



Бюро развития электросвязи
(BDT)

Осн.: Циркуляр BDT/DNS/CYB/054

Женева, 27 августа 2020 года

Кому:

- Государствам – Членам МСЭ
- Членам Сектора МСЭ-D
- Академическим организациям – Членам МСЭ
- Координаторам МСЭ по вопросам глобальной кибербезопасности

Предмет: **Приглашение войти в Группу экспертов по подготовке четвертого издания Глобального индекса кибербезопасности (GCI)**

Уважаемая госпожа,
уважаемый господин,

Международный союз электросвязи (МСЭ) предлагает вам выдвинуть кандидатуру эксперта для работы над определением весовых коэффициентов для четвертого издания Глобального индекса кибербезопасности (GCI) в составе Группы экспертов.

При подготовке четвертого издания GCI МСЭ применяется многосторонний подход, в рамках которого будет задействован опыт различных структур, занимающихся вопросами кибербезопасности, нацеленный на повышение качества GCI, активизацию международного сотрудничества и поощрение обмена знаниями по этой теме.

Экспертам будет предложено представить предложения по основным составляющим GCI, в наибольшей степени связанным с областью их знания, путем присвоения весовых коэффициентов вопросам четвертого издания GCI в зависимости от значимости вопросов для принципов кибербезопасности. Пятью основными составляющими GCI являются правовые меры, технические меры, организационные меры, меры по созданию потенциала и меры в области сотрудничества. Более подробная информация представлена в прилагаемом круге ведения, а также на [веб-сайте GCI](#).

Если вы принимаете данное приглашение и выдвигаете кандидатуру эксперта, то он должен принять участие в виртуальном собрании Группы экспертов по определению весовых коэффициентов для GCI, проводимом **15 октября 2020 года**. В ходе этого собрания эксперты, которые проведут обсуждения и получают рекомендации, будут подготовлены к представлению своих предложений по весовым коэффициентам в виде электронной таблицы Microsoft Excel в срок до **31 октября 2020 года**. Предложения от всех членов Группы экспертов будут сведены в таблицу с весовыми коэффициентами, которая будет использоваться для оценки ответов стран на вопросник GCI.

Обратите внимание, что копия данного письма направлена координатору вашей страны по вопросам GCI. Будем весьма признательны за получение ответа от вас или координатора вашей страны до **30 сентября 2020 года** на адрес электронной почты: gci@itu.int.

Хотела бы выразить благодарность Государствам-Членам, Членам Сектора МСЭ-D, а также работавшим ранее группам экспертов, внесшим вклад в методическое обеспечение подготовки предыдущих изданий GCI.

Надеюсь на продолжение нашего сотрудничества.

С уважением,

(Оригинал подписан)

Дорин Богдан-Мартин
Директор

ПРИЛОЖЕНИЕ 1

Круг ведения



**Программа МСЭ/БРЭ в области
кибербезопасности**

**Группа экспертов по определению весовых
коэффициентов для GCI**

Круг ведения

Август 2020 года

GCI

Глобальный индекс кибербезопасности (GCI), впервые опубликованный в 2015 году, помогает странам определять области в сфере кибербезопасности, в которых необходимы улучшения, а также стимулирует их принимать меры по укреплению кибербезопасности, повышая таким образом общемировой уровень кибербезопасности. На основании собранной информации в Индексе выявляются практические методы, которые могут внедрить Государства-Члены и которые соответствуют их национальным условиям. Также GCI способствует распространению передового опыта и формированию глобальной культуры кибербезопасности.

Сфера охвата и структура GCI закреплены в [Резолюции 130 \(Пересм. Дубай, 2018 г.\) Полномочной конференции МСЭ](#), в которой формулируется задача усиления роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий. Вопросник GCI, из которого выводятся показатели, субпоказатели и микропоказатели, создается и утверждается путем консультаций в рамках Вопроса 3 "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности среди Членов МСЭ" 2-й Исследовательской комиссии.

Группа экспертов по определению весовых коэффициентов для GCI

Задачей Группы экспертов является определение весовых коэффициентов показателей, субпоказателей и микропоказателей GCI, а также представление предложений по внесению изменений в вопросник для будущих изданий GCI.

Члены Группы экспертов GCI назначаются для представления обстоятельных и непредвзятых рекомендаций по распределению баллов в рамках модели GCI. Рекомендации группы экспертов GCI по весовым коэффициентам показателей и субпоказателей должны отражать значимость того или иного показателя для общей приверженности Государства-Члена обеспечению кибербезопасности. В конкретные направления деятельности Группы экспертов входят:

- представление предложений по расчету основного индекса и субиндексов, как показано в Приложении В к настоящему документу; и
- представление вкладов по возможным будущим изданиям GCI.

В исключительных случаях и с согласия большинства Группа экспертов может рекомендовать пересмотр вопросов для следующего издания GCI.

МСЭ выполняет роль секретариата Группы экспертов. Участие в деятельности Группы экспертов могут принять Государства – Члены МСЭ и Члены Сектора, а также эксперты, работавшие над предыдущими изданиями GCI.

Состав Группы экспертов должен отражать гендерное и региональное разнообразие, обеспечивать представленность различных областей знания, а также в нем должен соблюдаться баланс между различными заинтересованными сторонами, включая правительственные структуры, частный сектор и академические организации.

Процесс определения весовых коэффициентов

Процесс оценки состоит из следующих шагов:

- 1 МСЭ предоставляет каждому члену Группы экспертов все соответствующие материалы, а именно:
 - а) таблицу весовых коэффициентов с вопросами GCI;
 - б) круг ведения, руководство о порядке действий и пояснения к показателям (настоящий документ).
- 2 Собрание Группы экспертов по GCI для обсуждения процесса работы и ответа на вопросы состоится **15 октября 2020 года**.

- 3 После первоначального собрания члены Группы экспертов в индивидуальном порядке заполняют электронную таблицу MS Excel со своими рекомендованными значениями весовых коэффициентов каждого показателя, субпоказателя и микропоказателя и вышлют на адрес электронной почты gci@itu.int в срок до **31 октября 2020 года**.
- 4 После того как все рекомендации будут представлены членами Группы экспертов, рекомендованные значения весовых коэффициентов будут усреднены и сведены в единую таблицу весовых коэффициентов.
- 5 Усредненные рекомендованные значения весовых коэффициентов будут разосланы членам Группы экспертов.

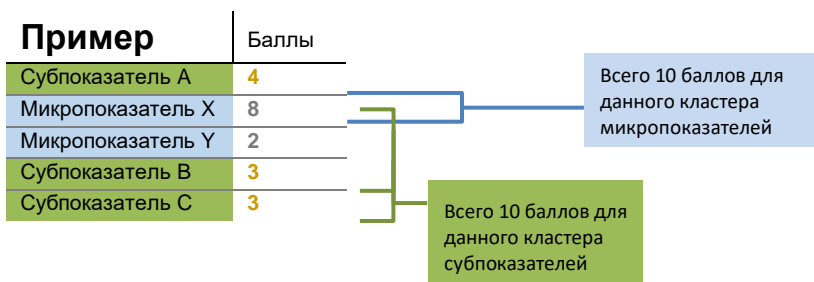
ПРИЛОЖЕНИЕ А

Как распределяются весовые коэффициенты

Следует рассматривать весовые коэффициенты только для тех основных составляющих, в отношении которых вы указали наличие экспертного знания. Весовые коэффициенты для составляющих, в отношении которых наличие такого знания указано не было, учитываться не будут.

GCI основан на иерархической модели вложений. Каждая "ветвь" модели будет далее именоваться кластером, например, "кластер показателей", "кластер субпоказателей" и "кластер микропоказателей".

В каждом кластере распределяется десять баллов. На основании своего экспертного знания вы распределяете больше баллов показателям/субпоказателям/микропоказателям, имеющим большую значимость.



Как пользоваться таблицей весовых коэффициентов

Данная инструкция касается электронной таблицы в файле *GCI-Questionnaire-weightage-calculation.xlsx*.

Этот файл предназначен для использования в среде Microsoft Excel. В других программах некоторые функции могут не работать.

Начало работы

ITU Определение весовых коэффициентов для четвертого издания Глобального индекса кибербезопасности (GCIv4) МСЭ

Фамилия респондента: Введите свою фамилию здесь ← 1

Предложения экспертов являются одним из важнейших элементов Глобального индекса кибербезопасности (GCI). Данный рабочий документ предназначен для представления участниками Группы экспертов их индивидуальной оценки надлежащих весовых коэффициентов компонентов GCIv4 (основных составляющих, показателей, субпоказателей и микропоказателей).

Укажите вашу оценку по наиболее корректным весовым коэффициентам основных составляющих, показателей, субпоказателей и микропоказателей. Вы можете распределить **10 баллов** в пределах каждой группы показателей, субпоказателей и микропоказателей.

Определения основных составляющих, показателей, субпоказателей и микропоказателей см. здесь:

[GCIv4 Definitions](#)

Если у Вас есть вопросы или замечания, свяжитесь с командой GCI по адресу электронной почты:

gci@int.itu

Обратите внимание ниже на основные составляющие, по которым вы представляете предложение. Они должны соответствовать области(ям) экспертного знания, указанной вами в вопроснике Группы экспертов.

Смотрите здесь: **Перейти к основной составляющей GCI:**

- Правовые меры
- Технические меры
- Организационные меры
- Создание потенциала
- Меры в области сотрудничества

→ 2

← 3

- 1 Введите свою фамилию
- 2 Сверьтесь с основными составляющими, в которых вы оцениваете весовые коэффициенты. Они должны соответствовать указанным вами областям экспертного знания.
- 3 Вы можете щелкнуть по значку составляющей, чтобы перейти к той, по которой вы представляете предложение.

Ввод весовых коэффициентов

ITU Определение весовых коэффициентов для четвертого издания Глобального индекса кибербезопасности МСЭ				Определения см. в GCiv4 Definitions: Legal Measures			
ПРАВОВЫЕ МЕРЫ	Вес (из 10 баллов)	Комментарии	Вес в GCiv4 в целом				
			Основная составляющая	Показатель	Субпоказатель	Микропоказатель	
1 Материальное право в области киберпреступности	7		20	14.00			
1.1 Имеется ли материальное право о несанкционированных действиях в онлайн-среде?	4				1.60		
1.1.1 Имеется ли материальное право о незаконном доступе к устройствам, компьютерным системам и данным?	3	4				1.68	
1.1.2 Имеется ли материальное право о незаконном вмешательстве (посредством ввода, изменения и удаления данных) в устройства, данные и компьютерные системы?	2					1.12	
1.1.3 Имеется ли материальное право о незаконном перехвате работы устройств, компьютерных систем и данных?	2.5					1.40	
1.1.4 Имеется ли материальное право о краже личных данных и информации в онлайн-среде?	2.5	5				1.40	
1.2 Имеются ли положения о подлоге с использованием компьютерных технологий (пиратство/нарушение авторского права)?	3				4.20		

- 4 Измените весовой коэффициент показателя, субпоказателя или микропоказателя путем ввода значения в ячейку или использования кнопок прокрутки для увеличения или уменьшения значения.

- a) В каждом кластере вы распределяете 10 баллов. Если итоговая сумма будет меньше или больше десяти, то все ячейки кластера станут красного цвета, см. ниже:

3	▲	▼
5	▲	▼
3	▲	▼

- b) Стрелки вверх и вниз изменяют значение на единицу.
- c) Для ввода дробных значений перед числом поставьте знак =. Например, =1/3 для 1/3.
- d) Если вы не желаете распределить все 10 баллов или желаете распределить больше, сделайте соответствующее указание в графе "Комментарии". Ваш весовой коэффициент будет пересчитан на основании значения в 10 баллов при выводе среднего арифметического из ответов всех экспертов.

- 5 Вы можете оставить свои замечания о весовых коэффициентах показателей, субпоказателей и микропоказателей в графе "Комментарии".
- 6 Вы можете пройти по ссылке *Определения GCiv4*, чтобы лучше понять, что означает каждый показатель.
- 7 Графа "Вес в GCI в целом" показывает значимость показателя в окончательных значениях GCI в соответствии с вашей оценкой. Редактирование или изменение этих ячеек невозможно.

Завершение работы

- 1 По завершении работы выберите вариант "сохранить как" (более подробную информацию о том, как это сделать, см. в [Руководстве службы поддержки Microsoft](#)) и добавьте Вашу фамилию в конце имени документа.

Пример: *GCI-Questionnaire-weightage-calculations-ФАМИЛИЯ.xlsx*

- 2 Прикрепите документ с таблицей к электронному письму и отправьте его на адрес: gci@itu.int до указанного срока.

ПРИЛОЖЕНИЕ В

Определения основных составляющих и показателей

Правовые меры

Правовые меры имеют решающее значение для формирования согласованной системы, чтобы различные структуры выстраивали свою деятельность в соответствии с общими правовыми и регуляторными основами, будь то по вопросам запретов конкретных деяний, преследуемых по уголовному законодательству, или по соответствию минимальным регуляторным требованиям.

Правовая среда может быть измерена на основании наличия правовых институтов и эффективных систем по проблематике кибербезопасности и киберпреступности. Она включает следующие показатели эффективности:

- **Нормы материального права в области киберпреступности**

Материальное право относится ко всем категориям публичного и частного права, включая договорное право, нормы права, относящиеся к недвижимости, гражданское право, наследственное право и уголовное право, которые, по сути, создают, определяют и регулируют соответствующие права.

- **Регуляторные положения в области кибербезопасности**

Регуляторное положение – это правило, основанное на определенной части законодательства и предназначенное для ее исполнения.

Технические меры

В отсутствие адекватных технических мер и возможностей для обнаружения инцидентов и реагирования на них Государства-Члены и их соответствующие структуры уязвимы для киберрисков, которые способны нивелировать выгоды, обусловленные использованием цифровых информационных технологий. Вследствие этого Государствам-Членам следует иметь возможность разрабатывать стратегии по внедрению общепринятых критериев минимальной безопасности и схем аккредитации для приложений и систем программного обеспечения. Технические меры могут быть оценены на основании наличия созданных или поддержанных Государством-Членом технических институтов и систем в сфере кибербезопасности. Данная подгруппа включает следующие показатели эффективности:

- **Национальные/правительственные группы реагирования на инциденты**

Группы реагирования на компьютерные инциденты, также известные как CIRT/CSIRT/CERT, являются конкретными организационными структурами, отвечающими за координацию и поддержку при реагировании на инциденты в области компьютерной безопасности или инциденты на национальном уровне.

- **Отраслевые группы CIRT/CSIRT/CERT**

Отраслевая группа CIRT|CSIRT|CERT – это организация, которая реагирует на связанные с компьютерной безопасностью или кибербезопасностью инциденты, затрагивающие ту или иную отрасль. Отраслевые CERT, как правило, создаются в важнейших отраслях, таких как здравоохранение, коммунальные услуги, экстренные службы и финансовый сектор.

- **Национальная система для применения стандартов кибербезопасности**

Первостепенное значение имеет создание государственной системы (или систем) применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственные органы) и в управлении критической инфраструктурой (даже если она эксплуатируется частным сектором). Эти стандарты, среди прочего, включают стандарты,

разработанные следующими организациями: ИСО, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.

- **Защита ребенка в онлайн-среде (COP)**

Это показатель наличия в стране национального агентства, занимающегося вопросами защиты ребенка в онлайн-среде, телефонного номера для сообщений о проблемах, связанных с пребыванием детей в онлайн-среде, а также любых технических механизмов и возможностей, используемых для защиты детей в онлайн-среде.

Организационные меры

Организационные и процедурные меры необходимы для надлежащей реализации национальных инициатив вне зависимости от их характера. Государством-Членом должна быть сформулирована общая стратегическая цель, а также план реализации, получения результатов и их анализа. Для реализации стратегии и оценки успешности или неуспешности плана необходимо создание таких структур, как национальные агентства. Организационные структуры могут быть оценены на основании наличия и количества институтов и стратегий, структурирующих разработку мер в области кибербезопасности на национальном уровне. К данной подгруппе относятся следующие показатели эффективности:

- **Национальная стратегия кибербезопасности**

Разработка политики содействия обеспечению кибербезопасности – один из высших национальных приоритетов. Национальная стратегия кибербезопасности должна определять меры по поддержанию устойчивых и надежных национальных критических информационных инфраструктур, в том числе в таких областях, как безопасность и защита граждан; защита материальных и интеллектуальных ценностей граждан, организаций и Государства-Члена; реагирование на кибератаки на критические инфраструктуры и их предотвращение; минимизация урона от кибератак и времени восстановления.

- **Ответственный орган**

К органам, ответственным за реализацию национальной стратегии/политики кибербезопасности, могут относиться постоянные комитеты, официальные рабочие группы, консультативные советы или междисциплинарные центры. Такие органы также могут быть непосредственно ответственными за работу национальных CIRT.

- **Показатели кибербезопасности**

Наличие любых официально признанных национальных или отраслевых контрольных или референтных показателей для измерения развития кибербезопасности, а также методов оценки риска, проверок кибербезопасности и других инструментов и мероприятий, направленных на измерение и оценку результатов деятельности в целях ее улучшения в будущем. Например, на основе стандарта ИСО/МЭК 27004, предназначенного для измерений, связанных с управлением информационной безопасностью.

Меры по созданию потенциала

Создание потенциала неразрывно связано с первыми тремя группами мер (правовыми, техническими и организационными). Понимание технологий, рисков и последствий может помочь в разработке более эффективного законодательства, лучших политических мер и стратегий, а также может способствовать более эффективному распределению ролей и зон ответственности. Данная область знания чаще всего рассматривается с технической точки зрения, однако множество последствий из социально-экономической и политической сфер также могут быть отнесены к ней.

Система создания потенциала в области кибербезопасности должна включать кампании по повышению осведомленности населения и наращиванию ресурсов. В данную подгруппу входят следующие показатели эффективности:

- **Кампании по повышению осведомленности населения в области кибербезопасности**

Повышение осведомленности населения предусматривает содействие проведению кампаний, охватывающих максимально возможное количество человек, а также использование НПО, учреждений, организаций, поставщиков услуг интернета, библиотек, местных торговых организаций, общественных центров, местных колледжей и программ обучения взрослых, школ и организованных родительских комитетов для распространения информации о безопасном поведении в кибер- и онлайн-пространстве.

- **Подготовка специалистов по кибербезопасности**

Наличие отраслевых программ профессиональной подготовки для повышения осведомленности широкой общественности (национальные дни, недели или месячники повышения осведомленности по кибербезопасности), содействие просвещению сотрудников различных профилей (технических, социальных профессий и т.п.) по вопросам кибербезопасности и поощрение сертификации специалистов в государственном или частном секторе.

Этот показатель также учитывает наличие утвержденной (или одобренной) правительством структуры (или структур) для сертификации и аккредитации специалистов по признанным на международном уровне стандартам кибербезопасности. В число этих сертификаций, аккредитаций и стандартов входят, помимо прочего, следующие: Cloud Security Knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²) и др.

- **Национальные учебные курсы и образовательные программы**

Открытие и поддержка национальных учебных курсов и программ, направленных на обучение молодежи навыкам и профессиям в области кибербезопасности в школах, колледжах, университетах и других образовательных учреждениях. В число профессий в области кибербезопасности входят, среди прочих, специалист по криптоанализу, специалист по экспертно-техническому анализу, специалист по реагированию на инциденты, по архитектуре безопасности, а также специалист по тестированию на проникновение.

- **Научно-исследовательские программы в области кибербезопасности**

Этот показатель используется для оценки инвестиций в национальные научно-исследовательские программы в области кибербезопасности, осуществляемые учреждениями, которые могут быть частными, государственными, академическими, неправительственными или международными. Он также служит для определения наличия признанного на общенациональном уровне учреждения, осуществляющего надзор за выполнением программы.

- **Национальная отрасль кибербезопасности**

Благоприятная экономическая, политическая и социальная среда, способствующая обеспечению кибербезопасности, стимулирует развитие частного сектора, ориентированного на обеспечение кибербезопасности. Проведение кампаний по повышению осведомленности общественности, развитие трудовых ресурсов, создание потенциала и внедрение правительственных стимулов дают толчок росту рынка продуктов и услуг в области кибербезопасности. Существование отечественной отрасли кибербезопасности является подтверждением наличия такой благоприятной среды и стимулирует рост новых компаний в области кибербезопасности и связанных с ними рынков услуг киберстрахования.

- **Механизмы стимулирования**

Этот показатель учитывает любые усилия правительства по стимулированию создания потенциала в области кибербезопасности, будь то путем предоставления налоговых льгот, грантов, финансирования, займов, реализации объектов или за счет других экономических и финансовых средств мотивации, включая признанный на национальном уровне специализированный орган, осуществляющий надзор за деятельностью по созданию потенциала в области кибербезопасности.

Меры в области сотрудничества

Для обеспечения кибербезопасности необходимо привлечение всех отраслей и областей знания, и по этой причине подход к этой задаче должен быть многосторонним. Сотрудничество укрепляет диалог и координацию, что позволяет сформировать более инклюзивное поле применения принципов кибербезопасности. Обмен информацией в лучшем случае затруднен между разными областями знаний, равно как и между участниками частного сектора. Ситуация на международном уровне еще более осложнена. В данную подгруппу включены следующие показатели эффективности:

- **Двусторонние соглашения**

Двусторонние соглашения (соглашения, заключаемые одной стороной с другой стороной) – это официально признанные национальные или отраслевые партнерства между правительством одной страны и правительством другой страны или региональной структурой, направленные на трансграничное совместное использование информации или ресурсов в области кибербезопасности (то есть сотрудничество или обмен информацией, квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами).

- **Участие в международных механизмах (форумах)**

Это может быть ратификация международных соглашений в области кибербезопасности, таких как Конвенция Африканского союза о кибербезопасности и защите личных данных, Будапештская конвенция по киберпреступности и т. д.

- **Многосторонние соглашения**

Многосторонние соглашения (соглашения, заключаемые одной стороной с несколькими сторонами) – это официально признанные национальные или отраслевые программы, в рамках которых между правительством одной страны и правительствами других стран или международными организациями осуществляется трансграничное совместное использование информации или ресурсов в области кибербезопасности (то есть сотрудничество или обмен информацией, квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами).

- **Государственно-частные партнерства**

Государственно-частные партнерства (ГЧП) – это совместные предприятия с участием государственного и частного секторов. Этот показатель эффективности служит для определения количества официально признанных национальных или отраслевых ГЧП, осуществляющих обмен информацией и активами (кадрами, процессами, инструментами) в области кибербезопасности между государственным и частным секторами (т. е. официальные партнерства в целях сотрудничества или обмена информацией, опытом, технологиями и/или ресурсами) на национальном или международном уровнях.

- **Межведомственные партнерства**

Этот показатель эффективности касается официальных партнерств между различными правительственными органами Государства-Члена (и не касается международных партнерств). Сюда могут относиться партнерства между министерствами, департаментами, программами и другими учреждениями государственного сектора, созданные в целях совместного использования информации или ресурсов.
