просвещению на национальном, региональном и международном уровнях.

**5.8** Используя структуру ГПК, МСЭ продолжает оказывать странам содействие, в частности в укреплении необходимого человеческого потенциала и навыков, определении национальных стратегий кибербезопасности, формировании навыков управления национальными группами реагирования на компьютерные инциденты (CIRT) и создании ресурсов для защиты детей в онлайновой среде.

**5.9** Так, например, важно отметить полезную роль [Глобального индекса кибербезопасности (GCI)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) в деятельности по повышению осведомленности. С момента своего появления в 2015 году GCI, по которому оценивается уровень выполнения Государствами-Членами их обязательств по обеспечению кибербезопасности, был трижды успешно опубликован по настоятельным просьбам Государств-Членов, частного сектора, академических организаций и других сторон. Будучи нацелен на выполнение задачи повышения осведомленности, GCI оказывает неизменное содействие Государствам-Членам в улучшении их положения в сфере кибербезопасности путем обмена передовым опытом для эффективного обеспечения кибербезопасности. Необходимо продолжать использование и усовершенствование GCI, доказавшего свою ценность как эффективный инструмент информирования и создания потенциала.

Руководящие указания по использованию направления 4 – Создание потенциала

**5.10** Для создания или усовершенствования потенциала различных заинтересованных сторон в области кибербезопасности в целях обеспечения их способности выполнять национальные и международные задачи в сфере кибербезопасности следует предпринимать конкретные шаги на национальном уровне. Поскольку деятельность по созданию потенциала осуществляется главным образом на национальном уровне, следует выделять достаточные ресурсы национальным участникам этого процесса[[28]](#footnote-28).

**5.11** Кроме того, в глобальном плане расширение возможностей людских ресурсов требует общей модульной гибкой системы подготовки по вопросам кибербезопасности для удовлетворения потребностей в повышении общественной осведомленности и выработки индивидуальной образовательной программы для конкретных специалистов. Необходимо уделять особое внимание проблеме гендерного разрыва в этой сфере. Имеется значительный незадействованный человеческий капитал, который можно привлечь к работе в сфере обеспечения кибербезопасности, в том числе женщины, которые пока составляют лишь 20% от общего числа работников этой сферы[[29]](#footnote-29).

**5.12** Качество официального образования на уровне школ или вузов и работа по повышению общественной осведомленности в целом в определенной степени зависят от качества, продуманности и актуальности исследовательской работы.

**5.13** Кроме того, важно уделять внимание вопросу создания потенциала микро-, малых и средних предприятий (ММСП), которые являются сегодня одними из ключевых игроков в условиях растущей цифровой экономики, позволяя им выявлять киберриски и управлять ими, а также использовать ресурсы ИКТ(включая широкополосную связь и интернет) безопасным и устойчивым образом.

|  |
| --- |
| **5.14** 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 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 в разработке национальных стратегий, планов, политики и механизмов реагирования на инциденты в области кибербезопасности при поддержке заинтересованных партнеров и других сообществ, занимающихся вопросами укрепления потенциала;  **d)** продолжать усилия по созданию потенциала для преодоления разрыва в стандартизации, в том числе путем оказания странам технической помощи по их просьбе.  **e)** усиливать поддержку и поощрение обмена 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;  **f)** продолжать развивать деятельность по созданию потенциала с учетом необходимости приобретения новых навыков для адаптации к требованиям безопасности возникающих технологий. Для этого необходимо развивать более тесное взаимодействие с академическими организациями, частным сектором и Государствами-Членами;  **g)** продолжать уделять особое внимание потребностям наиболее уязвимых групп населения, таких как женщины, дети, лица с ограниченными возможностями, лица с особыми потребностями и люди пожилого возраста, в рамках усилий по созданию потенциала;  **h)** продолжать развивать и укреплять применение индекса GCI в качестве инструмента для создания потенциала и повышения осведомленности;  **i)** подготовить "Руководство по разработке и внедрению образовательных программ в области кибербезопасности" в целях оказания поддержки Государствам-Членам в разработке/внедрении учебных курсов по кибербезопасности для молодежи в системах начального, среднего и высшего образования, а также профессионального обучения для взрослых, с тем чтобы обеспечить подготовку большего числа специалистов по вопросам кибербезопасности во всем мире и повысить осведомленность в области кибербезопасности во всех дисциплинах и среди всех будущих специалистов;  **j)** продолжать содействовать определению направлений научно-исследовательской деятельности, связанных с кибербезопасностью, и налаживанию диалога между различными заинтересованными сторонами, особенно в сфере возникающих технологий, используя возможности академических организаций и частного сектора, являющихся членами МСЭ, как, например, в случае с ежегодным Всемирным саммитом МСЭ "ИИ во благо";  **k)** распространять инструменты, ресурсы и передовой опыт среди Государств-Членов, отраслевых организаций и других заинтересованных сторон, чтобы поддержать их усилия, направленные на создание потенциала ММСП для решения проблем в области безопасности, а также укреплять уверенность и доверие при использовании ИКТ;  **l)** продолжать содействовать развитию культуры кибербезопасности. |

# Раздел 6 Направление 5: Международное сотрудничество

Введение

**6.1** За последнее десятилетие стало очевидным, что ни одна структура или организация не способна справиться в одиночку со всеми существующими и возникающими проблемами в области кибербезопасности. Решить эти проблемы можно только на основе партнерства, которое подразумевает тесное взаимодействие и координацию между всеми заинтересованными сторонами в целях создания общедоступной, открытой, безопасной и надежной экосистемы ИКТ.

**6.2** Направление 5, посвященное международному сотрудничеству, затрагивает все остальные направления ГПК, формируя основу для укрепления доверия, уверенности и безопасности при использовании ИКТ, какого бы аспекта это ни касалось. В Отчете HLEG 2008 года в рамках этого направления предусматривалась разработка стратегии международного сотрудничества, диалога и координации в целях противодействия киберугрозам.

Изменение условий международного сотрудничества с 2008 года

Глобальные диалоги высокого уровня

**6.3** Обсуждения по различным вопросам кибербезопасности, включая технические аспекты, киберпреступность, конфиденциальность, защиту данных и другие проблемы, ведутся в рамках целого ряда форумов и процессов. Они проводятся как под эгидой различных учреждений ООН, включая МСЭ и другие международные организации, так и по инициативе иных заинтересованных сторон, а также многие другие международные и региональные форумы.

**6.4** Все эти форумы и процессы весьма эффективны с точки зрения повышения осведомленности и улучшения понимания, однако вместе с тем важно определить возможности для синергии между этими разнообразными усилиями, чтобы международное сообщество могло объединиться и найти решения.

**6.5** Организация Объединенных Наций, обладающая огромными возможностями в плане созыва мероприятий, служит удобной площадкой для продвижения сотрудничества, диалога и координации между заинтересованными сторонами из всех государств в целях решения проблем, связанных с киберпространством, на международном уровне. Как подчеркивается в Отчете HLEG 2008 года, МСЭ, будучи специализированным учреждением системы ООН в области ИКТ, может продолжать играть важную роль в соответствующих областях в рамках своего мандата.

**6.6** В Рекомендации 1.15 Отчета HLEG 2008 года[[30]](#footnote-30) было предложено созвать "Всемирную конференцию", однако помимо этого можно было бы более эффективным образом использовать уже существующие конференции, форумы и процессы, такие как [Форум ВВУИО](https://www.itu.int/net4/wsis/forum/2020/ru) по вопросам развития и [ФУИ](https://www.intgovforum.org/multilingual/ru/) по вопросам управления, которые возникли и укреплялись в рамках процесса ВВУИО. Форум ВВУИО является крупнейшим ежегодным мероприятием сообщества ICT4D и предоставляет несколько механизмов, позволяющих собрать все мировое сообщество для обсуждения и определения конкретных шагов по решению задач развития, связанных с укреплением доверия и безопасности при использовании ИКТ (Направление деятельности C5), включая, среди прочего, работу с содействующими организациями по направлениям деятельности, диалоги высокого уровня и специальные сессии с участием заинтересованных сторон.

**6.7**Одним из наиболее знаковых событий последнего десятилетия стало признание важнейшего значения кибербезопасности национальными правительствами на высшем политическом уровне. Это нашло свое отражение в принятии многими странами стратегии цифровой трансформации, которая опирается на общегосударственный подход и предусматривает создание централизованных межотраслевых механизмов координации, которые, как правило, подчиняются напрямую главе государства или правительства.

**6.8** Еще одним важным обстоятельством в этом контексте является проведение значительного числа двусторонних переговоров между технологически развитыми странами и регионами.

Международные многосторонние партнерства

**6.9** МСЭ неоднократно доказывал свою эффективность в продвижении международного сотрудничества, выступая в роли единственной содействующей организации по Направлению деятельности C5 ВВУИО.

**6.10** МСЭ создал целый ряд многосторонних партнерств, используя:

• официальные механизмы, такие как МоВ и другие аналогичные договоренности (например, с FIRST, Интерполом, УНП ООН, ВЭФ и другими);

• такие инициативы, как "Защита ребенка в онлайновой среде", на основе партнерства[[31]](#footnote-31) с более чем 80 организациями, представляющими все группы заинтересованных сторон; и

• такие механизмы, как оперативные группы, например ОГ по технологиям цифрового реестра, квантовым технологиям, ИИ для здравоохранения и т. д., которые служат платформой для обсуждения всеми заинтересованными сторонами вопросов доверия и уверенности при использовании возникающих технологий.

**6.11** За последнее десятилетие МСЭ существенно расширил свой членский состав за счет привлечения различных заинтересованных сторон, особенно из числа частных компаний и академических организаций, и на сегодняшний день членами Союза являются 193 государства и около 900 компаний частного сектора, университетов, международных и региональных организаций, что отражает быстро меняющийся характер современного цифрового общества.

Улучшение координации внутри системы ООН

**6.12** Как упоминалось выше в пунктах 2.4 и 2.5 настоящего документа, Генеральной Ассамблей ООН создан ряд процессов, чтобы помочь решить проблемы обеспечения международной безопасности в киберпространстве. Эти процессы включают ГПЭ и РГОС. В [заключительном основном докладе РГОС](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) (2019−2021 гг.) содержался, в частности, вывод о том, что будущий регулярный институциональный диалог не должен дублировать существующие мандаты, усилия и виды деятельности ООН, ориентированные на цифровые аспекты и другие вопросы, и что любой будущий механизм регулярного институционального диалога под эгидой Организации Объединенных Наций должен представлять собой процесс, нацеленный на достижение конкретных целей и учитывающий результаты предыдущей деятельности, быть открытым, прозрачным, опираться на принципы консенсуса и достигнутые результаты. С учетом этого важно, чтобы работа МСЭ дополняла направления работы, которая в настоящее время уже ведется в этом отношении в рамках системы ООН, в частности упомянутые выше процессы ГА ООН.

**6.13** Сложная структура мандата системы ООН иногда становится препятствием для выработки прагматического и эффективного согласованного подхода. Поэтому очень важно, чтобы организации системы ООН продолжали работу по согласованию своих усилий, включая рационализацию программ и мероприятий по вопросам кибербезопасности в целях повышения их эффективности.

**6.14** Поэтому, важно стремиться к формированию в рамках ООН общего понимания нужд и потребностей, связанных с надлежащей организацией программ и инициатив, которые будут служить эффективным подспорьем для усилий, прилагаемых правительствами, отраслевыми организациями и всеми другими соответствующими заинтересованными сторонами.

**6.15** 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. 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 Координационным советом руководителей системы ООН (КСР) в ноябре 2013 года.

**6.16** Эта мера имела ключевое значение, однако, для того чтобы обеспечить эффективную координацию, необходимы дальнейшие системные изменения. Тот факт, что Генеральный секретарь ООН определил цифровое сотрудничество в качестве одного из приоритетов[[32]](#footnote-32), дает возможность заняться проблемой дальнейшего улучшения внутренней координации и сотрудничества в рамках системы ООН в целом, используя различные межучрежденческие механизмы, включая КСР.

Руководящие указания по использованию направления 5 − Международное сотрудничество

|  |
| --- |
| **6.17** Учитывая сквозной характер этого направления и многообразие форматов сотрудничества и партнерства в различных Секторах МСЭ, всем Секторам МСЭ необходимо 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 направления 5:  **a)** 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. Будучи специализированным учреждением ООН 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 в рамках своего мандата.  **b)** МСЭ следует содействовать укреплению посреднических усилий, направленных на объединение различных игроков, опираясь на процесс ВВУИО и принимая во внимание усилия Группы высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, особенно Рекомендацию 4 (глобальное обязательство по доверию и безопасности). Для этих целей могут использоваться механизмы, предусмотренные в процессах, связанных с Направлением деятельности С5, в рамках Форума ВВУИО, а также механизмы ФУИ и другие.  **c)** Следует и дальше поощрять проведение двусторонних и многосторонних обсуждений между ключевыми игроками; вместе с тем, учитывая глобальный характер киберугроз, также необходимо способствовать организации более широких дискуссий с привлечением большего числа участников, включая частный сектор и другие заинтересованные стороны. В этом отношении МСЭ также мог бы в областях, относящихся к его мандату, 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 активно взаимодействовать с другими ключевыми учреждениями системы ООН, чтобы согласовывать внутренние усилия Секретариата ООН и оптимизировать свои программы и виды деятельности в области кибербезопасности, с тем чтобы более эффективным образом служить мировому сообществу. |

# Раздел 7 Общие руководящие указания для всей структуры ГПК

|  |
| --- |
| **7.1** 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 ГПК 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 единый доступ ко всем соответствующим ресурсам.  **c)** Вся работа, которая осуществляется МСЭ в рамках ГПК, должна опираться на четкий анализ потребностей его членов, используя такие инструменты, 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 другие 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 проблемы 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. 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. 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. 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)
4. Дополнительная информация о процессе, а также о вкладах, полученных от Государств-Членов и других заинтересованных сторон, размещена по адресу: <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. WSIS Outcome Documents, 2005, размещено по адресу: [https://www.itu.int/net/wsis/outcome/booklet.pdf](https://www.itu.int/net/wsis/outcome/booklet.pdf" \o "https://www.itu.int/net/wsis/outcome/booklet.pdf). [↑](#footnote-ref-5)
6. Judge Stein Schjolberg: Report from the Chairman of HLEG, 2008, размещено по адресу: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-6)
7. Рекомендации, представленные в Отчете HLEG 2008 года, сопровождены кратким обзором обмена мнениями и обсуждений, проведенных в ходе собрания по каждой из рекомендаций. Несмотря на то, что члены HLEG не достигли полного консенсуса по всем рекомендациям, относительно многих из них большинство экспертов HLEG придерживались в целом единого мнения. [↑](#footnote-ref-7)
8. В [директиве Европейского парламента и Совета Европейского союза от 12 августа 2013 года об атаках на информационные системы, заменяющей Рамочное решение Совета (2005 г.),](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040) дается следующее определение критической инфраструктуры: *объекты, системы или их части, которые находятся на территории государств-членов и имеют ключевое значение для поддержания жизненно важных общественных функций*, *обеспечения здоровья, безопасности, охраны и экономического и социального благополучия людей и нарушение работы или уничтожение которых привело бы к значительным последствиям для государства-члена в результате сбоя в обеспечении этих функций*. [↑](#footnote-ref-8)
9. Число активных пользователей Facebook в месяц по состоянию на 4-й квартал 2019 года, см.: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. [↑](#footnote-ref-9)
10. Mark Zuckerberg: *The Internet needs new rules. Let’s start in these four areas*, Washington Post, March 30, 2019, размещено по адресу: <https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html>. [↑](#footnote-ref-10)
11. Группа правительственных экспертов, размещено по адресу: <https://www.un.org/disarmament/group-of-governmental-experts/>. [↑](#footnote-ref-11)
12. Рабочая группа открытого состава, размещено по адресу: <https://www.un.org/disarmament/open-ended-working-group/>. [↑](#footnote-ref-12)
13. Для получения более подробной информации см.:

    − Ежегодный отчет Совету МСЭ о деятельности МСЭ по укреплению доверия и безопасности при использовании ИКТ, размещен по адресу: <https://www.itu.int/en/council/2021/Pages/default.aspx>.

    − Отчет Совету 2021 года об использовании МСЭ структуры ГПК, размещен по адресу: <https://www.itu.int/md/S21-CL-C-0036/en>. [↑](#footnote-ref-13)
14. Stein Schjolberg, The History of Cybercrime (3rd Edition, February 2020). [↑](#footnote-ref-14)
15. Комиссия Европейского союза запустила программу под названием "[Горизонт-2020](https://ec.europa.eu/programmes/horizon2020/en)", направленную на развитие потенциала интернета вещей, и программу работы на 2016−2017 годы для поддержки экспериментальной и инновационной деятельности. Осуществляется сбор предложений по ряду тем, включая, в частности, безопасность и конфиденциальность IoT. Ведется поиск передовых концепций обеспечения сквозной безопасности в чрезвычайно распределенной, неоднородной и динамичной среде IoT. Подходы должны носить комплексный характер и предусматривать идентификацию и аутентификацию, защиту данных и возможности предотвращения кибератак на уровне устройства и системы. Они должны решать соответствующие проблемы безопасности и приватности, в частности проблему конфиденциальности, осведомленности пользователя о рисках, связанных с его данными, и управления такими данными, а также целостности, устойчивости и авторизации (см. решение C (2015) 6776 Европейской комиссии от 13 октября 2015 года). [↑](#footnote-ref-15)
16. T. Ballell, *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact*, Uniform Law Review, Volume 24, Issue 2, June 2019, Pages 302−314, размещено по адресу: <https://doi.org/10.1093/ulr/unz018>. [↑](#footnote-ref-16)
17. Моделью правовой основы могла бы послужить [директива 2011/92/EU Европейского парламента и Совета от 13 декабря 2011 года](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en) о борьбе с сексуальным насилием над детьми, их сексуальной эксплуатацией и детской порнографией. [↑](#footnote-ref-17)
18. Judge Stein Schjolberg, 2018 & Judge Stein Schjolberg, 2019, размещено по адресу: [https://www.cybercrimelaw.net/Cybercrimelaw.html](https://www.cybercrimelaw.net/Cybercrimelaw.html" \t "_blank" \o "https://www.cybercrimelaw.net/cybercrimelaw.html). [↑](#footnote-ref-18)
19. Например, <https://www.justice.gov/olp/lawful-access>. [↑](#footnote-ref-19)
20. ITU Standards Landscape, размещено по адресу: [https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance](https://www.itu.int/net4/ITU-T/landscape" \l "?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance). [↑](#footnote-ref-20)
21. HLEG Report 2008, Para 2.1, Page 9, id at 6. [↑](#footnote-ref-21)
22. HLEG Report 2008, Para 2.2, Page 9, id at 6. [↑](#footnote-ref-22)
23. HLEG Report 2008, Para 2, Page 9, id at 6. [↑](#footnote-ref-23)
24. National CIRTs, МСЭ, размещено по адресу: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>. [↑](#footnote-ref-24)
25. *Там же*. [↑](#footnote-ref-25)
26. *Там же*. [↑](#footnote-ref-26)
27. Tим Бернерс-Ли в своем открытом письме *"30 years on, what’s next #ForTheWeb?"* [*"30 лет спустя: какое будущее ждет Сеть?"*] от 12 марта 2019 года по случаю 30-летия основания Всемирной паутины (размещено по адресу: <https://webfoundation.org/2019/03/web-birthday-30/>) отметил, что, *"хотя Сеть создала возможности, позволила быть услышанными маргинализированным слоям населения и упростила нашу повседневную жизнь, она также создала возможности и для мошенников, позволила быть услышанными тем, кто распространяет идеологию ненависти, и упростила совершение всевозможных преступлений".*  [↑](#footnote-ref-27)
28. S. Ghernaouti, Cyberpower, Crime, Conflict and Security in Cyberspace, EPFL Press 2013. [↑](#footnote-ref-28)
29. Laurence Bradford, *Cybersecurity needs women: Here’s why*, 18 октября 2018 года, размещено по адресу:  
    <https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8>. [↑](#footnote-ref-29)
30. HLEG Report 2008, Para 1.15, Page 9, *id* at 6. [↑](#footnote-ref-30)
31. Более подробная информация размещена на адресу: <https://www.itu.int/en/cop/Pages/partners.aspx>. [↑](#footnote-ref-31)
32. Дополнительная информация размещена по адресу: <https://www.un.org/en/digital-cooperation-panel/>. [↑](#footnote-ref-32)