ITU Публикации

Международный союз электросвязи
Сектор развития

Глобальный индекс кибербезопасности

2020 год

Глобальный индекс кибербезопасности, 2020 год

Оценка выполнения обязательств по обеспечению кибербезопасности

Выражение признательности

Глобальный индекс кибербезопасности (GCI) – это инициатива Международного союза электросвязи (МСЭ), специализированного агентства ООН по ИКТ, предпринятая и развиваемая усилиями широкого круга специалистов и участников из разных стран и международных организаций. МСЭ хотел бы поблагодарить всех партнеров и участников за их напряженную работу и усилия по поддержке GCI и, что еще важнее, за помощь в углублении нашего коллективного понимания своих обязательств в области кибербезопасности.

МСЭ хотел бы особо выделить вклады, полученные от 2-й Исследовательской комиссии МСЭ-D и Консультационной группы по управлению Бюро развития электросвязи (БРЭ), а также их работу по внесению изменений в вопросник GCI. Группа по кибербезопасности БРЭ хотела бы поблагодарить членов МСЭ за выдвижение кандидатур экспертов для консультирования в процессе расчета весовых коэффициентов. Подробнее о процессе расчета весовых коэффициентов и участии экспертов можно узнать из методики. Неоценимую поддержку в определении весовых коэффициентов оказали следующие эксперты из числа членов МСЭ:

г-н Абдельазиз Альзаруни (Регуляторный орган электросвязи и цифрового управления (TDRA), Объединенные Арабские Эмираты), проф. д-р Марко Герке (Cybercrime Research Institute GmbH, Германия), г-жа Мелисса Хэтэуэй (Потомакский институт политических исследований, Соединенные Штаты Америки), г-н Скотт Джеймс Шекелфорд (Университет штата Индиана, Программа по кибербезопасности и управлению интернетом, Соединенные Штаты Америки), г-н Герик Гонсалвес (ANNSI, Бенин), инженер-консультант Эммануэль Текисо (BOCRA, Ботсвана), г-н Дламини (Министерство ИКТ, Эсватини), г-н Филлемон Йоханнес (Министерство информационно-коммуникационных технологий, Намибия), г-н Палакием АССИХ (Cyber Defense Africa S.A.S., Того), г-н Нава Дж. Саматебеле (Управление информационно-коммуникационных технологий, Замбия), г-н Гонсало Диас де Вальдес Олаварриета (Чили), г-жа Джессика Мачадо Альварес (правительство Кубы, Куба), инженер Ракель Пинья (Венесуэла), магистр наук Хакобо Белло Хойя (Национальная гвардия Секретариата безопасности и гражданской защиты, Мексика), г-н Ренцо Зегарра (Министерство транспорта и связи, Перу), г-н Джуниор Макинтайр (Карибский союз электросвязи (CTU), Тринидад и Тобаго), г-н Фернандо Эрнадес (Регуляторный орган связи, Уругвай), г-жа Анна-Рэйчел Инне (Американский реестр интернет-номеров (ARIN), Соединенные Штаты Америки), г-н Мохаммад Одех Альсаламин (Иордания), г-жа Нада Хатер (Министерство цифровой экономики и предпринимательства, Иордания), г-н Юсуф Ахмед Бухиджи (Министерство транспорта и связи, Королевство Бахрейн), г-жа Азиза Аль Рашди (Министерство транспорта, связи и информационных технологий, Оман), г-н Абдулрахман Аль-Хассан (Национальное управление кибербезопасности (NCA), Саудовская Аравия), инженер Мохаммад Алави (Министерство связи и информационных технологий, Государство Палестина), г-н Халили Урахман Кабирзой (Корневой орган сертификации Афганистана (ARCA), Афганистан), г-н Насратулла Гафури (Корневой орган сертификации Афганистана (ARCA), Афганистан), г-жа Сюй Мин (Министерство информации и информационных технологий, Группа реагирования на чрезвычайные ситуации Национальной компьютерной сети, Китай), г-жа Вань Синьсинь (Министерство информации и информационных технологий, Группа реагирования на чрезвычайные ситуации Национальной компьютерной сети, Китай), г-жа Кэтрин М. Субхьядас (Департамент связи, Фиджи), Пуан Лиана Шохаймай (Министерство связи и мультимедиа, Малайзия), Пуан Нурул Адиа Хани Хусин (Министерство связи и мультимедиа, Малайзия), г-н Ян Наунг Со (Национальный центр кибербезопасности, Департамент информационных технологий и кибербезопасности, Мьянма), г-н Джаккрапонг Чавонг (Министерство цифровой экономики и общества, Таиланд), г-н Алан Олегович Хубаев (Департамент информационной безопасности Минцифры России, Россия), г-н Андрей Сергеевич Живов (Департамент международного сотрудничества Минцифры России, Россия), г-н Ильгыз Турганбаев (Государственный комитет информационных технологий и связи Республики Кыргызстан, Республика Кыргызстан), г-н Мухамеджан Алымкулов (Государственный комитет информационных технологий и связи Республики Кыргызстан, Республика Кыргызстан), г-н Владимир Юрьевич Шурин (Департамент информационной безопасности Службы безопасности Республиканского унитарного предприятия, Беларусь), г-н Несторас Чоулиарас (Генеральный секретариат связи и почты Министерства цифрового управления, Греция), г-жа Эгле Василяускайте (Министерство национальной обороны Литовской Республики, Литва), г-н Тадас Шакунас (Министерство национальной обороны Литовской Республики, Литва), г-жа Радоя (Сербия), г-н Матей Шалмик (Национальный центр кибербезопасности SK-CERT, Словакия), г-н Растислав Янота (Национальный центр кибербезопасности SK-CERT, Словакия), г-н Эйдан Мерчленд (Соединенное Королевство), г-н Мигель Пинто (BitSight, Соединенные Штаты Америки), г-жа Нунил Пантжавати (Индонезия), г-жа Интан Рахаю (Индонезия), г-н Макайреж ДЖОНГА (Группа по компьютерной безопасности и реагированию на инциденты Гамбии (gmCSIRT), Гамбия), г-жа Банхале

Гуфу (Кения), г-жа Сонам Чоки (Департамент информационных технологий и связи, Бутан), Акил Таха Саадун (Секретариат ИКТ, Ирак) и Тхар Кадхим Али (CERTIraq, Ирак).

Группа по кибербезопасности МСЭ хотела бы поблагодарить координаторов GCI, собравших данные по деятельности своих стран в сфере обеспечения кибербезопасности. Подготовка данного отчета была бы невозможна без усилий координаторов GCI по отдельным странам.

Группа признательна многим коллегам и стажерам из МСЭ, помогавшим подготовить этот отчет.

Группа приносит свои извинения любым лицам и организациям, непреднамеренно не включенным в этот список, и выражает благодарность всем, кто внес свой вклад в создание GCI.

С любыми комментариями и вопросами в отношении этой публикации просьба обращаться в группу кибербезопасности МСЭ по адресу gci@itu.int.

Правовая оговорка

ISBN

978-92-61-33924-1 (электронная версия)
978-92-61-33934-0 (версия EPUB)
978-92-61-33944-9 (версия Mobi)

Предисловие

Потребность в безопасном и надежном киберпространстве стала важной как никогда, особенно с учетом того, что все мы все больше зависим от жизненно важных цифровых коммуникаций. Одна из величайших проблем, вызванных пандемией COVID-19, – найти способы конструктивного взаимодействия друг с другом, несмотря на неопределенность, тревогу и перемены. Еще до пандемии обеспечение кибербезопасности стало необходимым условием гарантии безопасности в онлайновой среде, позволяющей нам решать свои важные повседневные задачи.

Меня воодушевляет способность людей адаптироваться к этой неопределенной среде и использовать информационные технологии для поиска творческих решений. Многие организации, включая Международный союз электросвязи, столкнулись с новыми проблемами, обусловленными необходимостью удаленной работы. Кибербезопасность неразрывно связана с удаленной работой – от управления вызовами между участниками видеосвязи до обеспечения безопасного обмена документами. Поэтому МСЭ продолжает сотрудничать со странами, чтобы все эффективнее и активнее оказывать влияние в тех областях, где в нас нуждаются больше всего.

Когда в 2015 году впервые вышел Глобальный индекс кибербезопасности, мало кто мог представить себе ситуацию, в которой мы находимся сегодня. Это последнее издание Глобального индекса кибербезопасности поможет в осуществлении дальнейших шагов по обеспечению безопасности цифровых экосистем, необходимых для восстановления и роста, путем измерения обязательств в области кибербезопасности, взятых на себя отдельными странами, и их приоритетности.

Это издание показывает, что многие страны добиваются прогресса в решении своих задач по реагированию на вызовы кибербезопасности вопреки недобросовестным субъектам, которые пользуются нашей потребностью в информации, нашими опасениями по поводу пандемии, переходом к работе из дома и дистанционному обучению, зависимостью от систем здравоохранения и т. п.

Глобальный индекс кибербезопасности показывает, что многие страны приняли новые законы и правила в сфере кибербезопасности, касающиеся таких вопросов, как неприкосновенность частной жизни, несанкционированный доступ и безопасность в онлайновой среде. Он также подчеркивает необходимость разработки стратегий и механизмов для развития потенциала и оказания помощи правительствам и предприятиям в подготовке к инцидентам кибербезопасности и смягчению растущих киберрисков. Сегодня более чем в половине стран мира имеются группы реагирования на компьютерные инциденты (CIRT), и почти две трети стран разработали ту или иную национальную стратегию кибербезопасности, определяющую общую ситуацию в области обеспечения кибербезопасности в этих странах.

Глобальный индекс кибербезопасности наглядно демонстрирует, что на самом деле кибербезопасность является проблемой развития и что существует острая потребность в устранении растущего разрыва в киберпотенциале между развитыми и развивающимися странами путем расширения знаний, повышения квалификации и развития компетенций. Нам необходимо восполнить этот пробел, обратившись к его первопричинам и создав потенциал цифровой инфраструктуры, цифровых навыков и ресурсов в развивающемся мире.

Я надеюсь, что Глобальный индекс кибербезопасности будет оставаться полезным инструментом развития потенциала для органов государственной власти и политических деятелей, специалистов по кибербезопасности и научных работников, который поможет им выявлять области, где требуются

усовершенствования, и освещать примеры передового опыта по укреплению национальной кибербезопасности.

Я хотела бы поблагодарить страны за их участие и ценный вклад в эти усилия, особенно за участие в процессе разработки, сбора данных и проверки этого издания Индекса. Я также хотела бы поблагодарить всех, кто участвует в работе исследовательской комиссии, за их поддержку и целеустремленность. Предлагаю всем Государствам – Членам МСЭ и дальше информировать нас о ходе работы по связанным с кибербезопасностью обязательствам, чтобы мы могли на деле совместно использовать опыт, исследования и решения для создания надежного киберпространства для всех.

Дорин Богдан-Мартин
Директор Бюро развития электросвязи МСЭ

Резюме

Глобальный индекс кибербезопасности (GCI) был впервые издан Международным союзом электросвязи (МСЭ) в 2015 году для оценки степени выполнения 193 Государствами – Членами МСЭ и Государством Палестина[1] обязательств по обеспечению кибербезопасности, с тем чтобы помочь им определить направления совершенствования и побудить к конкретным действиям, повышая их осведомленность о ситуации в сфере кибербезопасности во всем мире. По мере нарастания рисков, определения приоритетных направлений и развития ресурсов обеспечения кибербезопасности GCI также адаптировался, с тем чтобы дать более точную картину принимаемых странами мер по укреплению кибербезопасности.

Настоящий отчет направлен на улучшение понимания обязательств стран в отношении кибербезопасности, выявление пробелов, поощрение внедрения передового опыта и предоставление странам полезной информации для укрепления их позиций в области кибербезопасности.

Страны сообщили об использовании ими GCI для содействия:

- дискуссиям на официально учрежденных форумах, позволяющим проводить самооценку и улучшать координацию;
- сбору информации об общих национальных инициативах и ресурсах, используемых для управления кибербезопасностью на национальном уровне;
- сравнительному анализу примеров передового опыта партнеров и соседей по региону;
- повышению осведомленности различных заинтересованных сторон о потребности в координации на национальном уровне.

Итоговые показатели GCI демонстрируют общее улучшение и укрепление позиций по всем пяти компонентам программы кибербезопасности, однако пробелы в сфере кибербезопасности на региональном уровне все еще сохраняются. В отчете приведены наглядные примеры практических мер, принимаемых в отдельных странах.

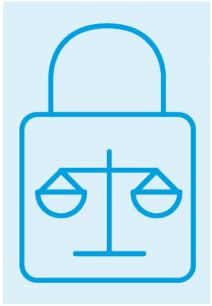
Количество оцениваемых стран	Год сбора данных	Количество координаторов по странам	Количество разосланных вопросников	Среднее повышение общей оценки с 2018 года
194	**2020**	**169**	**150**	**9,5%**

Индекс отражает 82 вопроса об обязательствах Государств-Членов в области кибербезопасности по пяти основным компонентам:

- правовые меры;
- технические меры;
- организационные меры;
- меры по развитию потенциала;
- меры в области сотрудничества.

[1] Государство Палестина участвовало в работе МСЭ в соответствии с Резолюцией 99 (Пересм. Дубай, 2018 г.) Полномочной конференции.

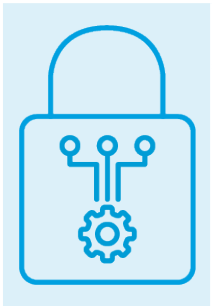
В нижеследующей таблице приведены глобальные обязательства по конкретным показателям для каждого компонента.



Правовые меры

Количественная оценка законов и постановлений по киберпреступности и кибербезопасности

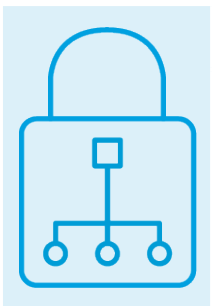
167	стран имеют законодательство о кибербезопасности в той или иной форме
133	постановления в отношении защиты данных
97	постановлений в отношении критически важной инфраструктуры



Технические меры

Количественная оценка реализации технических возможностей силами государственных и отраслевых организаций

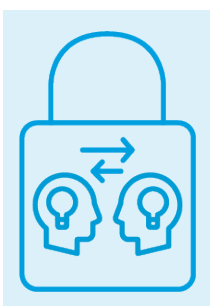
131	активная CIRT
104	участника региональных CIRT
101	механизм информирования в области защиты ребенка в онлайновой среде



Организационные меры

Количественная оценка национальных стратегий и организаций, реализующих меры по обеспечению кибербезопасности

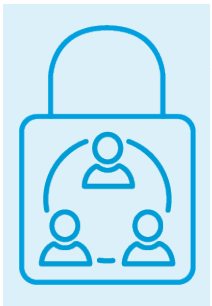
127	национальных стратегий кибербезопасности
136	агентств по кибербезопасности
86	сообщений о стратегиях и инициативах в области защиты ребенка в онлайновой среде



Развитие потенциала

Количественная оценка информационных кампаний, профессиональной подготовки, образования и стимулирования развития потенциала в области кибербезопасности

142	страны реализуют инициативы по повышению осведомленности в области кибербезопасности
94	страны имеют программы НИОКР в области кибербезопасности
98	стран сообщили о наличии национальной индустрии кибербезопасности



Сотрудничество

Количественная оценка партнерских отношений между учреждениями, фирмами и странами

166	стран участвуют в государственно-частном партнерстве в сфере кибербезопасности
90	стран имеют двусторонние соглашения в области кибербезопасности
112	стран участвуют в многосторонних соглашениях в области кибербезопасности

Изменения в Глобальном индексе кибербезопасности, влияющие на оценки

- Настоящее издание Глобального индекса кибербезопасности основано на данных, представленных рекордным количеством участвующих Государств-Членов: для издания 2013–2014 годов поступило 105 ответов, а в 2020 году было возвращено 150 заполненных вопросников.
- Содержание вопросника GCI было обновлено. Были переопределены, добавлены или исключены вопросы по каждому из пяти компонентов (правовые, технические, организационные меры, развитие потенциала и сотрудничество) в соответствии с изменившимися угрозами и прилагаемыми усилиями в области кибербезопасности. Изменения в вопроснике оказали влияние на результаты, поскольку эти изменения – один из факторов, влияющих на оценки и рейтинги стран.
- Весовые коэффициенты изменились по сравнению с предыдущими изданиями, что частично связано с изменениями в структуре вопросов, а также с добавлением и исключением вопросов.
- Весовые коэффициенты показателей основаны на рекомендациях экспертов. Члены МСЭ выдвинули кандидатуры экспертов, которые в процессе расчета весовых коэффициентов рекомендовали назначать их показателям, исходя из относительной важности этих показателей для обеспечения кибербезопасности. Различия в распределении весовых коэффициентов могут повлиять на оценки и рейтинги стран.
- Подготовлен раздел с дополнительной информацией по построению, составу и последним изменениям в вопроснике GCI (Приложение A).
- Оценки многих стран, особенно стран с лучшими показателями, все более сближаются, так что индивидуальные рейтинги следует интерпретировать с осторожностью.
- Некоторые страны отказались от проверки собранных данных или от участия в этом издании Глобального индекса кибербезопасности. Данные по этим странам (отмеченные знаком *) не следует рассматривать как официально подтвержденные каким-либо представителем страны. Поскольку данные собирались посредством онлайн-опроса, отсутствующие элементы следует интерпретировать не как несуществующие, а как неполученные.

Кроме того, в некоторых случаях участие страны могло положительно повлиять на оценки, поскольку чем больше вклад страны в вопросник, тем вероятнее утвердительные ответы.

Существует много таких областей, в которых отдельные страны преуспевают, и таких, в которых у них сохраняются возможности для дальнейшего наращивания усилий, так что не следует уделять чрезмерное внимание рейтингам стран.

По странам, не представившим ответы на вопросник, было проведено кабинетное исследование с использованием общедоступной информации на официальных сайтах и других ресурсах. Собранные данные по странам, для которых проводилось кабинетное исследование, могут неточно отражать положение в области кибербезопасности в этих странах. GCI не содержит оценочных данных.

Содержание

Перечень таблиц и рисунков

Таблицы

Рисунки

1 Глобальный индекс кибербезопасности – справочная информация и контекст

Четвертое издание Глобального индекса кибербезопасности (GCI) вышло совсем в другой обстановке, нежели предшествующие выпуски. В 2007 году, когда стартовала Глобальная программа кибербезопасности, оставался еще месяц до выпуска первого смартфона iPhone, а Facebook всего год назад был открыт для пользователей за стенами университетов Соединенных Штатов. Число пользователей сети составляло миллиард человек, и высказывались опасения, что объем созданных данных, 255 эксабайтов, превысит доступную емкость хранилищ[1]. Сегодня смартфоны изменили повседневную жизнь, а социальные сети обеспечили более широкий охват общества. К сети подключено 3,5 миллиарда пользователей, объем цифрового мира оценивается в 44 зеттабайта, а риск переполнения хранилища данных исключен благодаря облачным вычислениям[2]. Кроме того, распространение ИКТ затронуло более широкую национальную экосистему, открыв новые организационные возможности, такие как услуги электронного правительства, а также путь к новым экономическим и производственным парадигмам, таким как Индустрия 4.0 и расширенная цифровая экономика.

Цифровой разрыв в той или иной степени затрагивает все страны, и кибербезопасность – как ключевой фактор, способствующий развитию экономики, общества и государственного управления, которые полагаются на цифровые системы, – следует считать вопросом первостепенной важности.

Пандемия COVID-19 в значительной степени повлияла на жизнь общества. В апреле 2020 года, когда она началась, компания Akamai отметила, что интернет-трафик вырос на 30%[3]. Информационные технологии играют ключевую роль в поддержании связи между людьми – от обеспечения дистанционного присутствия до дистанционного обучения. Ключевым условием того, что цифровая эпоха сможет реализовать свой потенциал, является надежное и безопасное киберпространство. Спустя год после того как Всемирная организация здравоохранения объявила COVID-19 пандемией, а также в результате разработки новых систем управления и вакцинации наша зависимость от цифровых технологий продолжает расти. И по мере того как во всем мире обеспечивается подключение тех, кто не подключен, необходимо гарантировать безопасность и надежность киберпространства.

Отмечается все более широкое признание рисков в области кибербезопасности[4]. Продолжающаяся пандемия породила недоверие, особенно в онлайновой среде. Данные, собранные в GCI – это начало более широкого разговора о кибербезопасности, в ходе которого решающее значение для определения направлений дальнейшей деятельности будут иметь местный контекст и наблюдения.

GCI может стать отправной точкой для понимания того, как пандемия повлияла на усилия в области кибербезопасности и как страны работают над решением задачи обеспечения кибербезопасности и укрепления доверия, чтобы создать надежное и безопасное киберпространство после пандемии. В частности, некоторые страны сообщили о задержке принятия и ввода в действие законов, внедрения или совершенствования CIRT, разработки или пересмотра национальных стратегий кибербезопасности и осуществления усилий по развитию потенциала. Даже заключение соглашений о сотрудничестве тормозится из-за отсутствия личного общения и взаимодействия.

Мир продолжает меняться, и органам государственной власти следует проанализировать, какие существуют политические рычаги и практические методы повышения кибербезопасности. По мере развития и адаптации этих методов меняется и способ измерения кибербезопасности. В GCI обновлены вопросы о роли CIRT, соглашениях о сотрудничестве, организационной структуре и осведомленности общественности. Хотя эти изменения делают GCI в меньшей степени сопоставимым с прошлыми изданиями, новое издание точнее отражает текущие обязательства стран.

---

1 http://core.xsomo.com.jm/images/web/File/white%20papaers/Expanding_DigitalUniverse_IDC_WhitePaper_022507.pdf
2 https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/
3 https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html
4 http://reports.weforum.org/global-risks-report-2020/executive-summary/

2 Ключевые темы

2.1 Правовые меры: планирование будущих инициатив

Сегодня многие проблемы подрывают доверие к сети и не позволяют цифровому обществу полноценно функционировать. Например, убытки от киберпреступности во всем мире, по оценкам, вырастут с 1 трлн. долл. США в 2020 году[5] до 6 трлн. долл. США в 2021 году[6]. Насущным требованием является разработка нормативно-правовой базы для защиты общества и содействия созданию безопасной и надежной цифровой среды, что должно предшествовать любым национальным усилиям в области обеспечения кибербезопасности.

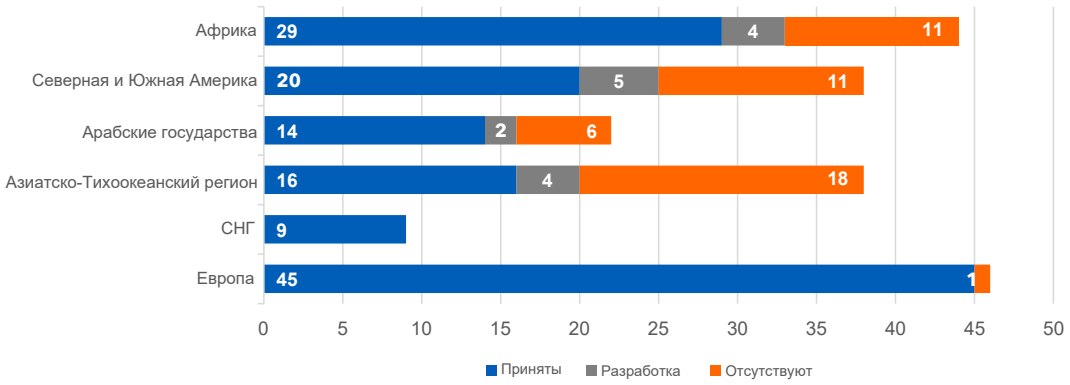
Нормативно-правовая база предусматривает принятие регламентарных положений, устанавливающих, в чем именно заключается незаконная деятельность в киберпространстве, а также определяющих необходимые процедурные инструменты расследования, судебного преследования и обеспечения соблюдения таких регламентарных положений; введение базовых показателей кибербезопасности и механизмов их соблюдения для ряда национальных заинтересованных сторон; а также установление процедур, обеспечивающих соблюдение международных обязательств.

Четвертое издание Глобального индекса кибербезопасности подводит итоги принятых мер в области кибербезопасности в рамках законодательной базы страны путем измерения наличия:

- основных требований, которые должны соблюдать заинтересованные стороны из государственного и частного секторов;
- правовых инструментов, запрещающих противоправные действия.

Защита данных

Рисунок 1. Страны, имеющие законодательные положения в области защиты данных



Источник: МСЭ

Законодательство в области защиты данных может принимать форму нормативного положения, которое, в частности, вынуждает организацию раскрывать факты нарушения кибербезопасности или устанавливает требования по проведению ежегодных проверок.

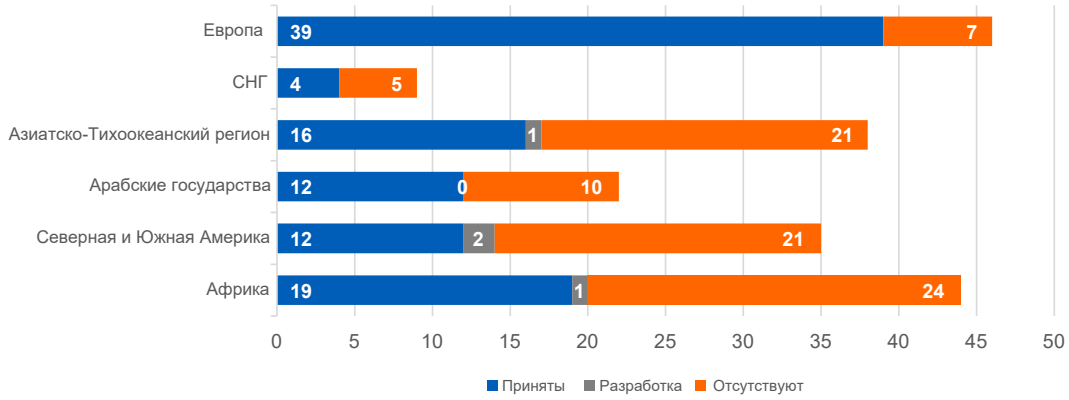
На первый взгляд сторонники неприкосновенности частной жизни могут заметить, что значительное число стран, в которых уже действуют нормативные положения в области защиты данных и неприкосновенности конфиденциальной информации, поработали над их обновлением. При этом 133 страны приняли нормативные положения о защите и неприкосновенности конфиденциальной информации, 15 стран находятся в процессе их разработки, а в 46 странах такие нормативные

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[6] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

положения отсутствуют. Многие страны, имеющие такие нормативные положения, внесли в них изменения, отражающие новые соглашения и нормы.

Со времени последнего издания Индекса многие страны ввели меры, требующие направления уведомления о нарушениях. В этом издании 102 страны ввели в свои законодательные положения и правила требования относительно уведомлений об утечке данных и инцидентах.

Рисунок 2. Страны, в которых введены меры, предусматривающие уведомление о нарушениях



Источник: МСЭ

Кража идентичности и данных в онлайновой среде

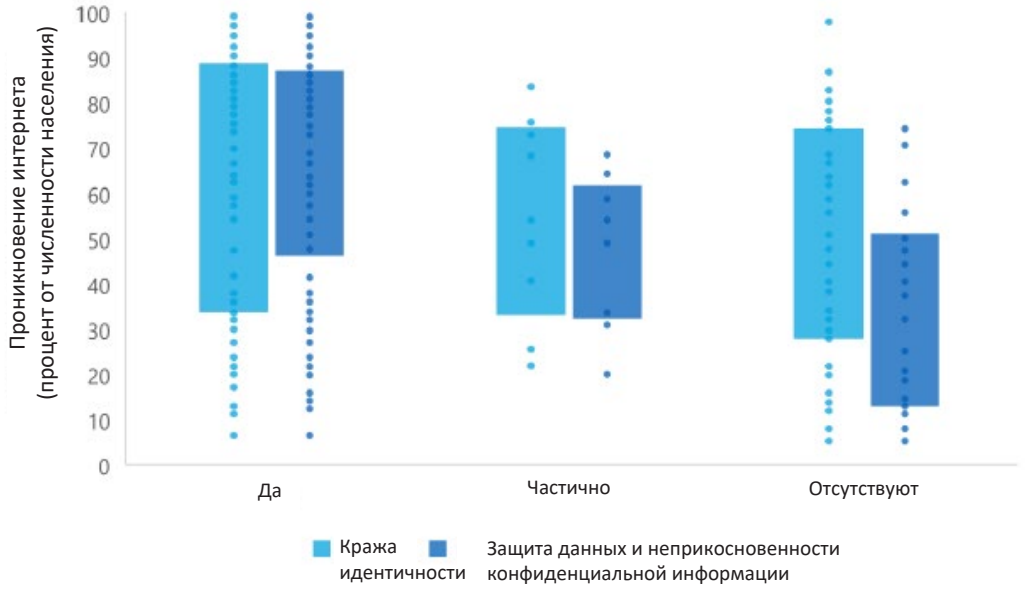
Несмотря на то что страны принимают меры по борьбе с незаконным доступом, законодательным положениям в отношении хищения персональных данных в онлайновой среде по-прежнему не уделяется должного внимания, хотя защита онлайновой идентичности имеет большое значение – особенно с учетом нынешнего перемещения в цифровую среду. Благодаря социальным сетям и новым методам работы мировое население перемещается в онлайновую среду, а следовательно, требуется надежная защита, поскольку кража идентичности может поставить под угрозу всю повседневную жизнь человека как в частном, так и в профессиональном плане.

Рисунок 3. Страны, имеющие законодательные положения в отношении хищения персональных данных

Источник: МСЭ

Как видно из рисунка 4, при рассмотрении медианного и среднего проникновения интернета оказывается, что в странах с высоким уровнем проникновения интернета с несколько большей долей вероятности можно говорить о существовании законов или постановлений о защите данных в онлайновой среде, чем в странах с низким уровнем проникновения интернета. И наоборот, нормативные положения о защите данных и неприкосновенности конфиденциальной информации более распространены в странах с высоким уровнем проникновения интернета. Эти тенденции отчасти отражают экономические условия, общее развитие и стратегии в области цифрового управления. Примечательно, что некоторые страны подготовились к более широкому проникновению интернета, заблаговременно приняв законодательные положения в отношении кражи идентичности и защиты данных и неприкосновенности конфиденциальной информации.

Рисунок 4. Законодательные положения в отношении кражи идентичности и защиты данных и неприкосновенности конфиденциальной информации, наложенные на доступность интернета (процент населения)



Источник: База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Как показано на рисунке 5, в большинстве стран приняты нормативные положения в отношении противозаконного доступа при малосущественных различиях между регионами.

Рисунок 5. Нормативные положения в отношении противозаконного доступа

Источник: База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Асоциальное поведение в онлайновой среде

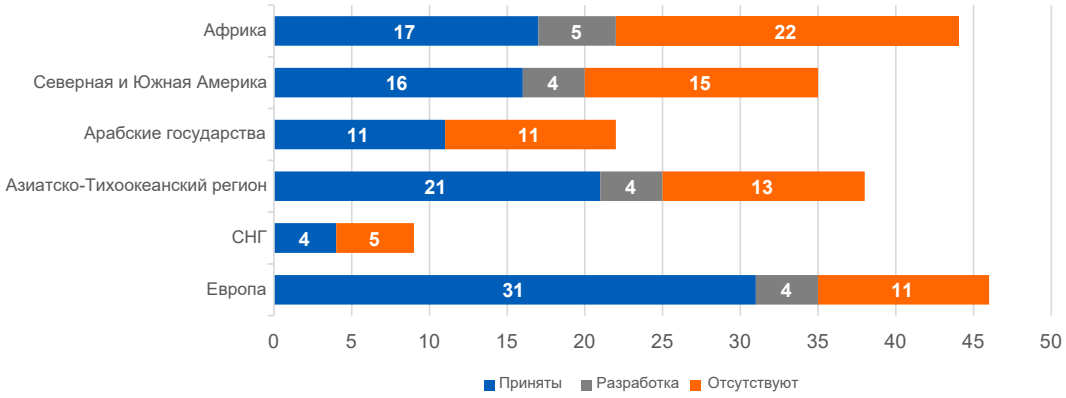
Асоциальное поведение в онлайновой среде – это насущная проблема, для решения которой страны принимают все более строгие правовые меры. GCI измеряет два аспекта – онлайновые домогательства и расизм/ксенофобию в онлайновой среде.

Домогательство в онлайновой среде остается постоянной проблемой: в Соединенных Штатах Америки в 2020 году "41% американцев испытали на себе ту или иную форму онлайнового домогательства"[7], а

[7] https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

в Европейском союзе онлайновым домогательствам подвергалась по крайней мере каждая десятая женщина[8]. В ходе опроса взрослых жителей 32 стран каждый пятый сообщил, что сталкивался с агрессивными высказываниями в онлайновой среде[9].

Рисунок 6. Страны, имеющие законодательные положения в отношении домогательств в онлайновой среде



Источник: База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Во всем мире 100 стран приняли законодательные положения, устанавливающие уголовную ответственность за домогательства и злоупотребления в онлайновой среде, в 17 странах они находится в стадии разработки и ввода в действие, а в 77 странах такие регламентарные положения отсутствуют. Однако зачастую не дается четкого определения того, какие действия являются злоупотреблениями.

На препятствия, связанные с нечеткостью определения, наталкиваются усилия по борьбе с расизмом и ксенофобией в онлайновой среде, однако разработкой таких законодательных положений в той или иной форме занимается значительное число стран. Некоторые страны расширяют или адаптируют к онлайновому контексту общие законы о расизме и ксенофобии. Критерии в отношении того, какие действия квалифицируются как правонарушение, в значительной мере различаются: то, что считается законным в одной стране, может быть отнесено к наказуемым правонарушениям в другой. Однако некоторые страны решили принять специальные положения о расистском поведении в онлайновой среде.

2.2 Технические меры: расширенное развертывание групп CIRT/CERT

Для уверенной борьбы с киберугрозами и киберинцидентами необходимы эффективные механизмы и институциональные структуры на национальном уровне. Группы реагирования на компьютерные инциденты (CIRT) или группы реагирования на нарушения компьютерной защиты (CERT) позволяют реагировать на инциденты на национальном уровне с использованием централизованного диспетчерского пункта и способствуют оперативным и систематическим действиям, предоставляя странам возможность накапливать опыт и повышать устойчивость средств кибербезопасности.

Национальные CIRT, как правило, создаются и действуют в соответствии с законодательством или государственной политикой. CIRT могут входить в состав государственного учреждения или действовать под эгидой определенного министерства или другой структуры. Ряд стран, которым не хватает времени, знаний или ресурсов для создания национальной CIRT, поручают это третьей стороне.

[8] https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf

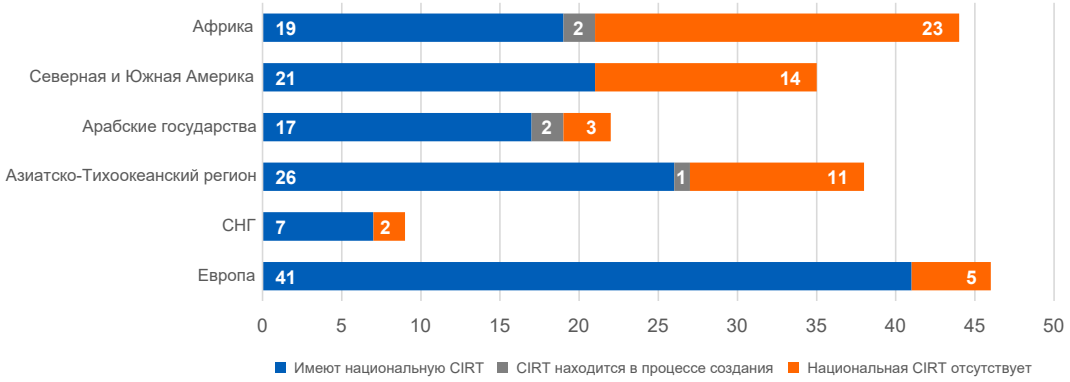
[9] https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1

Создаются новые CIRT

По состоянию на конец 2020 года национальные CIRT созданы в 131 стране, включая 10 новых CIRT, которые начали действовать уже после издания Глобального индекса кибербезопасности 2018 года. В настоящее время в стадии создания находятся еще четыре национальные CIRT.

Хотя многие страны добились прогресса в деле создания CIRT, некоторые, особенно наименее развитые страны (НРС), сталкиваются со значительными трудностями. Нехватка ресурсов и технических знаний, отсутствие экосистемы кибербезопасности, исследований и разработок, установленных приоритетов и политической воли могут помешать усилиям по решению проблем кибербезопасности с применением технических мер.

Рисунок 7. Количество стран, имеющих национальные CIRT



Источник: МСЭ

Несмотря на то что Африканский регион не является лидером в технической сфере, с момента публикации Глобального индекса кибербезопасности 2018 года в нем появилось шесть новых CIRT, так что количество стран, имеющих национальные CIRT, увеличилось с 13 до 19. В регионе Северной и Южной Америки 21 страна имеет национальные CIRT, а в регионе арабских государств – 17 стран. Не имеют национальных CIRT всего 2 страны в регионе СНГ и 6 стран в Европейском регионе.

GCI также отслеживает деятельность CIRT. Из 131 имеющейся CIRT 11 участвуют во всех нижеперечисленных видах деятельности:

- содействие повышению осведомленности в области кибербезопасности и защите ребенка в онлайновой среде посредством консультаций, рекомендаций, руководств, учебных курсов и видеопособий;
- предоставление рекомендаций по кибербезопасности для ИТ-специалистов;
- проведение учений по кибербезопасности в течение последних двух лет;
- взаимодействие с региональными CIRT и FIRST[10];
- сертифицирована Trusted Introducer[11] или имеет другой признанный сертификат.

В то время как национальные CIRT решают проблемы на национальном уровне, отраслевые CIRT удовлетворяют потребности в обеспечении кибербезопасности конкретной отрасли, такой как здравоохранение, транспорт, связь или коммунальные услуги. CIRT других типов обслуживают транснациональные или крупные компании, частные университеты и т. п.; в данном отчете GCI такие CIRT не отслеживаются.

[10] www.first.org
[11] www.trusted-introducer.org/

Рисунок 8. Количество отраслевых CIRT

Источник: МСЭ

Как видно из рисунка 8, в двух третях стран отраслевые CIRT отсутствуют. Из 76 стран, имеющих отраслевые CIRT, в 37 они организуют информационные кампании, учения по кибербезопасности и публично или конфиденциально обмениваются информацией об инцидентах и угрозах со своим сообществом.

2.3 Организационные меры: стратегия согласования

Организационные меры позволяют странам, которые занимаются вопросами кибербезопасности, исследовать механизмы управления и координации. К организационным мерам относятся обеспечение устойчивости системы кибербезопасности на высшем уровне исполнительной власти и распределение соответствующих ролей и обязанностей между различными национальными структурами, а также возложение на них ответственности за состояние национальной кибербезопасности.

Организационные меры принимаются не во всех странах с мощной инфраструктурой электросвязи. Сравнение Индекса телекоммуникационной инфраструктуры, рассматриваемого в публикации "Исследование ООН: Электронное правительство 2020. Цифровое правительство в десятилетии действий по достижению устойчивого развития" и входящего в состав Индекса готовности к внедрению электронного правительства[12], с общими оценками организационных мер показывает, что, хотя эта тенденция пока слабо выражена, в настоящее время многие страны для решения проблем кибербезопасности принимают меры, относящиеся к инфраструктуре электросвязи, но не организационные меры.

Отсутствие адекватных организационных мер может стать одной из причин отсутствия четкого определения обязанностей и сферы подотчетности в сфере управления национальной кибербезопасностью и препятствовать эффективной внутриправительственной и межотраслевой координации.

Важность современных национальных стратегий

Краеугольным камнем организационных мер по обеспечению кибербезопасности на национальном уровне часто служит национальная стратегия кибербезопасности (НСК). Согласно Инструкции МСЭ по разработке национальной стратегии кибербезопасности, НСК – это всеобъемлющая структура или стратегия, которую необходимо разработать, реализовать и соблюдать на основе многостороннего подхода, обеспечивающего согласованные действия государственных органов, частного сектора и

[12] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

гражданского общества по предотвращению инцидентов, подготовке к ним, а также по реагированию и восстановлению[13].

Все больше стран разрабатывают НСК для более структурированного управления обеспечением кибербезопасности. НСК может обеспечить ряд преимуществ, в том числе в отношении привлечения заинтересованных сторон, прояснения национальных приоритетов и планирования развития потенциала в области кибербезопасности.

По мере развития Глобального индекса кибербезопасности в нем все больше внимания уделяется странам, регулярно обновляющим свои НСК, чтобы адаптировать их к меняющимся реалиям. Действительно, создание НСК – это первый позитивный шаг страны к обеспечению кибербезопасности, но ее необходимо регулярно пересматривать в соответствии с меняющимися угрозами и приоритетами. Обычно страны придерживаются 4–5-летнего временного интервала обновления НСК. Некоторые страны выбрали более длительный период, составляющий десятилетие и более.

Из 127 стран, имеющих национальную стратегию кибербезопасности (введена ли она в действие только что, действует более пяти лет или находится в стадии разработки), 60 стран продемонстрировали прогресс в установлении более четких целей путем пересмотра и разработки новых стратегий кибербезопасности или обновления своих планов действий.

Защита критически важной инфраструктуры/национальный план обеспечения устойчивости

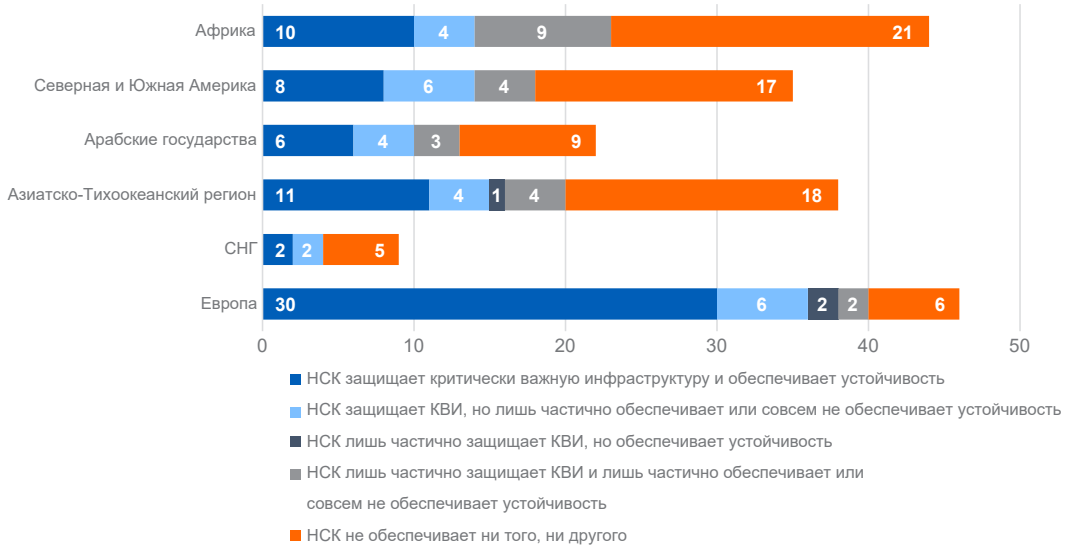
Один из важных аспектов разработки национальной стратегии кибербезопасности – наличие четкого набора целей по защите критически важной инфраструктуры. Постоянную проблему для стран составляет обеспечение непрерывности операций на национальном уровне. Остается подверженной угрозам кибербезопасности критически важная инфраструктура, такая как электросети, водоочистные сооружения и транспортные системы. Потенциальные последствия инцидента, связанного с критически важной инфраструктурой, разрушительны, и стратегия должна привлекать больше внимания к усилиям по управлению рисками, направленным на снижение вероятности и предотвращение эскалации события, приводящего к серьезным последствиям.

Ожидается, что за ближайший год расходы на обеспечение кибербезопасности критически важной инфраструктуры вырастут до 9 млрд. долл. США и в 2021 году достигнут 105,99 млрд. долл. США[14]. Поскольку сотрудники объектов критически важной инфраструктуры, подобно работникам, занятым во многих других отраслях, перешли на условия работы с соблюдением социальной дистанции, им необходимо сбалансировать увеличившуюся поверхность атаки. Аналитическая фирма ABI Research отмечает, что инвестиции в кибербезопасность в значительной мере зависят от региона, сектора экономики и возможностей установления соединений: наибольшие расходы приходятся на оборону, финансовые услуги и ИКТ, а в промышленных секторах они меньше[15].

---

13 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx
14 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/
15 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/

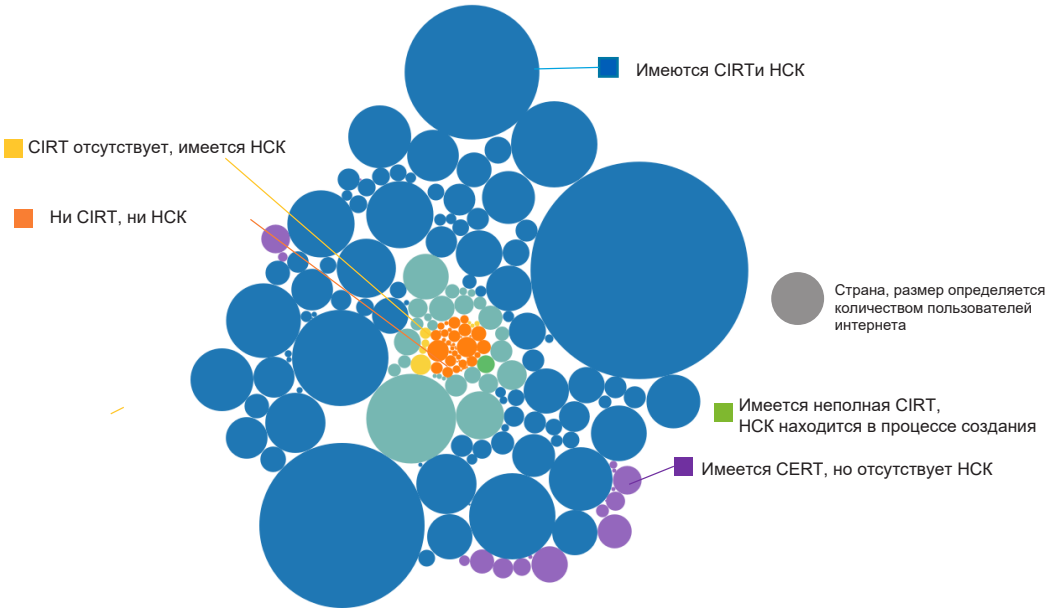
Рисунок 9. Страны, уделяющие внимание вопросам защиты критически важной инфраструктуры и обеспечению устойчивости



Источник: МСЭ

Уделение приоритетного внимания кибербезопасности как составной части критически важной инфраструктуры и устойчивости отражается не только в бюджетных обязательствах, но и в национальных стратегиях кибербезопасности. Национальные стратегии чаще охватывают вопросы защиты критически важной инфраструктуры и/или обеспечения устойчивости кибербезопасности. Однако многие страны не занимаются ни тем ни другим.

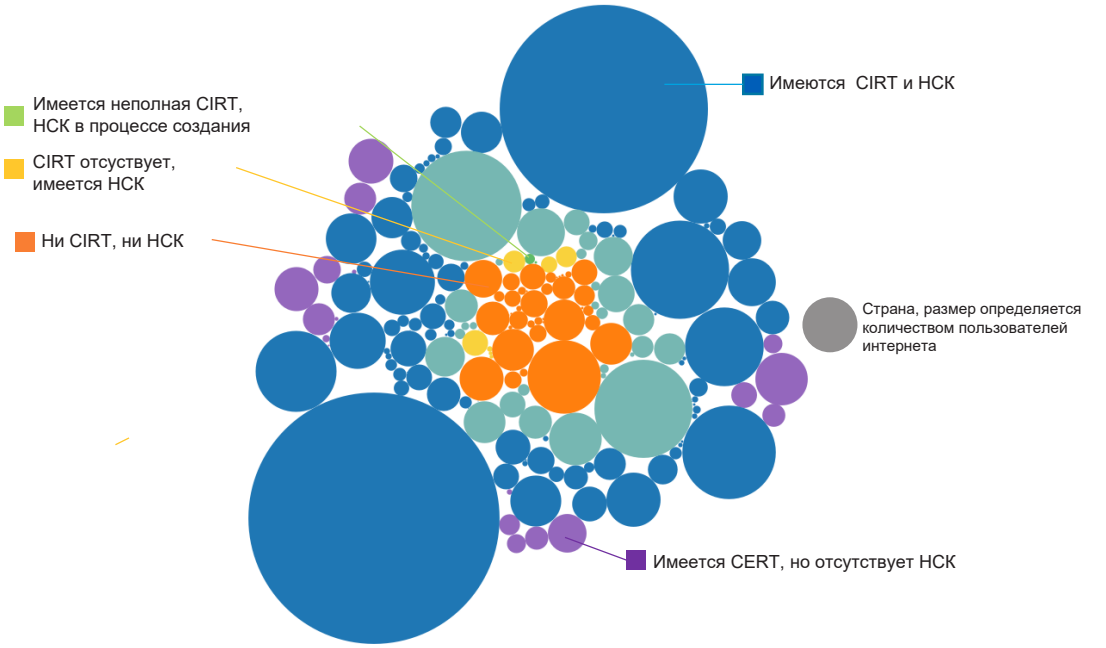
Рисунок 10. Количество интернет-пользователей (по охвату CIRT и национальной стратегией кибербезопасности)



Источник: Глобальный индекс кибербезопасности, База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Если сравнить все страны мира по количеству пользователей интернета, то оказывается, что более 95% пользователей интернета проживают в странах, где имеются национальная стратегия кибербезопасности и национальная CIRT.

Рисунок 11. Численность населения, лишенного возможности установления соединений (по охвату CIRT и национальной стратегией кибербезопасности)



Источник: Глобальный индекс кибербезопасности, База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Однако в менее соединенных странах НСК и/или национальная CIRT нередко отсутствуют. 9% населения, лишенного возможности установления соединений, проживает в странах, не имеющих национальной CIRT или национальной стратегии кибербезопасности, и еще 15% – в странах без НСК, но имеющих национальную CIRT. Более половины наименее развитых стран не имеют CIRT, а 60% не имеют национальной стратегии кибербезопасности или еще не приступили к ее разработке.

Таблица 1. Количество стран, имеющих НСК и CIRT

	Имеют НСК	НСК находится в процессе создания или разработана более 5 лет назад	НСК отсутствует
Национальная CIRT имеется	90 стран	29	18
Национальная CIRT отсутствует	7	1	49

Источник: МСЭ

Страны, не имеющие национальной стратегии кибербезопасности, реже имеют CIRT. Неудивительно, что из 63 стран, не имеющих CIRT, и 67 стран, не имеющих НСК, 49 стран не имеют ни CIRT, ни НСК.

Рисунок 12. Оценка жизненного цикла в рамках НСК

Источник: МСЭ

Национальная стратегия кибербезопасности – первый позитивный шаг к обеспечению кибербезопасности, но она нуждается в регулярном обновлении и пересмотре. Многие страны, имеющие НСК, не пересматривают и не корректируют их на регулярной основе, чтобы привести их в соответствие с изменяющимися угрозами и приоритетами в области кибербезопасности. Из 98 стран, имеющих актуальную НСК, только 60 проводят оценку жизненного цикла в рамках своей стратегии.

Рисунок 13. Проверки кибербезопасности на национальном уровне

Источник: МСЭ

Национальные проверки кибербезопасности (рисунок 13) более распространены, чем оценки жизненного цикла. Частота проведения этих проверок в рамках данного издания GCI не оценивалась.

Рисунок 14. Показатели для оценки рисков, связанных с киберпространством, на национальном уровне

Источник: МСЭ

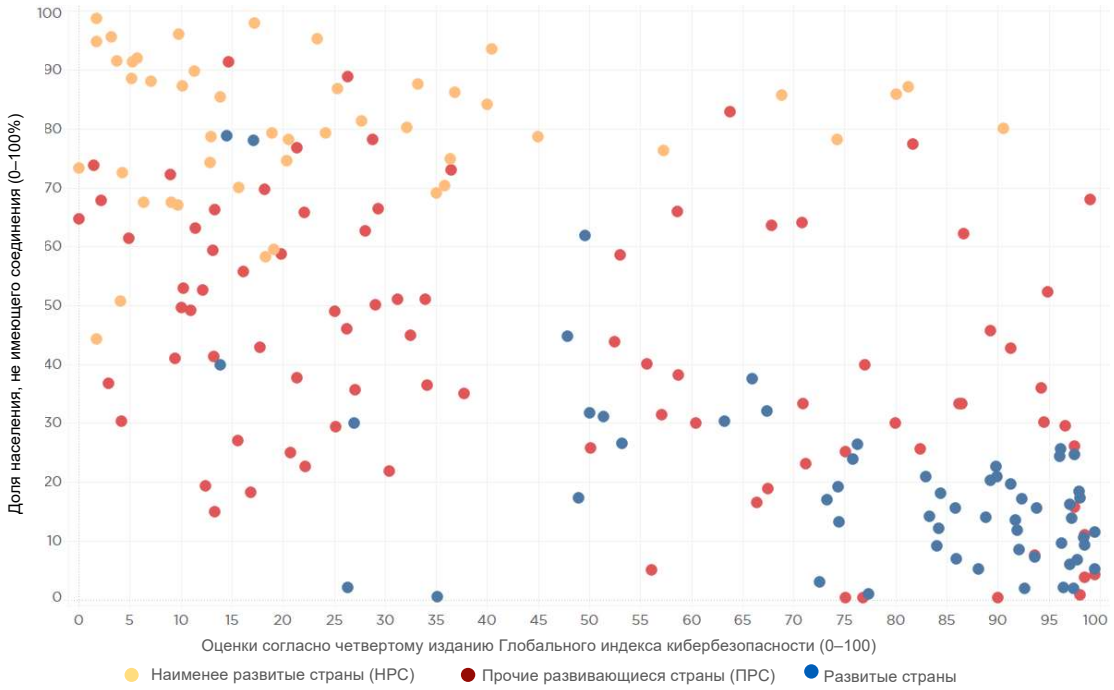
Аналогичным образом в большинстве стран отсутствуют показатели для оценки рисков, связанных с киберпространством, на национальном уровне. Отсутствие таких показателей может затруднить этим странам оценку текущих рисков, определение приоритетности мер, принимаемых в области кибербезопасности, и отслеживание достигнутого прогресса.

2.4 Меры по развитию потенциала: создание потенциала в области кибербезопасности

По оценкам Всемирного экономического форума, "каждый день около миллиона человек впервые выходят в интернет, и две трети мирового населения имеют мобильные устройства"[16]. Хотя применение цифровых технологий приносит огромные экономические и социальные выгоды, киберриски могут нивелировать эти выгоды от цифровизации. Защита киберпространства с помощью мер по развитию потенциала в области кибербезопасности является ключевым моментом, поскольку способствует решению таких проблем, как цифровой разрыв и киберриски.

[16] https://reports.weforum.org/global-risks-report-2020/executive-summary/

Рисунок 15. Глобальный индекс кибербезопасности и доля населения, не имеющего соединения



Источник: Глобальный индекс кибербезопасности, База данных МСЭ по всемирным показателям в области электросвязи/ИКТ

Как видно из рисунка 15, страны с худшими оценками в Глобальном индексе кибербезопасности чаще всего являются наименее развитыми странами и имеют большую долю населения, не имеющего соединения. По мере того как все больше людей получают возможность установления соединений, этим странам требуется поддержка по развитию потенциала в области кибербезопасности, чтобы эффективнее реагировать на угрозы. Однако многие страны, особенно НРС, при попытке сократить отставание в киберпотенциале сталкиваются с проблемами нехватки ресурсов, включая, среди прочего, отсутствие институциональных знаний, политические ограничения и дефицит навыков в области защиты своих систем ИКТ, как физических, так и виртуальных.

Среди наименее развитых стран резко выделяются показатели нескольких стран, таких как Бангладеш, Бенин, Руанда и Танзания, которые продемонстрировали твердую приверженность выполнению обязательств в области кибербезопасности. Примечательно, что все эти страны сообщили о наличии национальной отрасли кибербезопасности, что является ключевым признаком принятия мер по развитию потенциала.

Рисунок 16. Цели в области устойчивого развития (8, 9, 10)

Источник: ООН (https://sdgs.un.org/goals)

В целях обеспечения достойной работы и экономического роста, создания устойчивой инфраструктуры, содействия всеохватной и устойчивой индустриализации и стимулирования инноваций, а также сокращения неравенства внутри стран и между странами необходимо развивать потенциал кибербезопасности для активизации процессов, закрепления навыков и наращивания объема ресурсов, исследований и разработок, направленных на укрепление национального потенциала. Потенциал кибербезопасности также способствует развитию коллективных возможностей и

содействует международному сотрудничеству и партнерству в целях эффективного реагирования на вызовы цифровой безопасности, связанные с киберпространством.

Инструменты и меры по развитию потенциала могут способствовать управлению рисками, связанными с кибербезопасностью, защите граждан, инфраструктуры и предприятий, а также созданию более широких киберсообществ.

Повышение осведомленности общественности по вопросам кибербезопасности

Эффективное повышение осведомленности по вопросам кибербезопасности имеет важное значение для поддержания бдительности граждан, предприятий, органов государственной власти, молодежи и организаций. В связи с текущим переходом на цифровые услуги органы государственной власти должны позаботиться о том, чтобы все пользователи были осведомлены о рисках, с которыми они могут столкнуться в ходе осуществления деятельности в цифровой среде.

При сопоставлении кампаний по информированию общественности в области кибербезопасности с уровнем проникновения интернета все страны делятся на четыре основные группы:

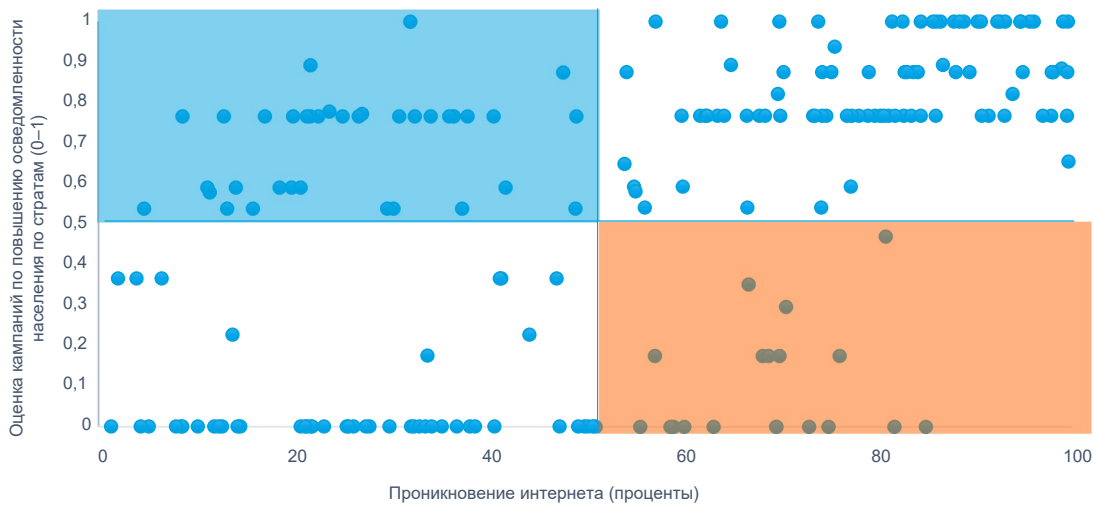
1 низкий уровень проникновения интернета/содействие повышению осведомленности по вопросам кибербезопасности (синий прямоугольник на рисунке 17): эти страны обладают более широкими возможностями для подключения тех, кто не подключен, и распространения знаний, необходимых в онлайновой среде;

2 низкий уровень проникновения интернета/отсутствие поддержки деятельности в области повышения осведомленности по вопросам кибербезопасности: эти страны еще не обеспечили возможность подключения тех, кто не подключен, и не распространяют информационные ресурсы в области кибербезопасности;

3 высокий уровень проникновения интернета/содействие повышению осведомленности по вопросам кибербезопасности: в этих странах имеется возможность установления цифровых соединений, и они участвуют в деятельности, направленной на повышение осведомленности по вопросам кибербезопасности, способствуя безопасному поведению в онлайновой среде;

4 высокий уровень проникновения интернета/отсутствие поддержки деятельности в области повышения осведомленности по вопросам кибербезопасности (оранжевый прямоугольник на рисунке 17): в этих странах имеется возможность установления цифровых соединений, но их население может быть не осведомлено о киберрисках.

Рисунок 17. Оценка кампаний по повышению осведомленности населения в области кибербезопасности (по странам в зависимости от проникновения интернета)



Источник: МСЭ

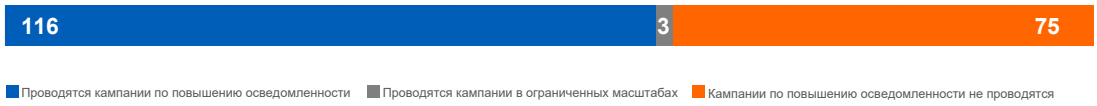
Кампании по информированию лиц с ограниченными возможностями здоровья и пожилых людей

В то время как интернет и цифровой мир открывают беспрецедентные возможности для всех, при принятии решений и выборе технологий лица с ограниченными возможностями здоровья и пожилые люди чаще всего не учитываются. По некоторым оценкам, по состоянию на 2021 год в мире насчитывается 752 миллиона человек в возрасте 65 лет и старше[17]. Если сравнить эту цифру с количеством стран, в которых проводятся информационные кампании, ориентированные на лиц с ограниченными возможностями здоровья и пожилых людей, то результат оказывается чрезвычайно скромным. Лишь 18% из 194 стран занимались повышением осведомленности лиц с ограниченными возможностями здоровья и 25% проводили кампании, ориентированные на пожилых людей. Малое количество стран, занимающихся повышением осведомленности среди этих двух конкретных групп населения, вызывает тревогу, поскольку это обусловливает значительный цифровой разрыв, так как лицам с ограниченными возможностями здоровья и пожилым людям приходится пользоваться цифровыми услугами, такими как приложения для отслеживания контактов в условиях пандемии COVID-19.

Уделение более пристального внимания повышению осведомленности в области кибербезопасности малых и средних предприятий (МСП), предприятий частного сектора и государственных учреждений

Во время пандемии COVID-19 наблюдается дальнейший рост объема деловых операций, осуществляемых в онлайновом формате, в связи с чем предъявляются повышенные требования к практическим методам обеспечения кибербезопасности на предприятиях частного сектора. МСП зачастую являются наиболее распространенной формой бизнеса в стране – в странах с формирующейся экономикой на их долю приходится 90% всех предприятий, 50% трудовых ресурсов, а вклад зарегистрированных МСП в ВВП достигает 40%[18]. При этом МСП нередко наименее подготовлены к решению проблем кибербезопасности. Поэтому необходимы мероприятия по повышению осведомленности МСП по вопросам кибербезопасности.

Рисунок 18. Количество стран, в которых проводятся кампании по повышению осведомленности в области кибербезопасности, ориентированные на МСП, предприятия частного сектора и государственные учреждения



Источник: МСЭ

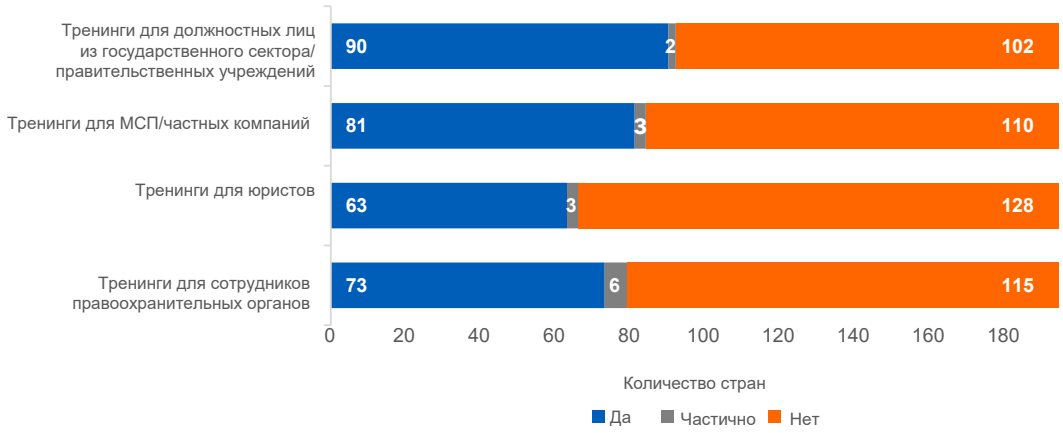
Результаты GCI показывают, что около 60% стран проводят или проводили в течение последних двух лет кампании по повышению осведомленности в области кибербезопасности среди МСП, предприятий частного сектора или государственных учреждений, тогда как 38% не сообщили о проведении каких-либо кампаний, относящихся к кибербезопасности. Они ограничиваются информированием целевой аудитории об основах безопасности в онлайновой среде и кибербезопасности, предоставляя соответствующие ресурсы, например через национальные CIRT, или предлагая инструменты для защиты сетей. 2% стран находятся на ранней стадии организации кампаний, ориентированных на МСП, предприятия частного сектора и государственные учреждения.

17 https://population.un.org/wpp/DataQuery/
18 https://www.worldbank.org/en/topic/smefinance

Правительства признают необходимость отраслевых образовательных программ и тренингов для специалистов по кибербезопасности

Все более важное значение приобретает реализация учебных программ, направленных на удовлетворение потребностей различных отраслей. Эксперты по кибербезопасности прогнозируют, что к 2021 году от 3,5[19] до 4 миллионов[20] вакансий в сфере кибербезопасности во всем мире останутся незаполненными. Несмотря на этот прогнозируемый пробел, значительному числу стран еще только предстоит разработать учебные программы для конкретных отраслей, а более 50% стран не имеют учебных программ, ориентированных на конкретные отрасли или профессии, в частности на сотрудников правоохранительных органов, юристов, работников МСП и компаний частного сектора, а также государственных служащих.

Рисунок 19. Количество стран, реализующих специальные учебные программы/тренинги для специалистов по кибербезопасности



Источник: МСЭ

Как видно из рисунка 19, 46% стран (90) сообщили, что они реализуют отраслевые учебные программы по вопросам кибербезопасности для государственных служащих и должностных лиц правительственных учреждений, 41% стран (81) организуют курсы повышения квалификации по вопросам кибербезопасности для ИТ-специалистов, в том числе из МСП и предприятий частного сектора, 37% стран (73) – для сотрудников правоохранительных органов, а 32% стран (63) заботятся о том, чтобы сотрудники судебных и правоохранительных органов не остались в стороне при реализации мер по обеспечению устойчивости и безопасности.

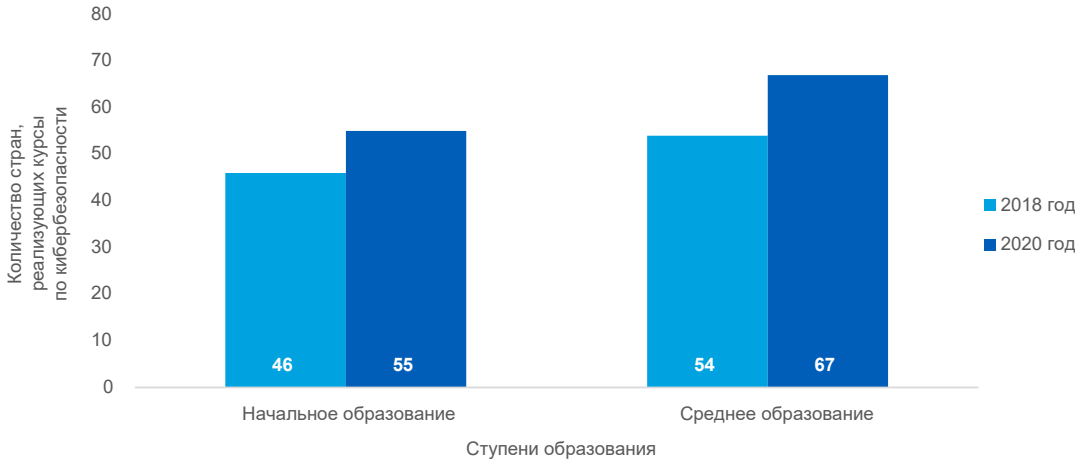
Страны сообщили, что они реализуют такие учебные программы в области кибербезопасности через свои национальные CIRT, национальные центры кибербезопасности, а также в рамках утвержденных или одобренных правительством курсов подготовки, проводимых другими региональными и международными организациями. Некоторые страны, которые стремятся увеличить число специалистов по кибербезопасности, но не в состоянии обеспечить обучение на национальном уровне, одобрили международные учебные программы, проводимые органами сертификации по кибербезопасности, такими как SANS[21], ISC2, ICSPA[22], ISACA[23] и др.

19 https://cybersecurityventures.com/jobs/
20 ESG Research Report: 2019 Digital Work Survey (esg-global.com).
21 https://www.sans.org/
22 https://icspa.org/about-us/
23 https://www.isaca.org/

Все более распространенными становятся учебные курсы по кибербезопасности для учреждений начального и среднего образования

Поскольку страны перешли на онлайн-обучение, курсы по безопасности в онлайновой среде и кибербезопасности проводятся не только в высших учебных заведениях, но и в начальной и средней школе.

Рисунок 20. Количество стран, включивших курсы по кибербезопасности в национальные учебные программы (по ступеням образования)



Источник: МСЭ

Как видно из рисунка 20, после издания Глобального индекса кибербезопасности 2018 года возросло количество стран, включивших курсы по кибербезопасности в национальные образовательные программы. На 5%, с 46 до 55, увеличилось количество стран, включивших в программу начального образования вводный курс по обеспечению безопасности ребенка в онлайновой среде, и на 7%, с 54 до 67, – количество стран, включивших в программу средней школы ресурсы для учащихся, интересующихся обеспечением кибербезопасности как специальностью, чтобы начать изучение этого предмета в раннем возрасте.

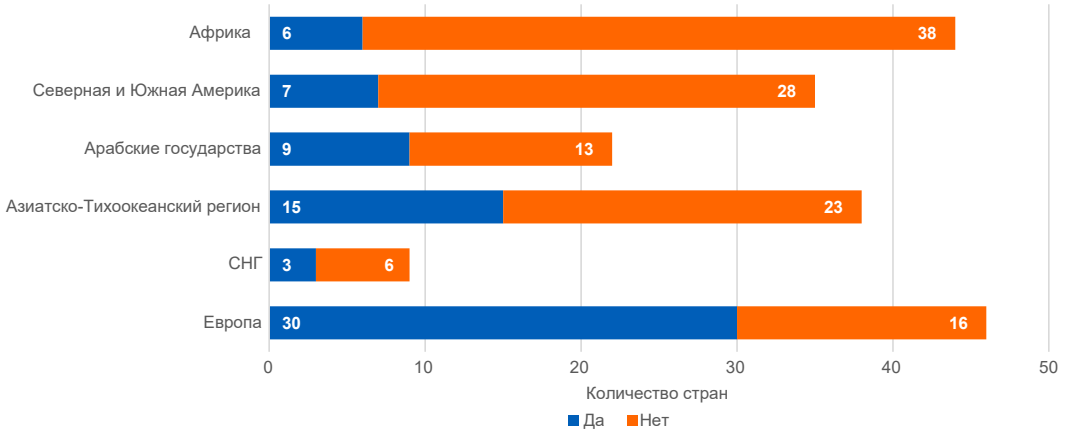
Государственные стимулы развития кибербезопасности отстают

Стимулирование обеспечения кибербезопасности на национальном уровне должно сопровождаться пропагандированием культуры кибербезопасности, содействующей изменению отношения руководителей предприятий к кибербезопасности, что позволит рассматривать ее не только как задачу, относящуюся к информационным технологиям, а перейти к более целостному мировоззрению, в рамках которого оценивается роль кибербезопасности в общем повышении производительности труда и рентабельности предприятия. Повышение приоритетности кибербезопасности в организациях – это процесс, требующий наличия инфраструктуры и механизмов, способствующих обеспечению кибербезопасности. Страны, стимулирующие развитие кибербезопасности на предприятиях частного сектора и поощряющие развитие компаний, специализирующихся на кибербезопасности, отличаются тем, что они вводят в свою структуру кибербезопасности поощряющие стимулы.

Страны могут способствовать обеспечению кибербезопасности на предприятиях частного сектора с помощью таких механизмов стимулирования, как налоговые льготы, основанные на параметрах кибербезопасности, налоговые каникулы или включение стандартов кибербезопасности в условия контрактов. Это должно стимулировать предприятия частного сектора уделять приоритетное внимание вопросам кибербезопасности в рамках производственных структур и процессов, что в свою очередь улучшит положение страны в области кибербезопасности в краткосрочной, среднесрочной и долгосрочной перспективах.

Однако данное издание GCI показывает, что 124 страны не указали никаких стимулов к обеспечению кибербезопасности, что означает необходимость принятия таких стимулов Государствами-Членами для ускоренного внедрения мер кибербезопасности.

Рисунок 21. Количество стран, в которых действует механизм стимулирования развития потенциала в области кибербезопасности



Источник: МСЭ

2.5 Меры в области сотрудничества: коллективные действия по обеспечению кибербезопасности

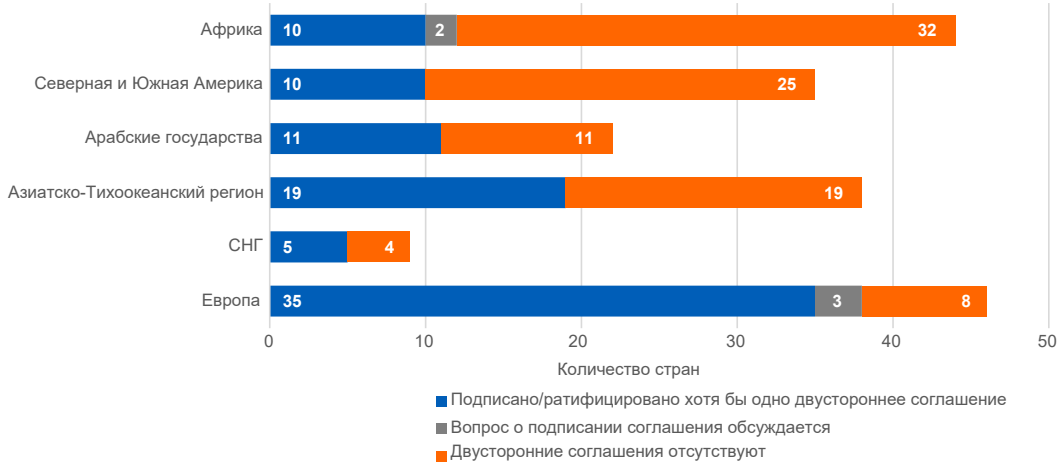
Риски кибербезопасности приобретают все более трансграничный характер[24], и сотрудничество по-прежнему является важным инструментом решения задач по обеспечению кибербезопасности. Из-за усиливающейся взаимозависимости и растущего количества взаимосвязанных инфраструктур обеспечение кибербезопасности представляет собой транснациональную задачу. Безопасность глобальной кибернетической экосистемы не может гарантировать или обеспечивать какая-либо одна заинтересованная сторона, и для расширения охвата и усиления воздействия требуется сотрудничество на национальном, региональном и международном уровнях. По этому направлению сотрудничества в вопроснике определяются страны, подписавшие двусторонние и многосторонние соглашения, а также страны, участвующие в межведомственных и государственно-частных партнерствах. К типичным целям сотрудничества в области кибербезопасности относятся согласование мер по обеспечению минимальной безопасности, обмен информацией и передовым опытом, а также кодификация норм поведения.

[24] https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019

Двусторонние и многосторонние соглашения

Двусторонние и многосторонние соглашения имеют решающее значение для кодификации норм поведения и расширения международного сотрудничества в области кибербезопасности.

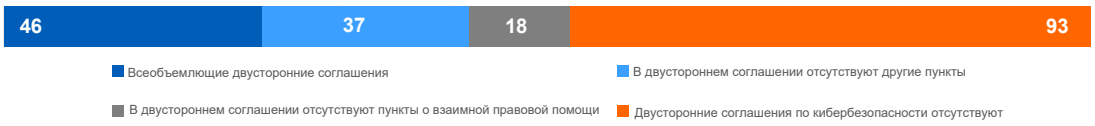
Рисунок 22. Страны, участвующие в двусторонних соглашениях по кибербезопасности



Источник: МСЭ

Полученные данные показывают, что двусторонние соглашения по кибербезопасности имеют 90 стран. Что касается типов соглашений, отслеживаемых в GCI, то некоторые страны заключают соглашения по кибербезопасности в области развития потенциала. Иногда соглашение касается только обмена информацией, при этом кибербезопасность не всегда является центральным пунктом соглашения и может входить как составная часть в другие темы. Двусторонние соглашения 37 стран включают как обмен информацией, так и меры по развитию потенциала, но не охватывают взаимную правовую помощь.

Рисунок 23. Страны, имеющие двусторонние соглашения по кибербезопасности (по затронутым темам)



Источник: МСЭ

Учитывая необходимость коллективных действий в области кибербезопасности, некоторые страны стремились к тому, чтобы подписать не только двусторонние, но и многосторонние соглашения. В данном издании Глобального индекса кибербезопасности многосторонними считаются соглашения, заключенные между тремя и более сторонами, включая органы государственной власти и региональные организации, но исключая международные конвенции, такие как Будапештская конвенция о киберпреступности.

Рисунок 24. Количество стран, участвующих в многосторонних соглашениях по кибербезопасности (подписанных и ратифицированных)

Источник: МСЭ

Многосторонние соглашения страны заключают чаще, чем двусторонние: почти 57% стран подписали хотя бы одно многостороннее соглашение против 46% стран, подписавших хотя бы одно двустороннее соглашение. Многие страны (99) подписали или ратифицировали многосторонние соглашения по обмену информацией и развитию потенциала.

Рисунок 25. Участие в международной деятельности

Источник: МСЭ

Помимо официального сотрудничества между двумя и более странами, участие в международной деятельности позволяет странам перенимать передовой опыт и узнавать о новых подходах к борьбе с киберугрозами. За последние два года участие в международной деятельности (конференции по кибербезопасности, семинары-практикумы, деятельность в рамках партнерств и соглашений с другими странами) приняли 140 стран.

Государственно-частное партнерство

Помимо сотрудничества с другими странами, страны сотрудничают с предприятиями частного сектора. Государственно-частное партнерство (ГЧП) имеет решающее значение для успеха усилий по обеспечению кибербезопасности, поскольку оно предусматривает обмен полезной информацией, обмен передовым опытом и информирование о потребностях и приоритетах в сфере НИОКР. В таблице 2 указано количество стран, участвующих в международном и/или внутреннем ГЧП.

Таблица 2. Страны, участвующие в международном и/или внутреннем ГЧП

	Международное ГЧП	Международное ГЧП в стадии становления	Международное ГЧП отсутствует
Внутреннее ГЧП	62	0	14
Внутреннее ГЧП в стадии становления	1	0	0
Внутреннее ГЧП отсутствует	12	1	104

Источник: МСЭ

Для взаимодействия с более широкой экосистемой кибербезопасности некоторые страны организовывают конференции и семинары-практикумы, а другие нанимают компании частного сектора для разработки учебных курсов для государственных учреждений. Все большее число стран сообщает о создании научно-технических парков для укрепления своих экосистем кибербезопасности. Эти платформы могут служить местом встречи представителей частного и государственного секторов, проведения тренингов, семинаров-практикумов, поддержки стартапов и проведения конкурсов. Такая межотраслевая инициатива направлена на развитие экосистемы кибербезопасности, обмен знаниями и компетенциями между различными заинтересованными сторонами, учеными, студентами, специалистами по кибербезопасности, стартапами, государственными учреждениями и иностранными компаниями. Собранные данные показывают, что почти половина стран участвует в партнерстве по крайней мере одного типа, 86 стран участвуют или в намерены участвовать в скором будущем в международном или внутреннем ГЧП, а 60 из них участвуют как во внутренних, так и в международных партнерствах.

2.6 Защита ребенка в онлайновой среде

Рисунок 26. Отчеты из серии публикаций МСЭ о защите ребенка в онлайновой среде

Источник: МСЭ

Как отмечается в руководящих указаниях МСЭ по защите ребенка в онлайновой среде, защита детей в онлайновой среде представляет собой общемировую проблему, для решения которой требуется глобальный подход[25]. Эти руководящие указания появились в то время, когда в результате перехода на дистанционное обучение дети находятся в онлайновой среде больше, чем когда-либо прежде, и во время пандемии COVID-19 они в большей степени подвержены рискам. В отличие от предыдущих поколений, которым в условиях пандемий приходилось обращаться к дистанционному обучению по

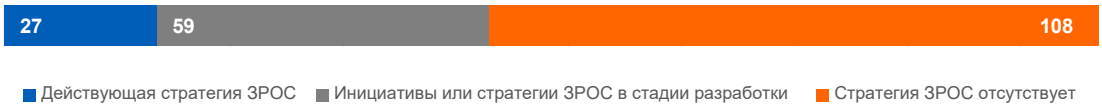
[25] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx

радио[26], нынешнее поколение учащихся благодаря цифровым технологиям получило возможность интерактивного обучения, которое позволяет им установить двустороннюю связь не только с учебными материалами, но и друг с другом.

Руководящие указания МСЭ по защите ребенка в онлайновой среде призваны помочь детям, родителям и преподавателям управлять рисками в сети, а также использовать потенциал цифровых технологий и укреплять цифровые навыки. Кроме того, руководящие указания содержат рекомендации для директивных органов по ускорению разработки и принятия надежной национальной стратегии и планов действий по защите ребенка в онлайновой среде, а также по содействию вовлечению в разработку такой политики предприятий частного сектора.

В этой связи вопросы, связанные с защитой ребенка в онлайновой среде, измеряют степень готовности стран к приходу цифрового поколения исходя из наличия ряда элементов, таких как законы о защите ребенка в онлайновой среде, механизм передачи сообщений о проблемах в онлайновой среде, информационные кампании и учебные программы для школ, а также разработка государственной стратегии защиты ребенка в онлайновой среде и следование этой стратегии.

Рисунок 27. Страны, имеющие стратегию защиты ребенка в онлайновой среде (ЗРОС)



Источник: МСЭ

Отвечая на вопросник, 86 из 194 стран сообщили о наличии мер по защите ребенка в онлайновой среде. Однако собранные данные показывают, что лишь у 13% из 194 стран имеется отдельная стратегия, направленная на защиту детей в сети. С другой стороны, в 30% стран инициативы по защите ребенка в онлайновой среде входят в состав более общей стратегии, законодательства или инициативы по борьбе с киберпреступностью.

Результаты также показывают, что Европейский регион демонстрирует высокие показатели по вопросам, относящимся к защите ребенка в онлайновой среде: полностью веденные в действие законы о защите ребенка в онлайновой среде имеются в 89% стран. В дополнение к этому во всем мире зарегистрирован 101 механизм передачи сообщений, включая горячие линии, веб-сайты, адреса электронной почты и социальные сети, а 81 страна пошла еще дальше и поделилась информацией о своей стратегии защиты ребенка в онлайновой среде и более широких инициативах.

2.7 Заключение

Модели поведения и методы обеспечения кибербезопасности постоянно развиваются. Цифровые технологии предлагают привлекательный инструмент, способный вести мир вперед, невзирая на глобальные чрезвычайные ситуации в области здравоохранения, изменение климата, старение населения и другие вызовы завтрашнего дня. Согласно прогнозам, в 2030 году, когда будут достигнуты цели в области устойчивого развития (ЦУР), 90% прогнозируемого населения мира, или 7,5 миллиарда человек, получат возможность установления соединений[27], а количество подключенных к сети устройств интернета вещей (IoT) составит от 24,1 миллиарда[28] до 125 миллиардов[29]. Чтобы усилия, прилагаемые для достижения ЦУР, носили устойчивый характер, необходимо обеспечить кибербезопасность, гарантирующую, что цифровые решения безопасны, надежны и заслуживают доверия.

---

26 https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/

27 https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

28 https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html

29 https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

Один из уроков COVID-19 заключается в том, что проблемы, для решения которых требуются коллективные действия, такие как охрана здоровья и кибербезопасность, необходимо решать с использованием междисциплинарного и целостного подхода. Для решения задач в рамках всех компонентов GCI – правовых, технических, организационных мер, а также мер по развитию потенциала и мер в области сотрудничества – потребуется обеспечить связь людей друг с другом и укрепить доверие. Помимо совместной работы внутри стран, может потребоваться оказание поддержки другим государствам, в меньшей степени способным к решению проблем кибербезопасности, таким как наименее развитые страны, малые островные развивающиеся государства и развивающиеся страны, не имеющие выхода к морю.

Чтобы двигаться вперед, странам необходимо обратить внимание на свои сильные и слабые стороны в области кибербезопасности и использовать свои конкурентные преимущества для развития общего киберпотенциала и системы здравоохранения. Глобальный индекс кибербезопасности поможет странам начать этот процесс. Чтобы продолжить его, странам, возможно, потребуется рассмотреть следующие вопросы:

- регулярные оценки своих обязательств в области кибербезопасности, включая значимые показатели;
- постоянное развитие национальных CIRT и создание отраслевых CIRT;
- мониторинг и обновление национальных стратегий кибербезопасности с четкими планами их реализации;
- обеспечение охвата цифровыми технологиями и поддержание разнообразия в составе работников сферы кибербезопасности, особенно среди недопредставленных групп, таких как женщины и молодежь;
- регулярное участие в международной деятельности в целях обмена передовым опытом, исследования конкретных ситуаций и повышения готовности и потенциала реагирования;
- повышение потенциала кибербезопасности микро-, малых и средних предприятий (ММСП); и
- регулярное участие всех заинтересованных сторон в обеспечении кибербезопасности, включая предприятия частного сектора, учебные заведения и гражданское общество.

3 Итоговые показатели GCI: оценки и рейтинги

3.1 Общие оценки и рейтинги стран

В следующей таблице приведены оценки и рейтинги всех стран, которым был разослан вопросник.

Таблица 3. Итоговые показатели GCI: общие оценки и рейтинги

Страна	Оценка	Рейтинг
Соединенные Штаты Америки**	100	1
Соединенное Королевство	99,54	2
Саудовская Аравия	99,54	2
Эстония	99,48	3
Корея (Республика)	98,52	4
Сингапур	98,52	4
Испания	98,52	4
Российская Федерация	98,06	5
Объединенные Арабские Эмираты	98,06	5
Малайзия	98,06	5
Литва	97,93	6
Япония	97,82	7
Канада**	97,67	8
Франция	97,6	9
Индия	97,5	10
Турция	97,49	11
Австралия	97,47	12
Люксембург	97,41	13
Германия	97,41	13
Португалия	97,32	14
Латвия	97,28	15
Нидерланды**	97,05	16
Норвегия**	96,89	17
Маврикий	96,89	17
Бразилия	96,6	18

Страна	Оценка	Рейтинг
Бельгия	96,25	19
Италия	96,13	20
Оман	96,04	21
Финляндия	95,78	22
Египет	95,48	23
Индонезия	94,88	24
Вьетнам	94,59	25
Швеция	94,55	26
Катар	94,5	27
Греция	93,98	28
Австрия	93,89	29
Польша	93,86	30
Казахстан	93,15	31
Дания	92,6	32
Китай	92,53	33
Хорватия	92,53	33
Словакия	92,36	34
Венгрия	91,28	35
Израиль**	90,93	36
Танзания	90,58	37
Северная Македония	89,92	38
Сербия	89,8	39
Азербайджан	89,31	40
Кипр	88,82	41
Швейцария**	86,97	42
Гана	86,69	43

Страна	Оценка	Рейтинг
Таиланд	86,5	44
Тунис	86,23	45
Ирландия	85,86	46
Нигерия	84,76	47
Новая Зеландия**	84,04	48
Мальта	83,65	49
Марокко	82,41	50
Кения	81,7	51
Мексика	81,68	52
Бангладеш	81,27	53
Иран (Исламская Республика)	81,07	54
Грузия	81,06	55
Бенин	80,06	56
Руанда	79,95	57
Исландия	79,81	58
Южно-Африканская Республика**	78,46	59
Бахрейн	77,86	60
Филиппины	77	61
Румыния	76,29	62
Молдова	75,78	63
Уругвай	75,15	64
Кувейт	75,07	65
Доминиканская Республика	75,05	66
Словения	74,93	67
Чешская Республика	74,37	68
Монако	72,57	69
Узбекистан	71,11	70
Иордания	70,96	71
Уганда	69,98	72
Замбия	68,88	73
Чили	68,83	74
Кот-д'Ивуар	67,82	75

Страна	Оценка	Рейтинг
Коста-Рика	67,45	76
Болгария	67,38	77
Украина	65,93	78
Пакистан	64,88	79
Албания	64,32	80
Колумбия	63,72	81
Куба	58,76	82
Шри-Ланка	58,65	83
Парагвай	57,09	84
Бруней-Даруссалам	56,07	85
Перу	55,67	86
Черногория	53,23	87
Ботсвана	53,06	88
Беларусь	50,57	89
Армения**	50,47	90
Аргентина	50,12	91
Кыргызстан	49,64	92
Камерун	45,63	93
Непал (Республика)	44,99	94
Чад	40,44	95
Буркина-Фасо**	39,98	96
Малави	36,83	97
Зимбабве	36,49	98
Мьянма	36,41	99
Сенегал	35,85	100
Лихтенштейн**	35,15	101
Судан	35,03	102
Панама	34,11	103
Алжир	33,95	104
Того	33,19	105
Ямайка**	32,53	106
Гамбия	32,12	107

Страна	Оценка	Рейтинг
Суринам	31,2	108
Ливан**	30,44	109
Босния и Герцеговина	29,44	110
Самоа	29,33	111
Фиджи	29,08	112
Ливия	28,78	113
Гайана	28,11	114
Эфиопия	27,74	115
Венесуэла	27,06	116
Андорра**	26,38	117
Папуа – Новая Гвинея**	26,33	118
Эквадор	26,3	119
Монголия	26,2	120
Сьерра-Леоне	25,31	121
Государство Палестина	25,18	122
Мозамбик	24,18	123
Мадагаскар**	23,33	124
Тринидад и Тобаго	22,18	125
Сирийская Арабская Республика**	22,14	126
Науру**	21,42	127
Тонга**	20,95	128
Ирак**	20,71	129
Гвинея**	20,53	130
Лаосская Народно-Демократическая Республика	20,34	131
Камбоджа**	19,12	132
Мавритания	18,94	133
Бутан	18,34	134
Эсватини	18,23	135
Кабо-Верде	17,74	136
Сомали	17,25	137
Таджикистан**	17,1	138

Страна	Оценка	Рейтинг
Барбадос	16,89	139
Боливия (Многонациональное Государство)	16,14	140
Сан-Томе и Принсипи	15,64	141
Антигуа и Барбуда	15,62	142
Конго (Республика)**	14,72	143
Туркменистан**	14,48	144
Кирибати	13,84	145
Сан-Марино	13,83	146
Багамы	13,37	147
Сальвадор**	13,3	148
Сейшельские Острова**	13,23	149
Гватемала	13,13	150
Ангола	12,99	151
Вануату	12,88	152
Сент-Китс и Невис**	12,44	153
Сент-Винсент и Гренадины**	12,18	154
Намибия	11,47	155
Нигер	11,38	156
Габон	11,36	157
Сент-Люсия**	10,96	158
Белиз	10,29	159
Мали**	10,14	160
Гвинея-Бисау	9,85	161
Либерия	9,72	162
Гренада	9,41	163
Лесото	9,08	164
Никарагуа**	9	165
Соломоновы Острова	7,08	166
Гаити	6,4	167
Тувалу**	5,78	168
Южный Судан**	5,75	169

Страна	Оценка	Рейтинг
Демократическая Республика Конго	5,3	170
Афганистан	5,2	171
Маршалловы Острова**	4,9	172
Тимор-Лешти**	4,26	173
Доминика	4,2	174
Коморские Острова**	3,72	175
Центральноафриканская Республика**	3,24	176
Мальдивские Острова**	2,95	177
Гондурас**	2,2	178
Джибути	1,73	179
Бурунди	1,73	179
Эритрея**	1,73	179
Экваториальная Гвинея**	1,46	180
Корейская Народно-Демократическая Республика **	1,35	181
Микронезия*	0	182
Ватикан*	0	182
Йемен*	0	182

* Данные отсутствуют

** Ответы на вопросник не получены

3.2 Оценки и рейтинги стран по регионам

Таблица 4. Итоговые показатели GCI: Африканский регион

Страна	Общая оценка	Региональный рейтинг
Маврикий	96,89	1
Танзания	90,58	2
Гана	86,69	3
Нигерия	84,76	4
Кения	81,7	5
Бенин	80,06	6
Руанда	79,95	7
Южно-Африканская Республика**	78,46	8
Уганда	69,98	9
Замбия	68,88	10
Кот-д'Ивуар	67,82	11
Ботсвана	53,06	12
Камерун	45,63	13
Чад	40,44	14
Буркина-Фасо**	39,98	15
Малави	36,83	16
Зимбабве	36,49	17
Сенегал	35,85	18
Того	33,19	19
Гамбия	32,12	20
Эфиопия	27,74	21
Сьерра-Леоне	25,31	22
Мозамбик	24,18	23
Мадагаскар	23,33	24
Гвинея**	20,53	25
Эсватини	18,23	26
Кабо-Верде	17,74	27
Сан-Томе и Принсипи	15,64	28
Конго (Республика)**	14,72	29
Сейшельские Острова**	13,23	30
Ангола	12,99	31
Намибия	11,47	32
Нигер	11,36	33

Страна	Общая оценка	Региональный рейтинг
Габон	11,38	34
Мали**	10,14	35
Гвинея-Бисау	9,85	36
Либерия	9,72	37
Лесото	9,08	38
Южный Судан**	5,75	39
Демократическая Республика Конго	5,3	40
Центрально-африканская Республика**	3,24	41
Бурунди	1,73	42
Эритрея**	1,73	42
Экваториальная Гвинея**	1,46	43

* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

Таблица 5. Итоговые показатели GCI: регион Северной и Южной Америки

Страна	Общая оценка	Региональный рейтинг
Соединенные Штаты Америки**	100	1
Канада**	97,67	2
Бразилия	96,6	3
Мексика	81,68	4
Уругвай	75,15	5
Доминиканская Республика	75,07	6
Чили	68,83	7
Коста-Рика	67,45	8
Колумбия	63,72	9
Куба	58,76	10
Парагвай	57,09	11
Перу	55,67	12
Аргентина	50,12	13
Панама	34,11	14
Ямайка**	32,53	15
Суринам	31,2	16
Гайана	28,11	17
Венесуэла	27,06	18
Эквадор	26,3	19
Тринидад и Тобаго	22,18	20
Барбадос	16,89	21
Боливия (Многонациональное Государство)	16,14	22
Антигуа и Барбуда	15,62	23
Багамские Острова	13,37	24
Сальвадор**	13,3	25
Гватемала	13,13	26
Сент-Китс и Невис	12,44	27
Сент-Винсент и Гренадины**	12,18	28
Сент-Люсия**	10,96	29
Белиз	10,29	30
Гренада	9,41	31
Никарагуа	9	32
Гаити	6,4	33
Доминика	4,2	34
Гондурас**	2,2	35

* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

Таблица 6. Итоговые показатели GCI: регион арабских государств

Страна	Общая оценка	Региональный рейтинг
Саудовская Аравия	99,54	1
Объединенные Арабские Эмираты	98,06	2
Оман	96,04	3
Египет	95,48	4
Катар	94,5	5
Тунис	86,23	6
Марокко	82,41	7
Бахрейн	77,86	8
Кувейт	75,05	9
Иордания	70,96	10
Судан	35,03	11
Алжир	33,95	12
Ливан**	30,44	13
Ливия	28,78	14
Государство Палестина	25,18	15
Сирийская Арабская Республика**	22,14	16
Ирак**	20,71	17
Мавритания	18,94	18
Сомали	17,25	19
Коморские Острова**	3,72	20
Джибути	1,73	21
Йемен*	0	22

* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

Таблица 7. Итоговые показатели GCI: Азиатско-Тихоокеанский регион

Страна	Общая оценка	Региональный рейтинг
Корея (Республика)	98,52	1
Сингапур	98,52	1
Малайзия	98,06	2
Япония	97,82	3
Индия	97,49	4
Австралия	97,47	5
Индонезия	94,88	6
Вьетнам	94,55	7
Китай	92,53	8
Таиланд	86,5	9
Новая Зеландия**	84,04	10
Бангладеш	81,27	11
Иран (Исламская Республика)	81,06	12
Филиппины	77	13
Пакистан	64,88	14
Шри-Ланка	58,65	15
Бруней-Даруссалам	56,07	16
Непал (Республика)	44,99	17
Мьянма	36,41	18
Самоа	29,33	19
Фиджи	29,08	20
Папуа – Новая Гвинея**	26,33	21
Монголия	26,2	22
Науру**	21,42	23
Тонга**	20,95	24
Лаосская Народно-Демократическая Республика	20,34	25
Камбоджа**	19,12	26
Бутан	18,34	27

Страна	Общая оценка	Региональный рейтинг
Кирибати	13,84	28
Вануату	12,88	29
Соломоновы Острова	7,08	30
Тувалу**	5,78	31
Афганистан	5,2	32
Маршалловы Острова**	4,9	33
Тимор-Лешти**	4,26	34
Мальдивские Острова**	2,95	35
Корейская Народно-Демократическая Республика**	1,35	36
Микронезия*	0	37

* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

Таблица 8. Итоговые показатели GCI: регион СНГ

Страна	Общая оценка	Региональный рейтинг
Российская Федерация	98,06	1
Казахстан	93,15	2
Азербайджан	89,31	3
Узбекистан	71,11	4
Беларусь	50,57	5
Армения**	50,47	6
Кыргызстан	49,64	7
Таджикистан**	17,1	8
Туркменистан**	14,48	9

* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

Таблица 9. Итоговые показатели GCI: Европейский регион

Страна	Общая оценка	Региональный рейтинг
Соединенное Королевство	99,54	1
Эстония	99,48	2
Испания	98,52	3
Литва	97,93	4
Франция	97,6	5
Турция	97,5	6
Люксембург	97,41	7
Германия	97,41	7
Португалия	97,32	8
Латвия	97,28	9
Нидерланды**	97,05	10
Норвегия**	96,89	11
Бельгия	96,25	12
Италия	96,13	13
Финляндия	95,78	14
Швеция	94,59	15
Греция	93,98	16
Австрия	93,89	17
Польша	93,86	18
Дания	92,6	19
Хорватия	92,53	20
Словакия	92,36	21
Венгрия	91,28	22
Израиль**	90,93	23
Республика Северная Македония	89,92	24
Сербия	89,8	25
Кипр	88,82	26
Швейцария**	86,97	27
Ирландия	85,86	28

Страна	Общая оценка	Региональный рейтинг
Мальта	83,65	29
Грузия	81,07	30
Исландия	79,81	31
Румыния	76,29	32
Молдова	75,78	33
Словения	74,93	34
Чешская Республика	74,37	35
Монако	72,57	36
Болгария	67,38	37

Страна	Общая оценка	Региональный рейтинг
Украина	65,93	39
Албания	64,32	40
Черногория	53,23	41
Лихтенштейн**	35,15	42
Босния и Герцеговина	29,44	43
Андорра**	26,38	44
Сан-Марино	13,83	45
Ватикан*	0	46

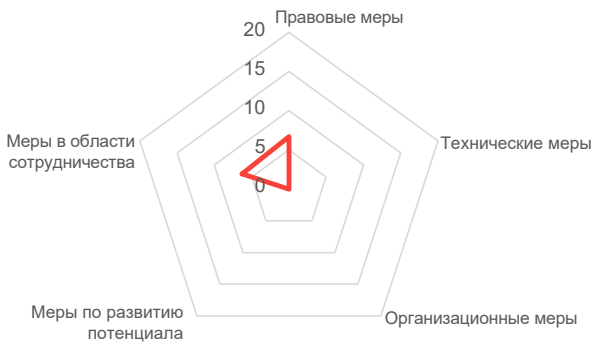
* Данные отсутствуют

** Ответы на вопросник не получены/данные собраны группой GCI

4 Глобальный индекс кибербезопасности, 2020 год: профили стран

Африканский регион

Ангола (Республика)



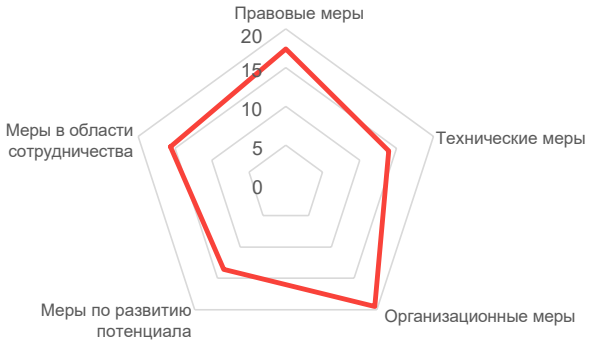
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры по развитию потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
12,99	6,70	0,00	0,00	0,00	6,30

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бенин (Республика)



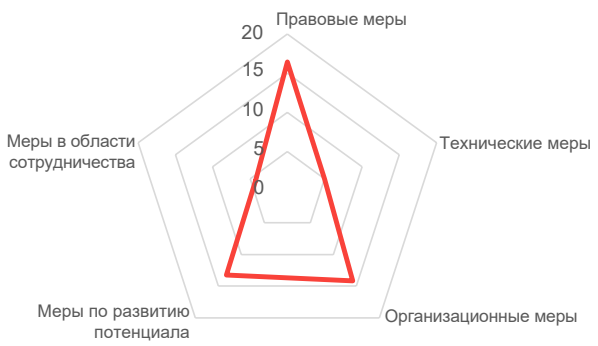
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
80,06	17,42	13,94	19,48	13,60	15,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Ботсвана (Республика)



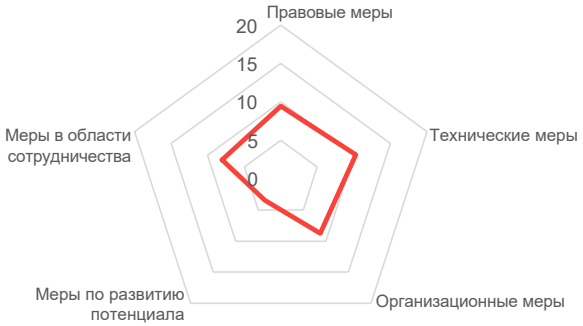
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества, технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
53,06	16,44	4,95	14,16	13,23	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Буркина-Фасо***



Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС),
страна, не имеющая выхода к морю

Относительно сильные стороны
Технические меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
39,98	9,47	10,25	8,75	3,47	8,04

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бурунди (Республика)

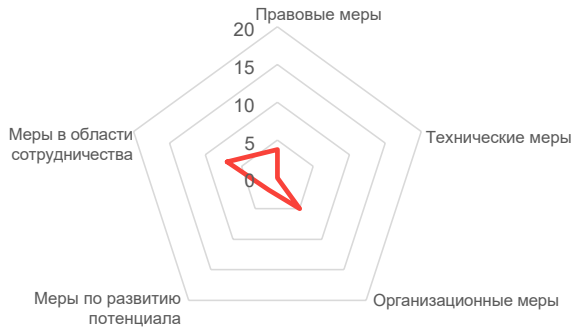
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
1,73	1,73	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кабо-Верде (Республика)



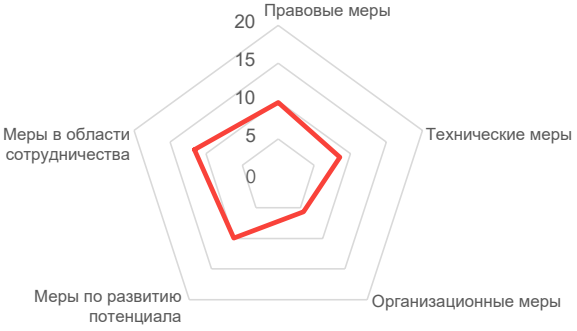
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
17,74	3,77	0,00	5,00	1,96	7,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Камерун (Республика)



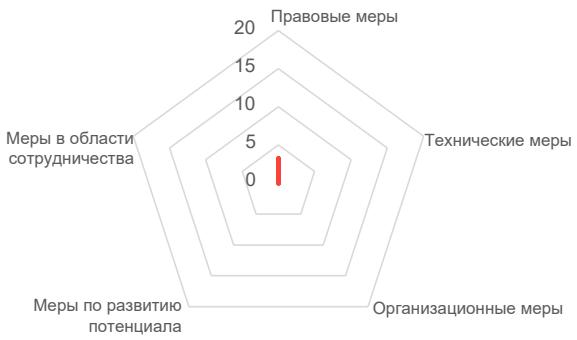
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
45,63	9,84	8,54	5,67	9,95	11,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Центральноафриканская Республика***



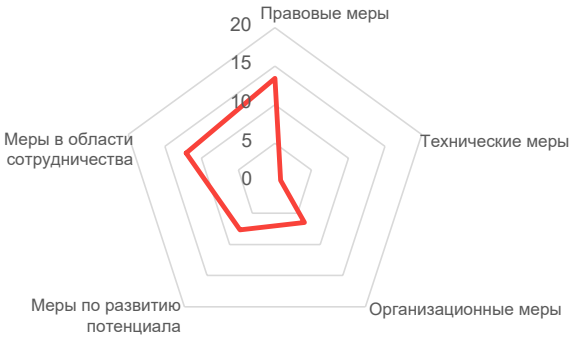
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, развитие потенциала, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
3,24	3,24	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Чад (Республика)



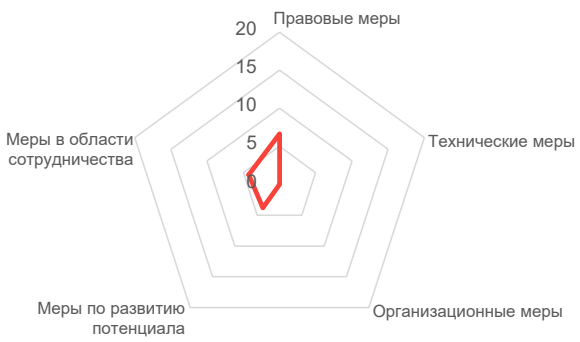
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
40,44	13,43	0,73	6,50	7,67	12,11

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Конго (Республика)***



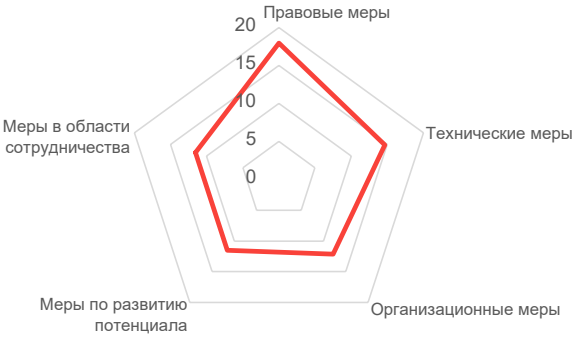
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
14,72	6,66	0,00	0,00	3,80	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кот-д'Ивуар (Республика)



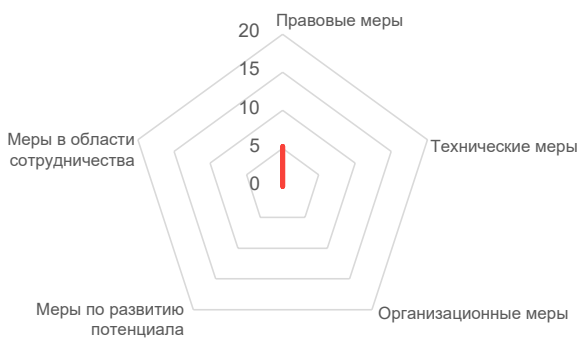
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
67,82	17,95	14,65	12,14	11,53	11,55

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Демократическая Республика Конго



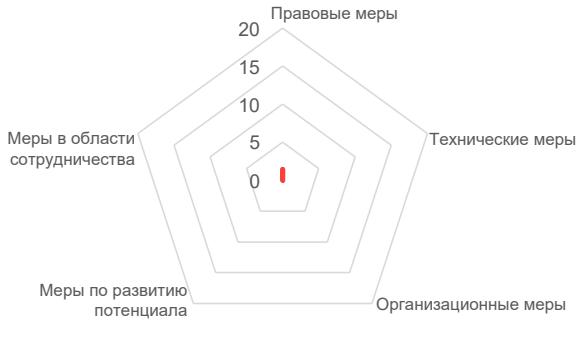
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
5,30	5,30	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Экваториальная Гвинея (Республика)***



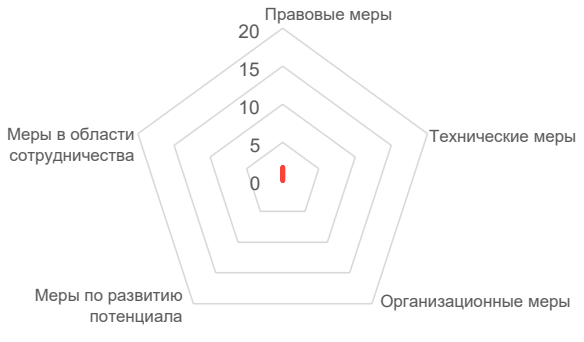
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
1,46	1,46	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Эритрея***



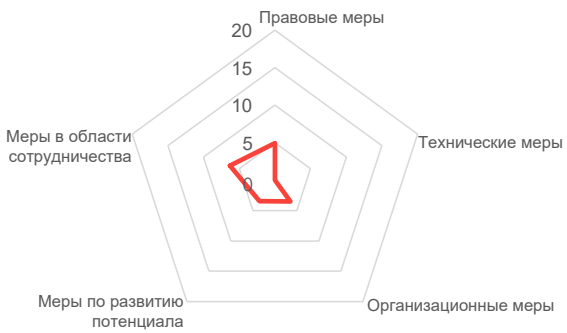
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
1,73	1,73	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Эсватини (Королевство)



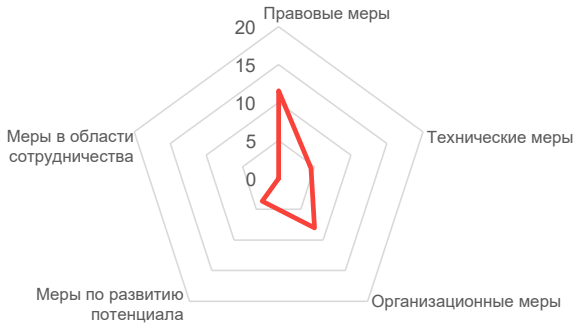
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
18,23	4,96	0,00	3,49	3,47	6,31

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Эфиопия (Федеративная Демократическая Республика)



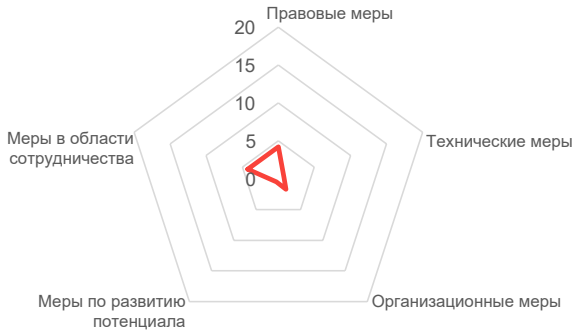
Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС),
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
27,74	11,56	4,46	8,03	3,69	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Габонская Республика



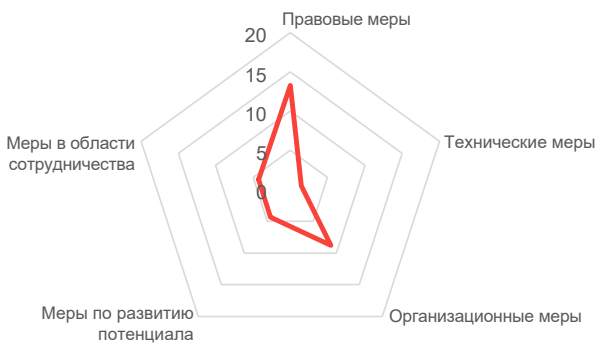
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
11,38	4,24	0,73	1,69	0,46	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гамбия (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
32,12	13,28	1,46	8,78	4,34	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гана

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, технические меры
Области возможного роста
Развитие потенциала, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
86,69	19,35	18,48	17,78	15,44	15,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Гвинея (Республика)***

Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
20,53	12,54	0,00	1,69	0,00	6,30

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гвинея-Бисау (Республика)

Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Правовые меры, технические меры, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
9,85	0,00	0,00	0,00	1,52	8,33

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кения (Республика)

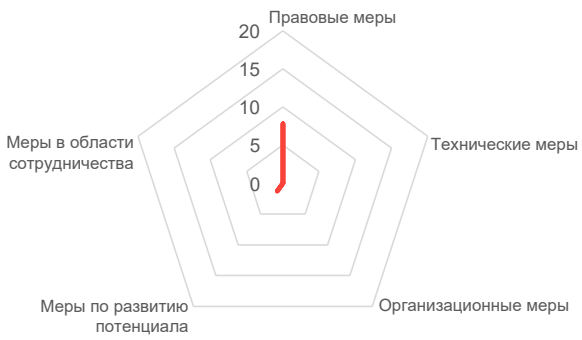
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
81,70	20,00	18,27	12,75	14,79	15,89

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Лесото (Королевство)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
9,08	7,82	0,00	0,00	1,26	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Либерия (Республика)

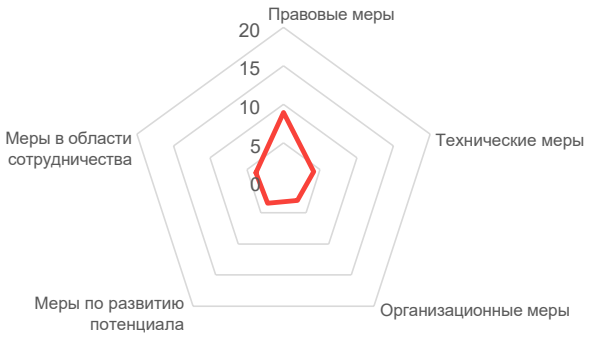
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
9,72	2,31	4,11	0,00	1,26	2,04

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Мадагаскар (Республика)***



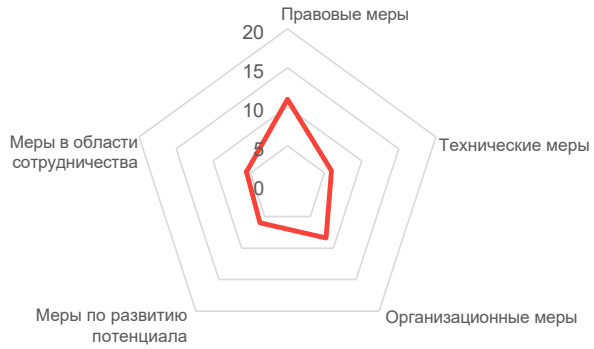
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
23,33	8,96	4,11	3,00	3,47	3,78

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Малави



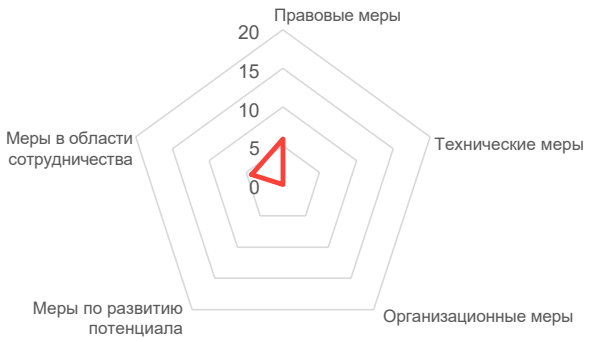
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры, организационные меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
36,83	10,98	5,92	8,40	6,00	5,54

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Мали (Республика)***



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
10,14	5,89	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Маврикий (Республика)

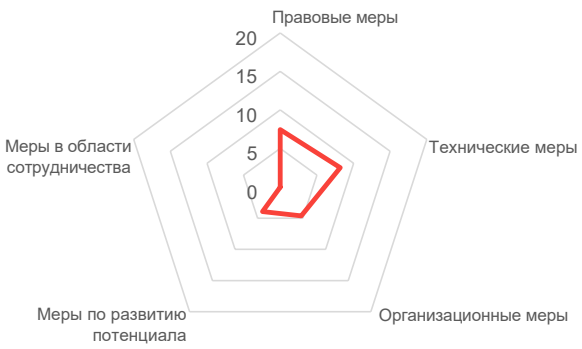
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Технические меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,89	19,27	20,00	18,38	19,54	19,70

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Мозамбик (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Технические меры, правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
24,18	7,46	8,19	4,62	3,92	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Намибия (Республика)

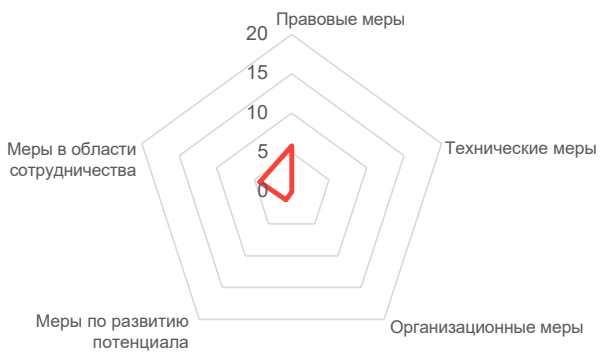
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
11,47	2,84	0,00	0,00	2,34	6,30

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Нигер (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры, меры в области сотрудничества
Области возможного роста
Технические меры, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
11,36	5,87	0,00	0,00	1,23	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Нигерия (Федеративная Республика)

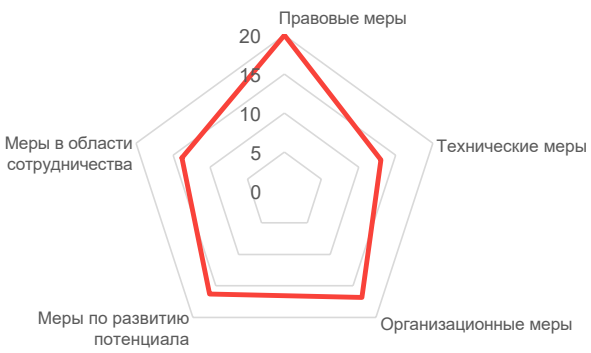
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
84,76	20,00	17,09	18,98	12,21	16,48

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Руанда (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
79,95	20,00	13,00	16,83	16,30	13,82

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сан-Томе и Принсипи (Демократическая Республика)

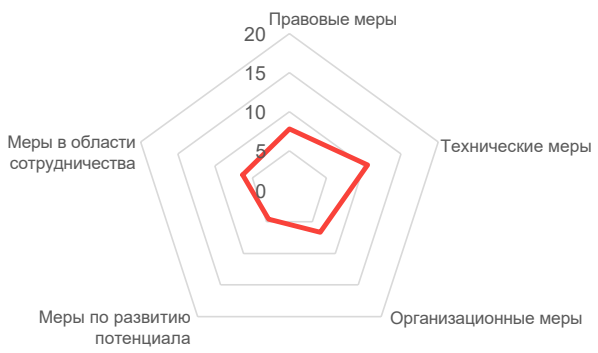
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
15,64	9,94	0,00	1,44	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сенегал (Республика)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
35,85	7,82	10,50	6,66	4,58	6,30

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Сейшельские Острова (Республика)***

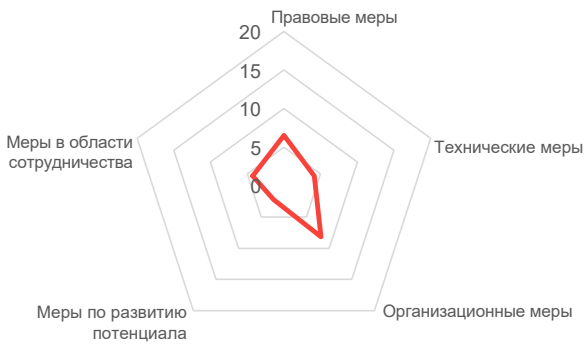
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,23	7,73	0,00	1,44	1,23	2,83

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сьерра-Леоне



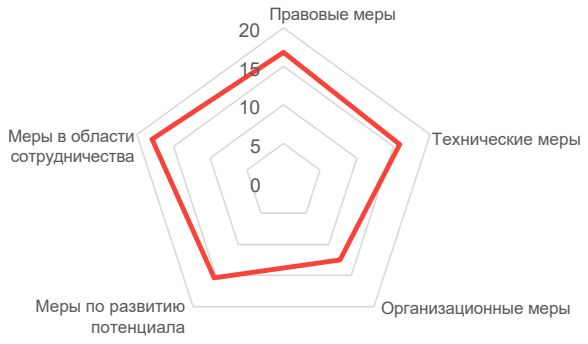
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Организационные меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
25,31	6,54	4,11	8,16	2,24	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Южно-Африканская (Республика)***



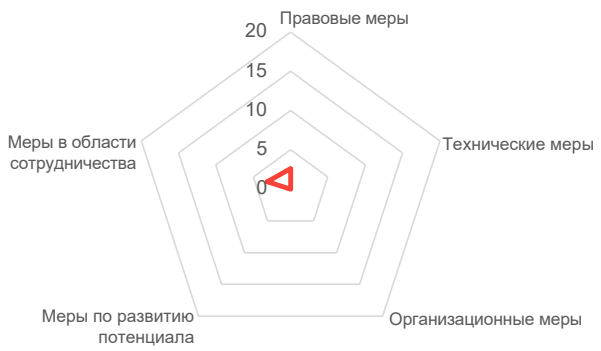
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
78,46	16,82	15,85	12,50	15,37	17,93

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Южный Судан (Республика)***



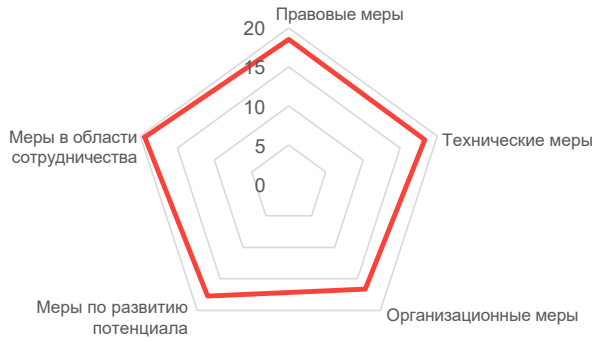
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
5,75	2,63	0,00	0,00	0,00	3,12

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Танзания (Объединенная Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
90,58	18,54	18,31	16,60	17,72	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Тоголезская Республика

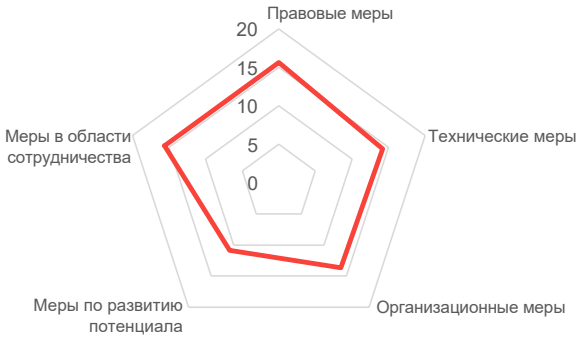
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
33,19	19,19	4,90	3,61	0,00	5,49

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Уганда (Республика)



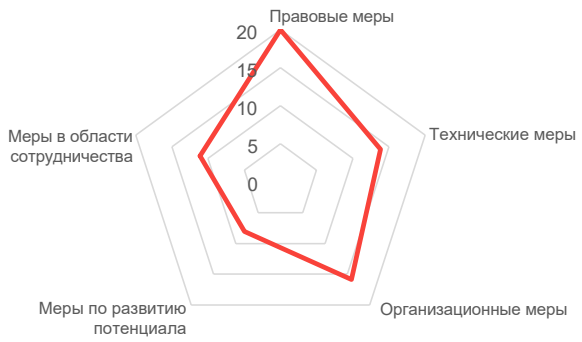
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
69,98	15,64	14,19	13,65	10,87	15,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Замбия (Республика)



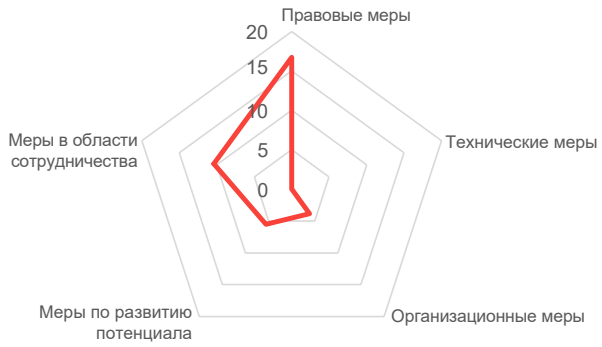
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
68,88	20,00	13,82	15,86	8,07	11,12

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Зимбабве (Республика)



Уровень развития
Развивающаяся страна, страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
36,49	16,73	0,00	3,84	5,52	10,40

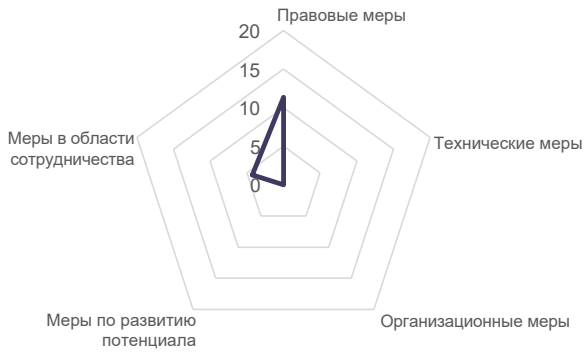
Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Регион Северной и Южной Америки

Антигуа и Барбуда



Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
15,62	11,36	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Республика Аргентина

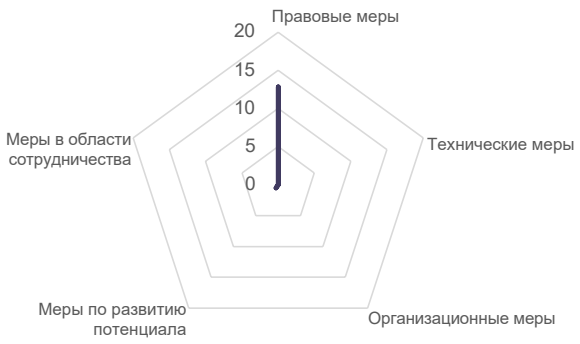
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
50,12	12,15	13,75	8,29	4,38	11,55

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Багамские Острова (Содружество)



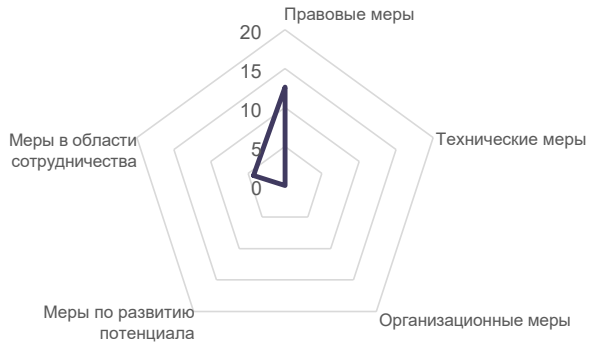
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,37	12,85	0,00	0,00	0,52	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Барбадос



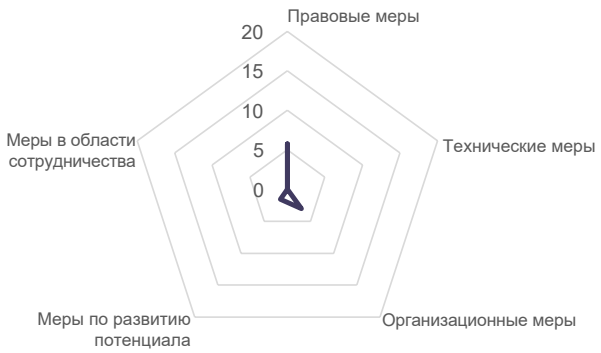
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
16,89	12,63	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Белиз



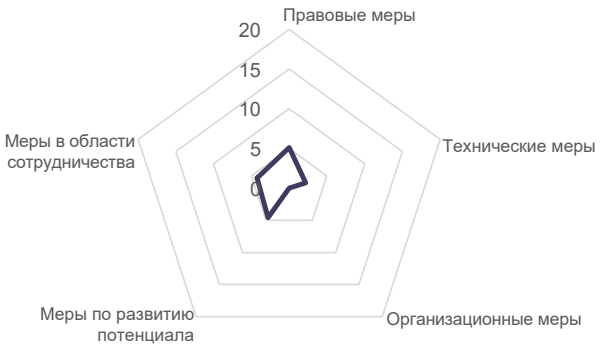
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
10,29	5,77	0,00	3,01	1,52	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Боливия (Многонациональное Государство)



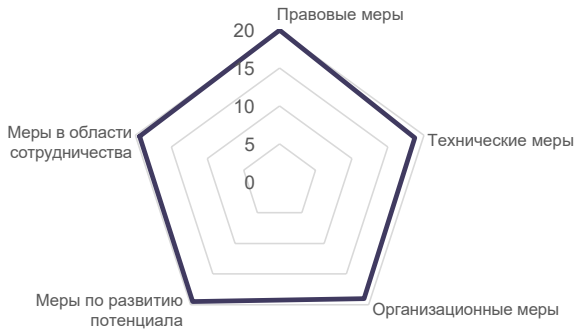
Уровень развития
Развивающаяся страна, страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
16,14	5,13	2,18	0,00	4,58	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бразилия (Федеративная Республика)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры,
организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,60	20,00	18,73	18,98	19,48	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Канада***

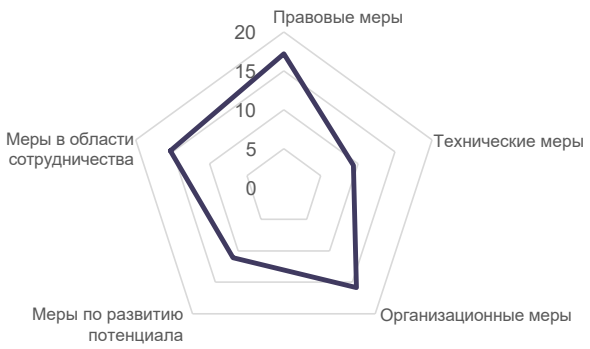
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
организационные меры,
меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,67	20,00	18,27	20,00	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Чили



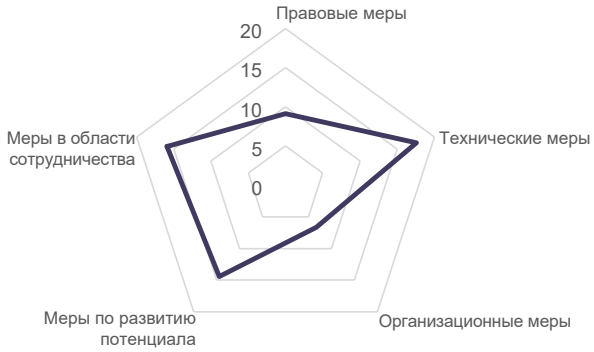
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
68,83	17,20	9,39	15,84	11,07	15,33

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Колумбия (Республика)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
63,72	9,14	17,58	6,67	14,42	15,93

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Коста-Рика

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
67,45	17,62	9,14	12,66	12,11	15,93

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Куба

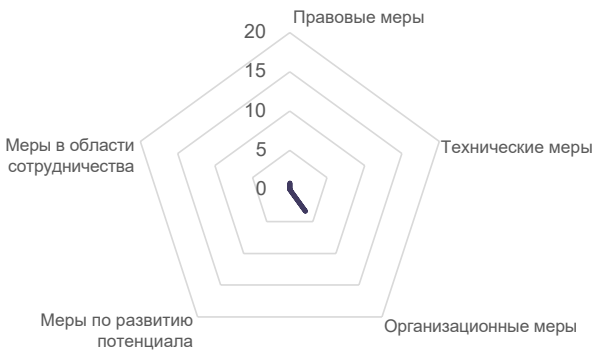
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
58,76	14,85	10,87	13,91	10,52	8,61

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Доминика (Содружество)



Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Организационные меры
Области возможного роста
Технические меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
4,20	0,85	0,00	3,35	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Доминиканская Республика

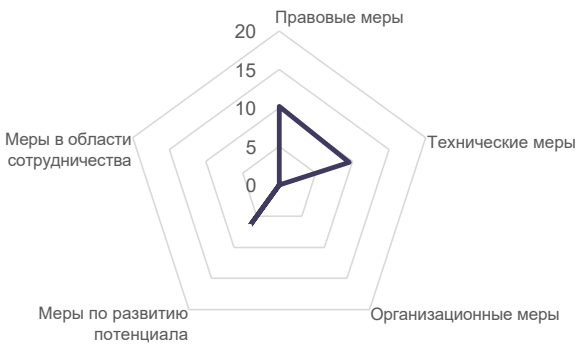
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Организационные меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
75,07	16,38	18,42	18,52	9,94	11,81

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Эквадор



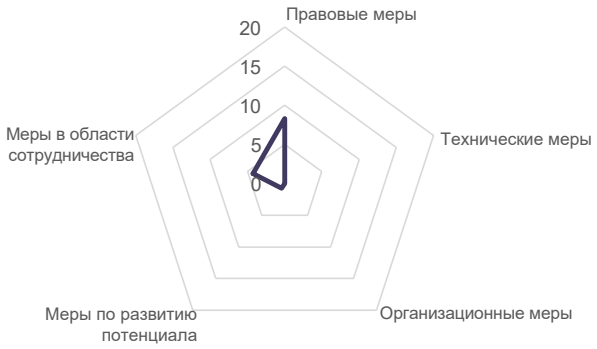
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
26,30	10,22	9,55	0,00	6,53	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Сальвадор (Республика)***



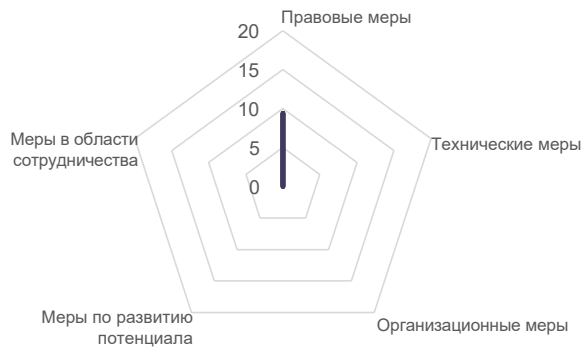
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, технические меры
Области возможного роста
Организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,30	8,32	0,00	0,00	0,72	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гренада



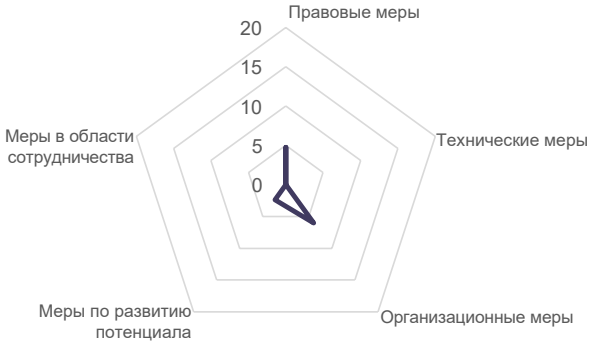
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области развития, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
9,41	9,41	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гватемала (Республика)



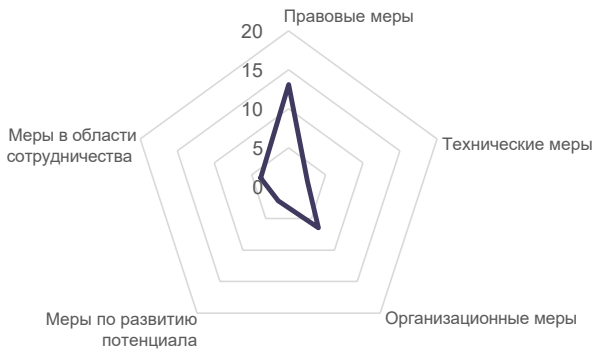
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Организационные меры
Области возможного роста
Технические меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,13	4,76	0,00	6,01	2,36	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гайана



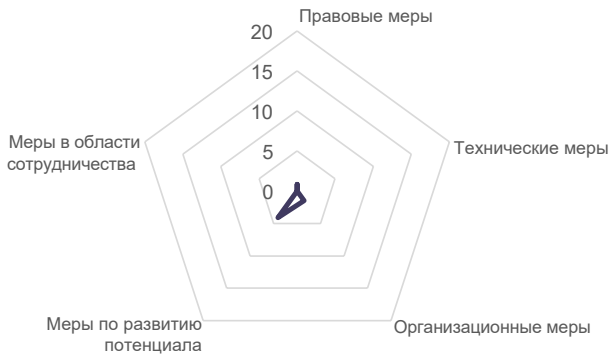
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
28,11	13,12	2,50	6,47	2,24	3,78

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Гаити (Республика)



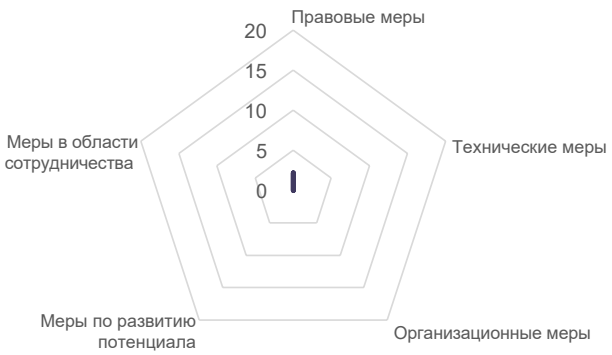
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
6,40	0,85	0,00	1,46	4,09	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Гондурас (Республика)***



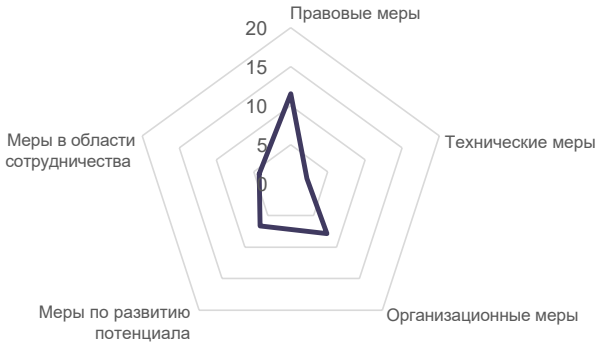
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры,
организационные меры,
меры в области сотрудничества,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
2,20	2,20	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Ямайка***



Уровень развития
Развивающаяся страна,
малое островное
развивающееся государство
(СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
32,53	11,54	2,18	7,87	6,68	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Мексика

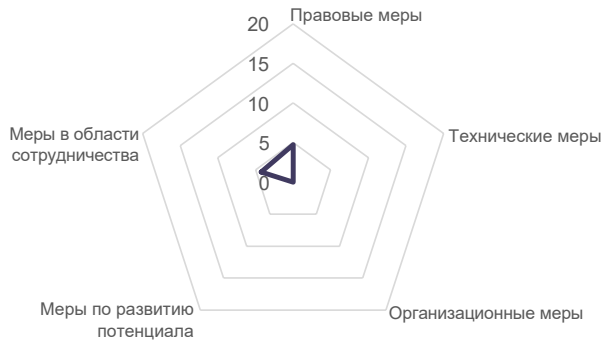
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
81,68	15,61	17,90	14,70	16,13	17,34

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Никарагуа***



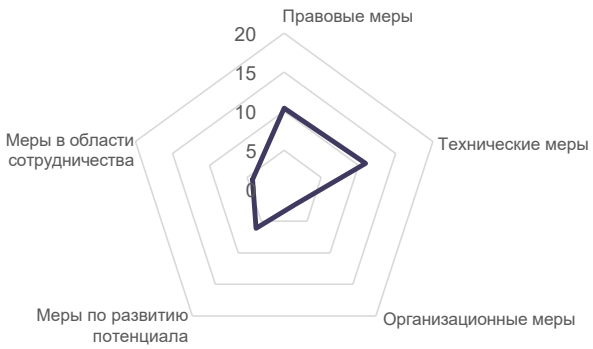
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
развитие потенциала
Области возможного роста
Технические меры,
организационные меры,
меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
9,00	4,74	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Панама (Республика)



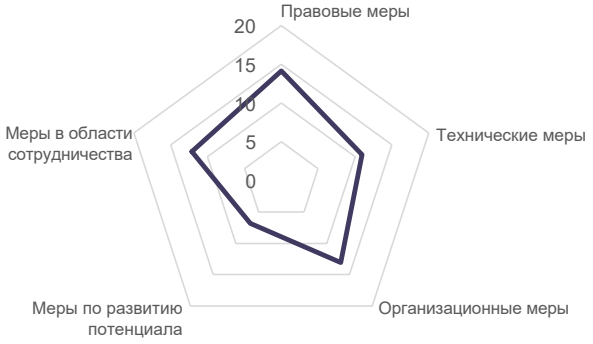
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры,
правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
34,11	10,41	10,94	2,37	6,12	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Парагвай (Республика)



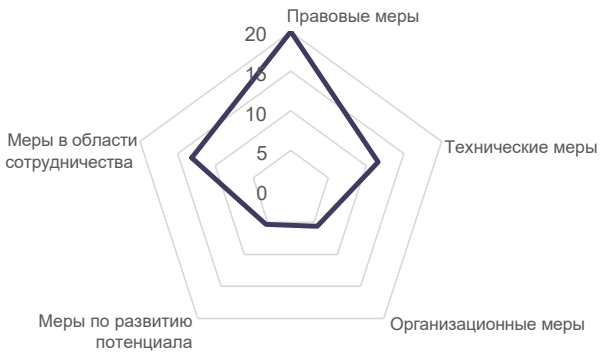
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
57,09	14,15	10,94	13,06	6,79	12,14

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Перу



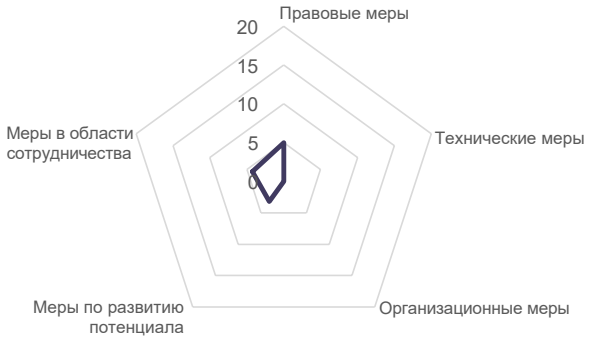
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
55,67	20,00	11,58	5,63	5,32	13,15

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сент-Китс и Невис (Федерация)



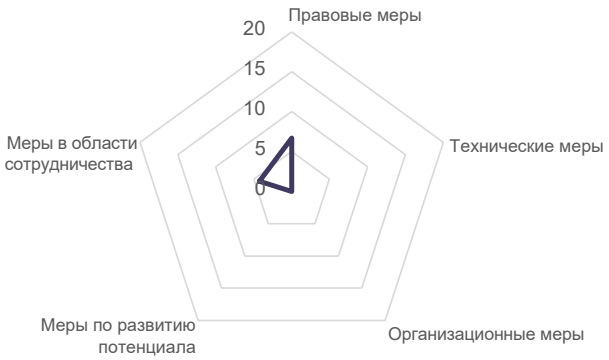
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
12,44	5,00	0,00	0,00	3,18	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Сент-Люсия***



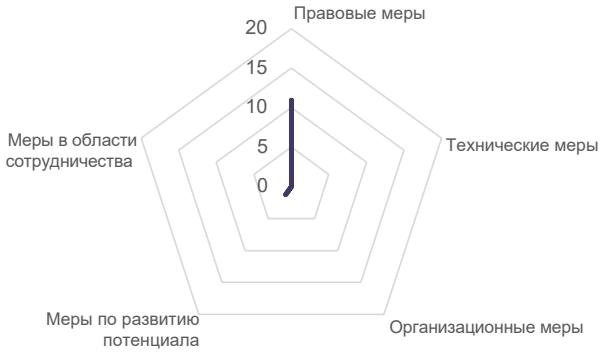
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
10,96	6,70	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Сент-Винсент и Гренадины***



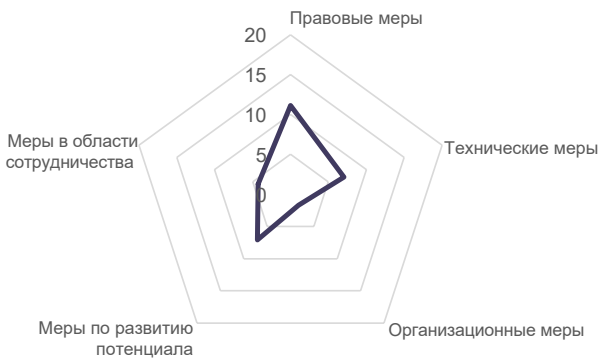
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
12,18	10,95	0,00	0,00	1,23	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Суринам (Республика)



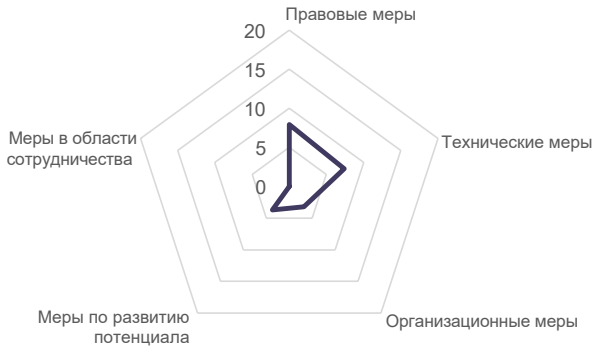
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
31,20	11,13	7,04	1,69	7,08	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Тринидад и Тобаго



Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
22,18	7,94	7,38	3,18	3,69	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Соединенные Штаты Америки***

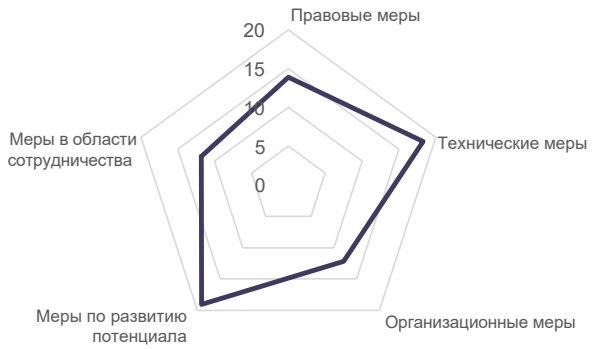
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
организационные меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Данные отсутствуют

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
100,00	20,00	20,00	20,00	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Уругвай (Восточная Республика)



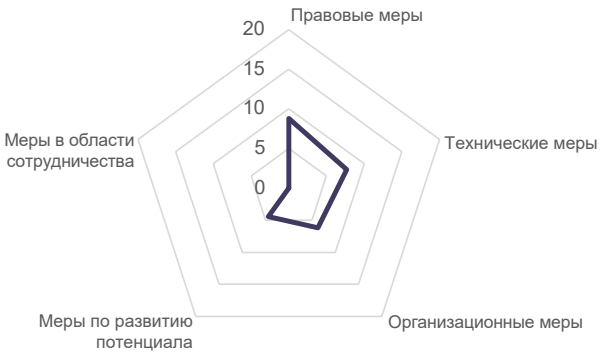
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
75,15	13,90	18,27	12,13	19,04	11,81

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Венесуэла (Боливарианская Республика)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
27,06	8,80	7,67	6,17	4,41	0,00

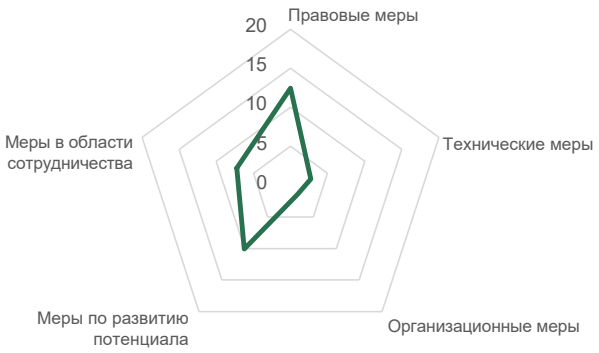
Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Регион арабских государств

Алжир (Народная Демократическая Республика)



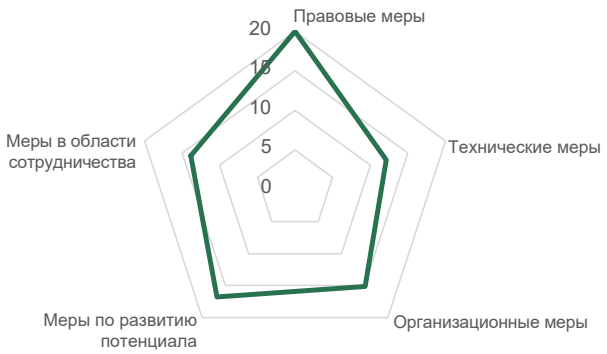
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
33,95	12,46	2,73	1,44	10,07	7,25

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бахрейн (Королевство)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
77,86	20,00	12,12	15,11	16,77	13,86

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Коморские Острова (Союз)***

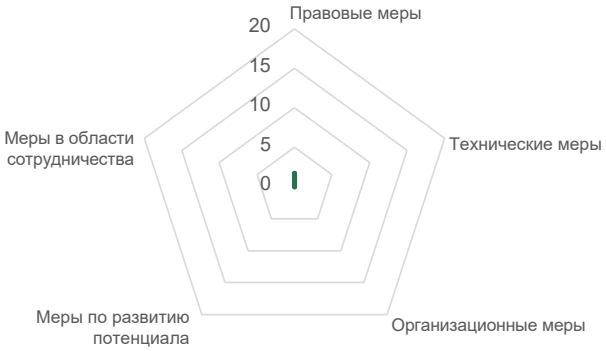
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Правовые меры, технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
3,72	0,00	0,00	1,69	0,00	2,04

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Джибути (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
1,73	1,73	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Египет (Арабская Республика)

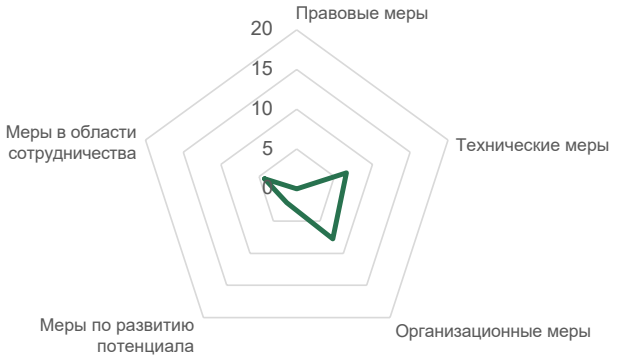
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
организационные меры,
развитие потенциала
Области возможного роста

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
95,48	20,00	17,45	20,00	19,12	18,91

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Ирак (Республика)***



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Организационные меры
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
20,71	0,00	6,56	7,75	2,14	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Иордания (Хашимитское Королевство)

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
70,96	18,53	10,74	15,70	11,47	14,51

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кувейт (Государство)

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
75,05	17,74	14,25	11,13	16,05	15,90

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Ливан***

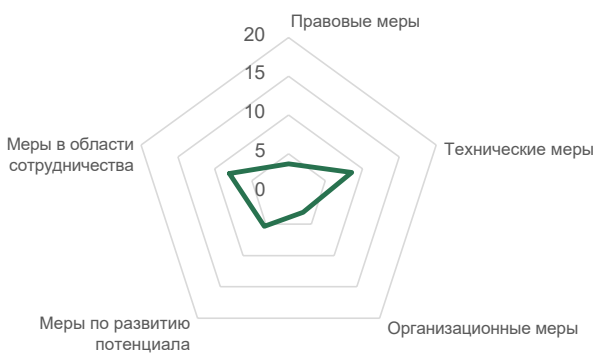
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
30,44	10,24	3,27	5,69	8,26	2,99

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Ливия (Государство)



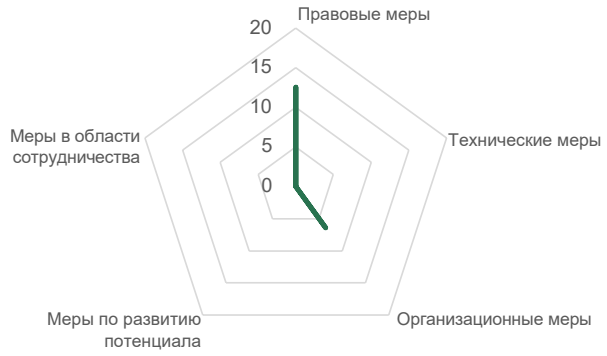
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры,
меры в области сотрудничества
Области возможного роста
Правовые меры,
организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
28,78	3,73	8,54	3,13	5,34	8,04

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Мавритания (Исламская Республика)



Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры,
меры в области сотрудничества,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
18,94	12,55	0,00	6,39	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Марокко (Королевство)

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
82,41	18,40	17,94	12,37	15,24	18,46

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Оман (Султанат)

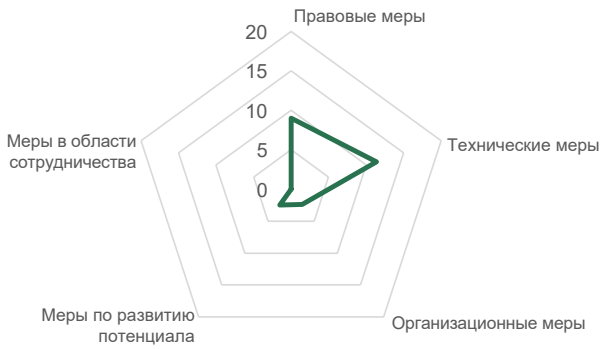
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
организационные меры,
развитие потенциала
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,04	20,00	16,64	20,00	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Государство Палестина



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
25,18	9,02	11,36	2,34	2,46	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Катар (Государство)

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
развитие потенциала
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
94,50	20,00	16,64	18,46	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Саудовская Аравия (Королевство)

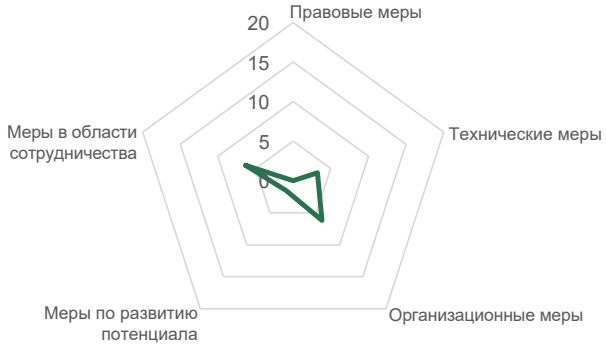
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
организационные меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
99,54	20,00	19,54	20,00	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сомали (Федеративная Республика)



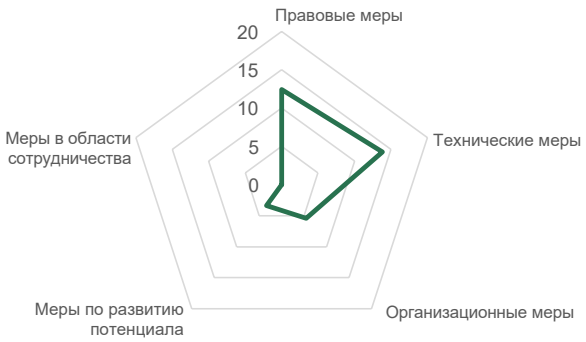
Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС)

Относительно сильные стороны
Организационные меры,
меры в области сотрудничества
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
17,25	0,00	3,25	6,17	1,52	6,31

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Судан (Республика)



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
35,03	12,43	13,81	5,41	3,38	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Сирийская Арабская Республика***

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
22,14	9,80	7,85	4,49	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Тунис

Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
86,23	20,00	19,54	12,21	16,96	17,52

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Объединенные Арабские Эмираты

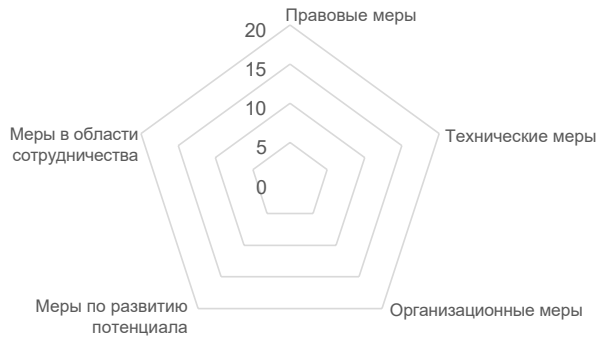
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,06	20,00	19,08	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Йемен (Республика)**



Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС)

Относительно сильные стороны
Данные отсутствуют
Области возможного роста
Данные отсутствуют

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
0	0	0	0	0	0

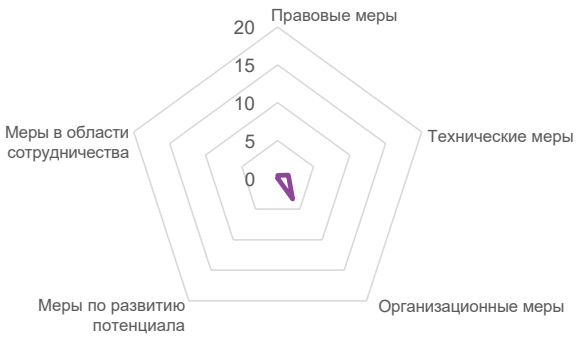
Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Азиатско-Тихоокеанский регион

Афганистан



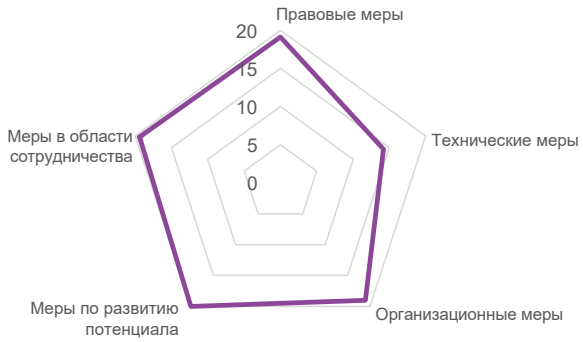
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Организационные меры
Области возможного роста
Развитие потенциала, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
5,20	0,40	1,46	3,35	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Австралия



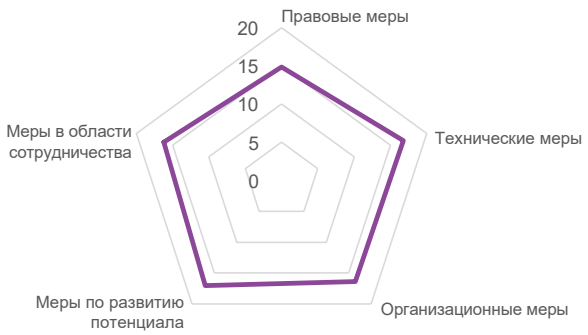
Уровень развития
Развитая страна

Относительно сильные стороны
Развитие потенциала, меры в области сотрудничества, правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,47	20,00	19,08	18,98	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бангладеш (Народная Республика)



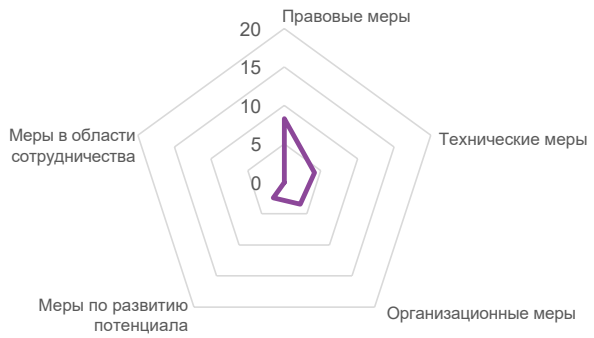
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Развитие потенциала, технические меры
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
81,27	14,86	16,77	16,39	17,03	16,22

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бутан (Королевство)



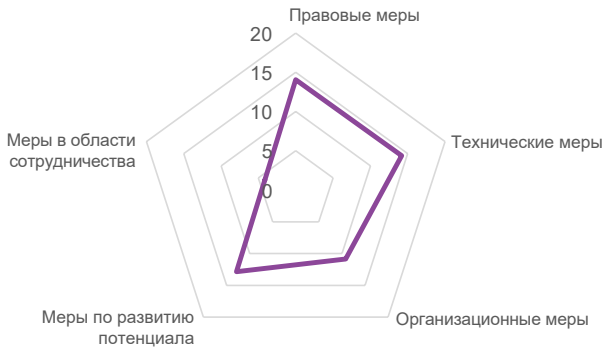
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
18,34	8,30	4,12	3,47	2,45	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бруней-Даруссалам



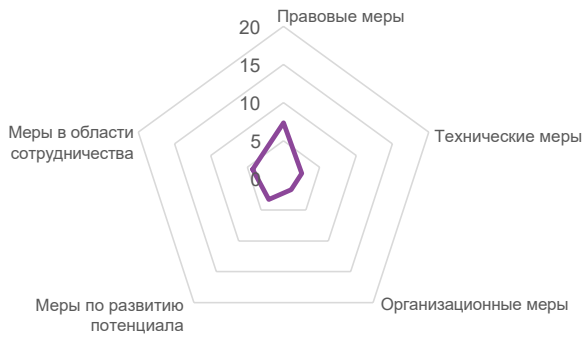
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
56,07	14,06	14,19	10,84	12,85	4,12

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Камбоджа (Королевство)***



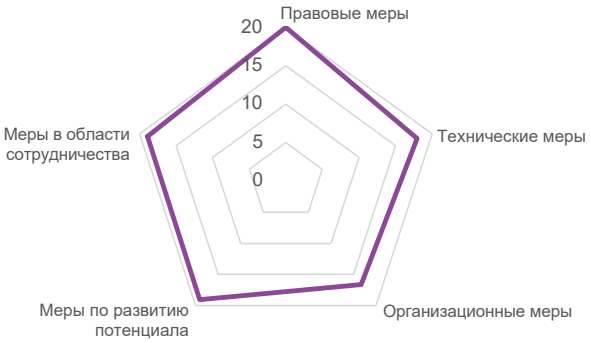
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
19,12	7,38	2,50	1,69	3,29	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Китай (Народная Республика)



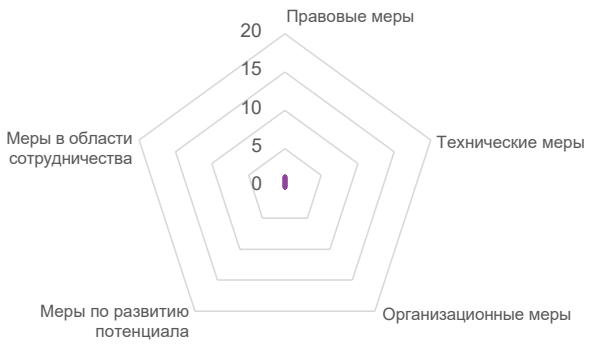
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
92,53	20,00	17,94	16,63	19,04	18,91

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Корейская Народно-Демократическая Республика***



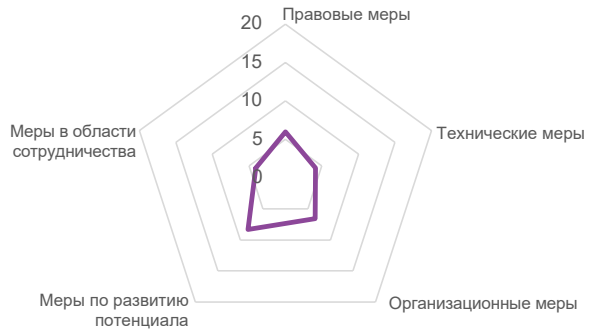
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры, меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
1,35	1,35	0,00	0,00	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Фиджи (Республика)



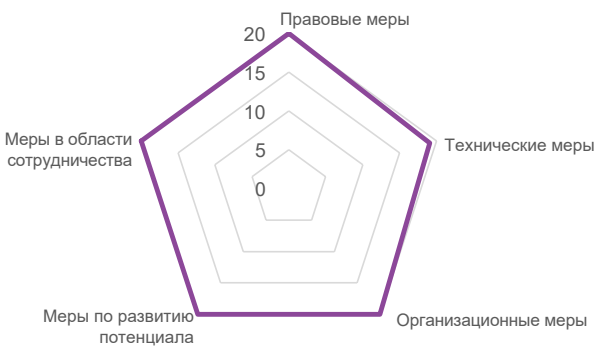
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС)

Относительно сильные стороны
Развитие потенциала
Области возможного роста
Технические меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
29,08	5,99	4,11	6,59	8,31	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Индия (Республика)



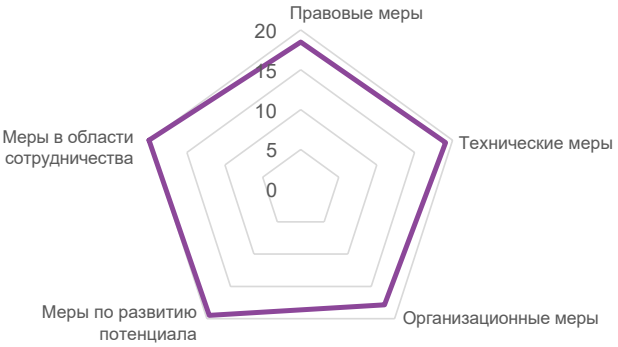
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры, организационные меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,49	20,00	19,08	18,41	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Индонезия (Республика)



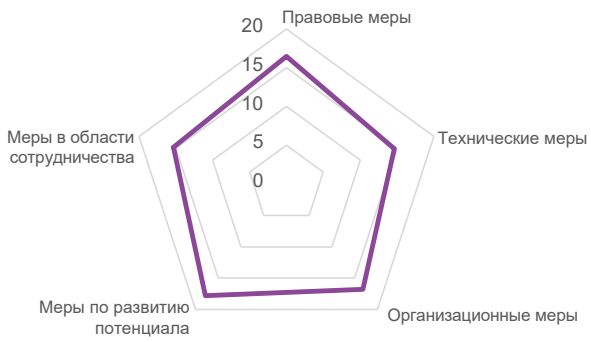
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Меры в области сотрудничества, технические меры, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
94,88	18,48	19,08	17,84	19,48	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Иран (Исламская Республика)



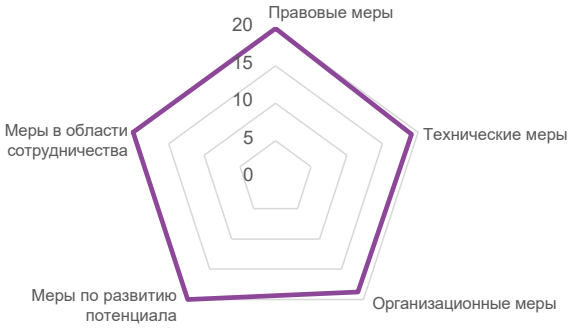
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Развитие потенциала, организационные меры
Области возможного роста
Технические меры, правовые меры, меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
81,06	16,48	14,63	16,82	17,80	15,33

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Корея (Республика)



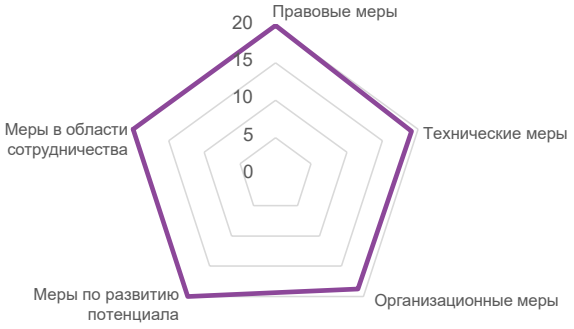
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,52	20,00	19,54	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Япония



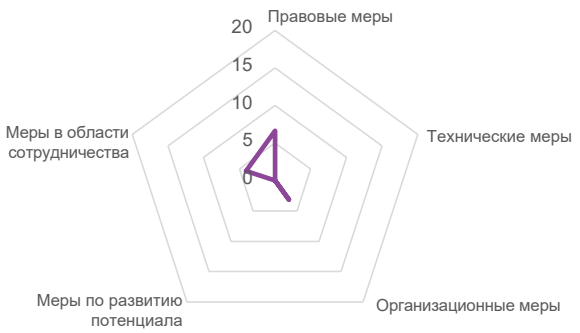
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,82	20,00	19,08	18,74	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кирибати (Республика)



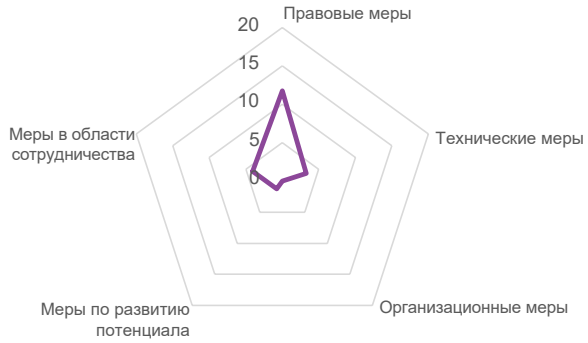
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,84	6,64	0,00	3,13	0,00	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Лаосская Народно-Демократическая Республика



Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
20,34	11,77	3,27	0,00	1,23	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Малайзия

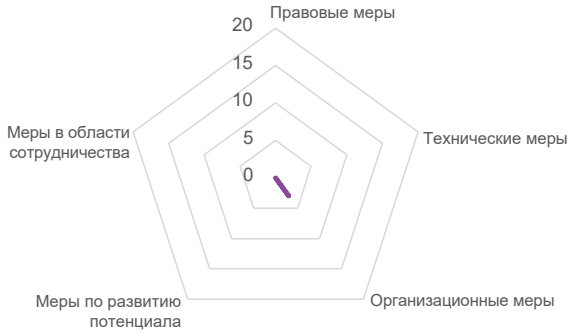
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,06	20,00	19,08	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Мальдивские Острова (Республика)***



Уровень развития
Развивающаяся страна,
малое островное
развивающееся государство
(СИДС)

Относительно сильные стороны
Организационные меры
Области возможного роста
Правовые меры,
технические меры,
меры в области сотрудничества,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
2,95	0,00	0,00	2,95	0,00	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Маршалловы Острова (Республика)***

Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
4,90	0,83	0,00	0,00	0,00	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Микронезия (Федеративные Штаты)**

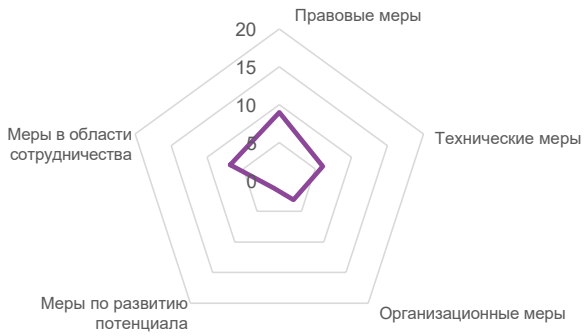
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Данные отсутствуют
Области возможного роста
Данные отсутствуют

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
0	0	0	0	0	0

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Монголия



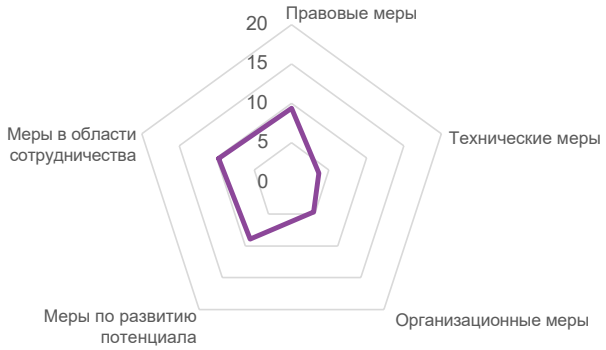
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
26,20	9,00	6,02	3,13	1,23	6,82

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Мьянма (Союз)



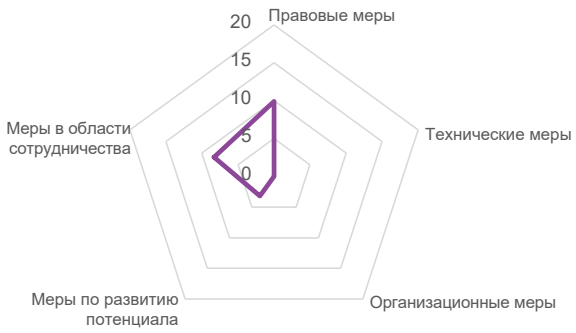
Уровень развития
Развивающаяся страна,
наименее развитая страна (НРС)

Относительно сильные стороны
Меры в области сотрудничества,
правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
36,41	9,39	3,64	4,71	8,92	9,75

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Науру (Республика)***



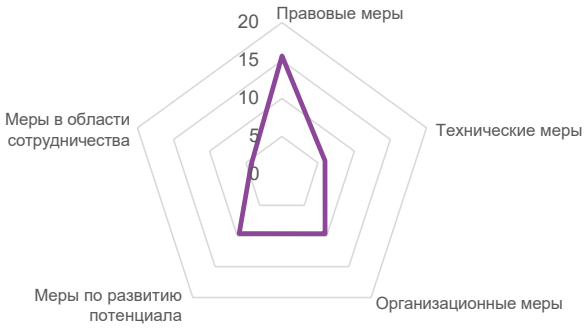
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
21,42	9,91	0,00	0,00	3,18	8,33

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Непал (Федеративная Демократическая Республика)***



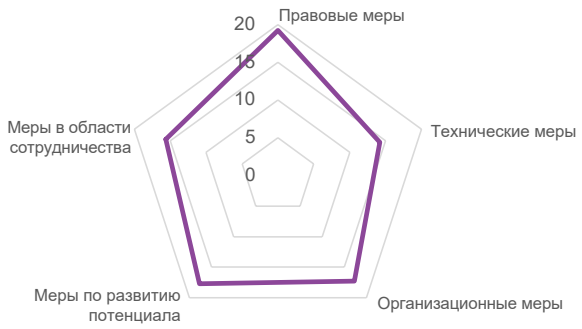
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
44,99	15,61	5,94	9,58	9,60	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Новая Зеландия***



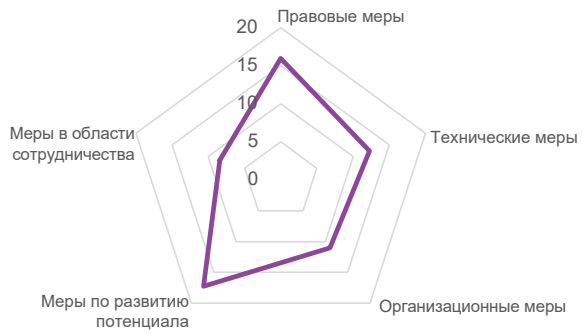
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
84,04	19,24	14,19	17,27	17,71	15,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Пакистан (Исламская Республика)



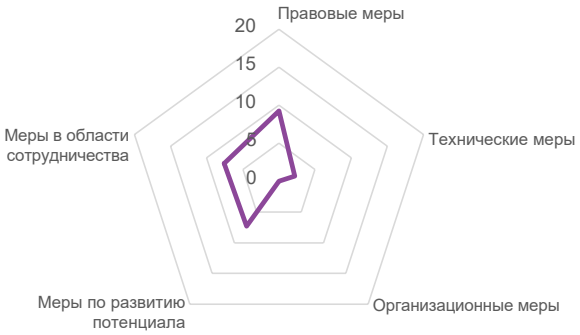
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Развитие потенциала
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
64,88	15,97	12,26	11,01	17,25	8,38

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Папуа – Новая Гвинея***



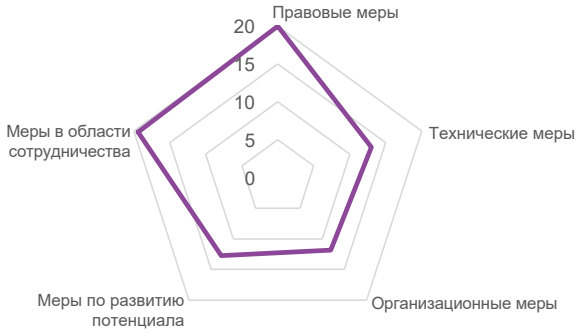
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Развитие потенциала
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
26,33	9,26	2,18	0,00	7,30	7,59

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Филиппины (Республика)



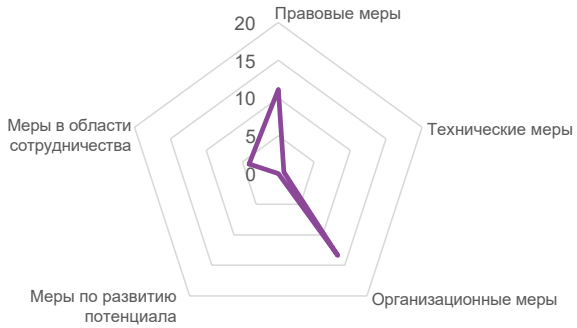
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
77,00	20,00	13,00	11,85	12,74	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Самоа (Независимое Государство)



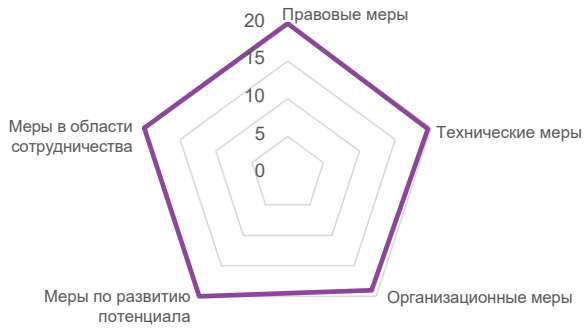
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Организационные меры
Области возможного роста
Развитие потенциала, технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
29,33	11,15	0,73	13,37	0,00	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сингапур (Республика)



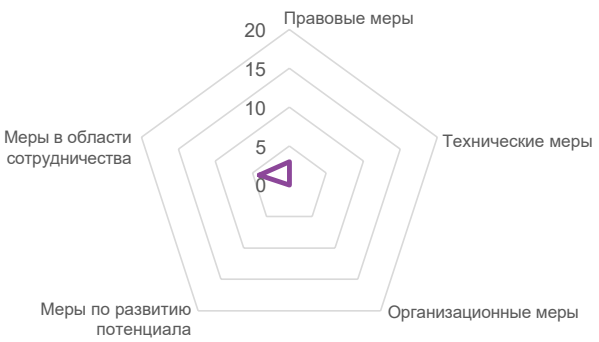
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Правовые меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,52	20,00	19,54	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Соломоновы Острова



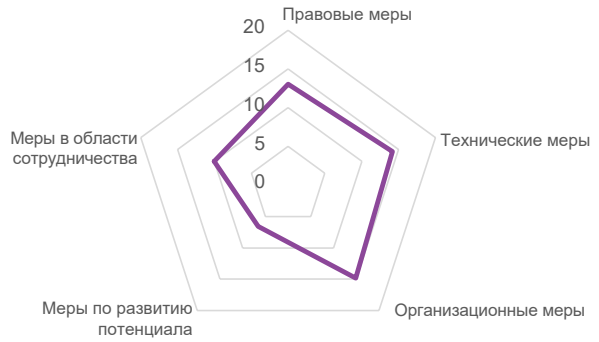
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Мерые в области сотрудничества, правовые меры
Области возможного роста
Технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
7,08	3,00	0,00	0,00	0,00	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Шри-Ланка (Демократическая Социалистическая Республика)



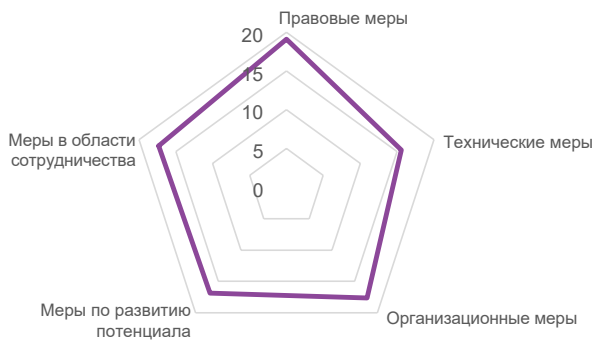
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Организационные меры, технические меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
58,65	13,05	14,15	14,82	6,58	10,04

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Таиланд



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
86,50	19,11	15,57	17,64	16,84	17,34

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Тимор-Лешти (Демократическая Республика)***

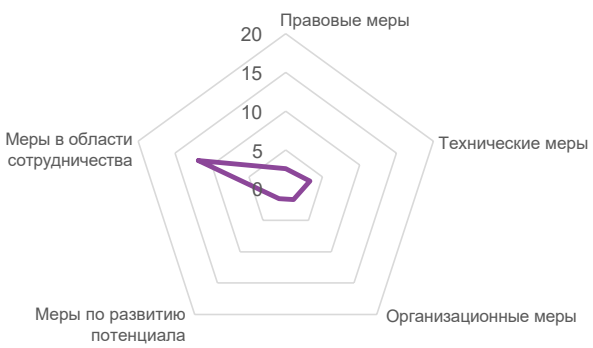
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Правовые меры, технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
4,26	0,00	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Тонга (Королевство)***



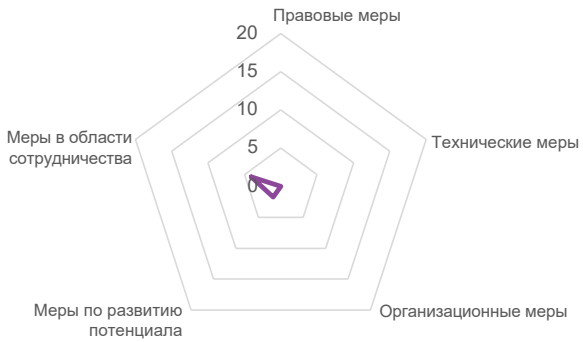
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Развитие потенциала, организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
20,95	2,63	3,27	1,69	1,52	11,85

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Тувалу***



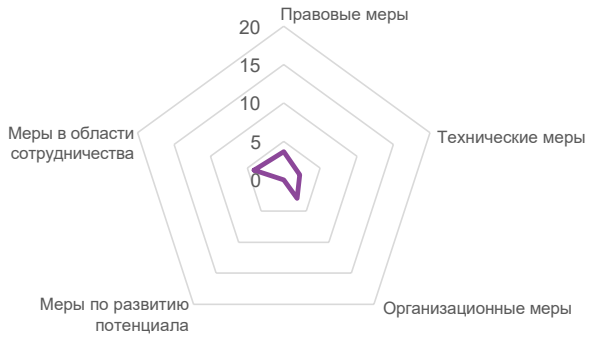
Уровень развития
Развивающаяся страна, наименее развитая страна (НРС), малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Правовые меры, технические меры, организационные меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
5,78	0,00	0,00	0,00	1,71	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Вануату (Республика)



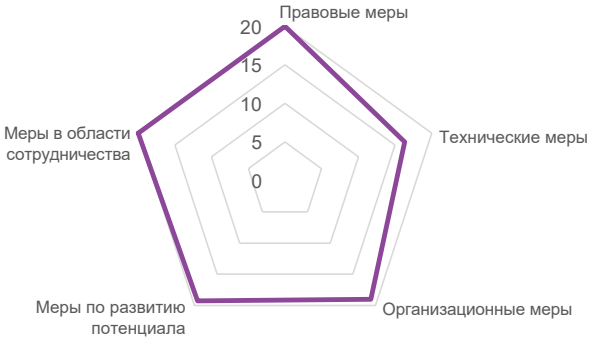
Уровень развития
Развивающаяся страна, малое островное развивающееся государство (СИДС)

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
12,88	3,69	2,18	2,95	0,00	4,07

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Вьетнам (Социалистическая Республика)



Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры, меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
94,55	20,00	16,31	18,98	19,26	20,00

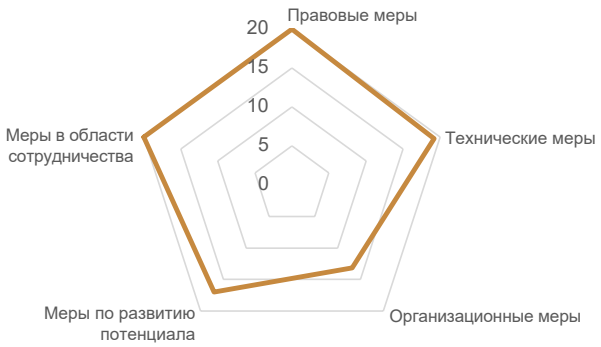
Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Регион Содружества Независимых Государств

Азербайджан (Республика)



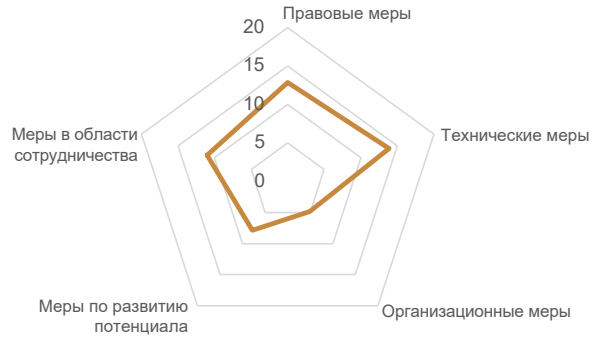
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
89,31	20,00	19,19	13,14	16,99	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Армения (Республика)***



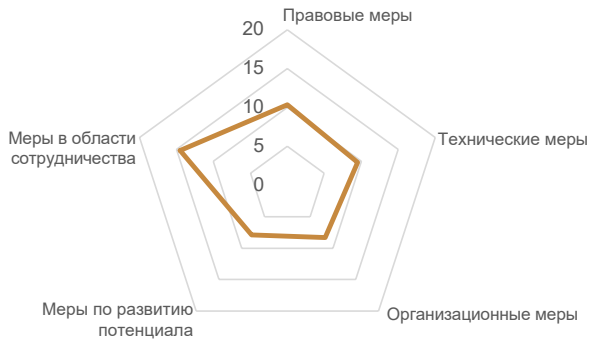
Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
50,47	12,87	13,86	4,87	7,85	11,02

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Беларусь (Республика)



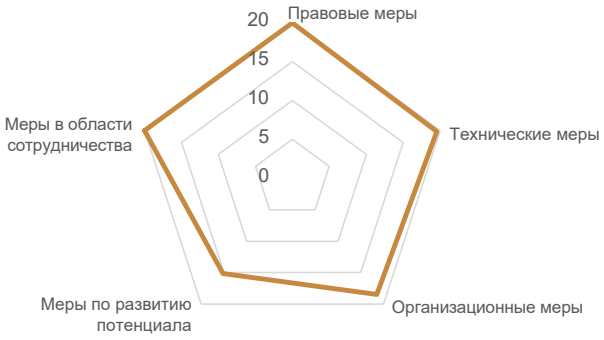
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
50,57	10,36	9,50	8,31	7,88	14,51

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Казахстан (Республика)



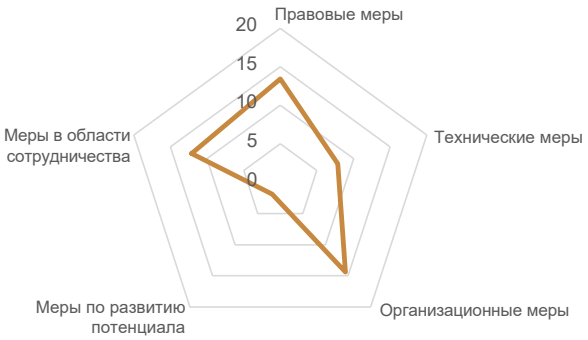
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Меры в области сотрудничества, технические меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
93,15	20,00	19,54	18,46	15,15	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кыргызская Республика



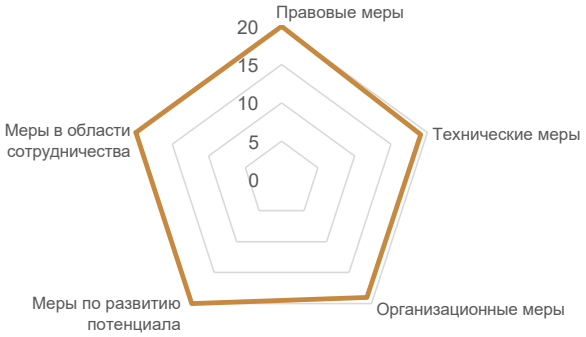
Уровень развития
Развивающаяся страна, страна, не имеющая выхода к морю

Относительно сильные стороны
Организационные меры, правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
49,64	13,43	7,85	14,37	1,87	12,11

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Российская Федерация



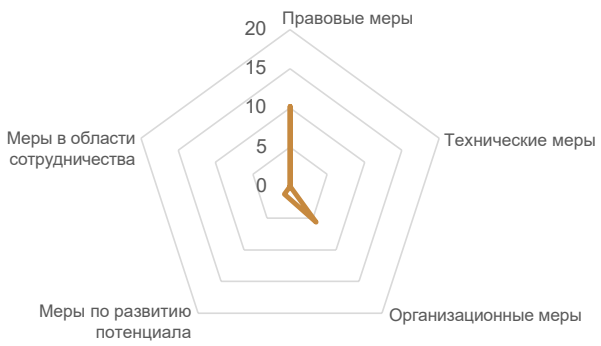
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры, меры в области сотрудничества, развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,06	20,00	19,08	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Таджикистан (Республика)***



Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры,
меры в области сотрудничества

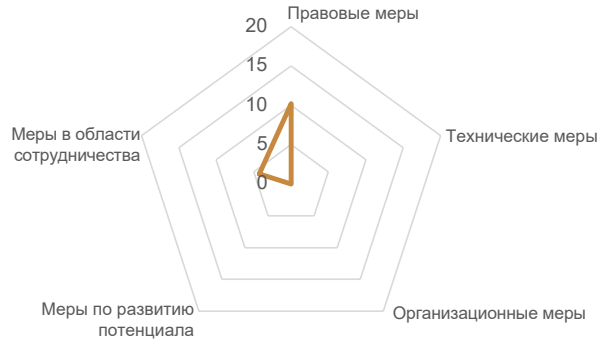
Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
17,10	10,22	0,00	5,63	1,25	0,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

*Туркменистан***



Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры,
организационные меры,
развитие потенциала

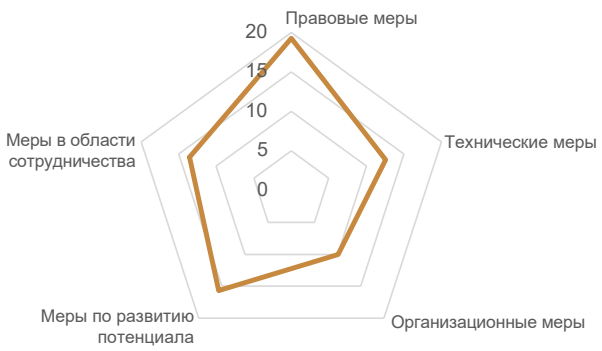
Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
14,48	10,22	0,00	0,00	0,00	4,26

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Узбекистан (Республика)



Уровень развития
Развивающаяся страна,
страна, не имеющая выхода к морю

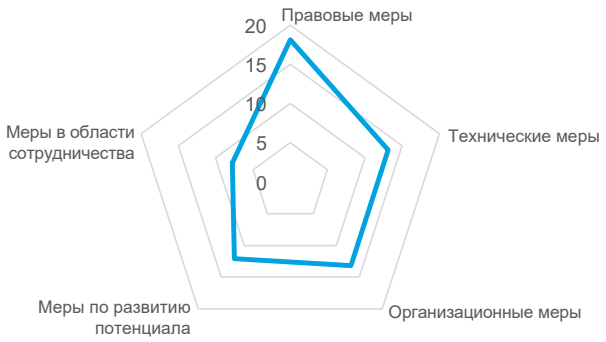
Относительно сильные стороны
Правовые меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Технические меры,
организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
71,11	19,27	12,56	10,05	15,68	13,56

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Европа

Албания (Республика)



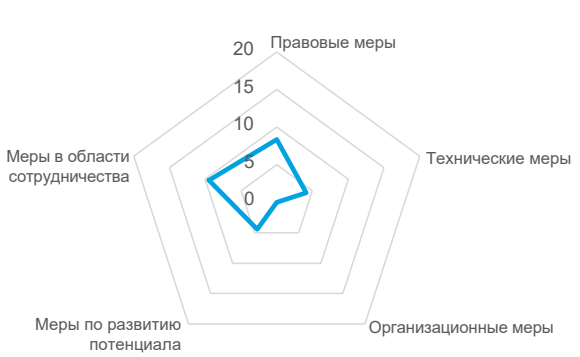
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
64,32	18,13	13,12	13,18	12,12	7,78

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Андорра (Княжество)***



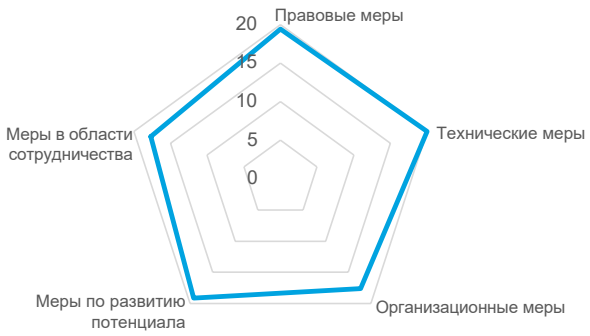
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
26,38	8,37	4,11	0,00	4,41	9,49

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Австрия



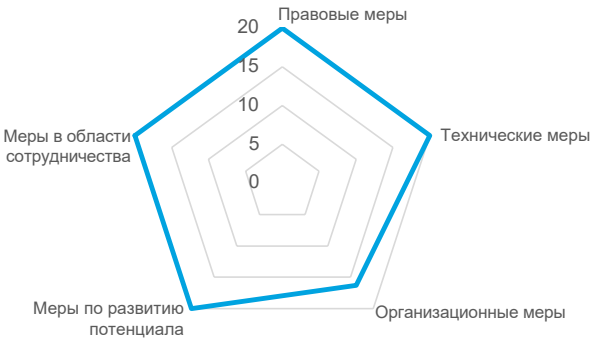
Уровень развития
Развитая страна

Относительно сильные стороны
Технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
93,89	19,43	20,00	17,64	19,13	17,70

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Бельгия



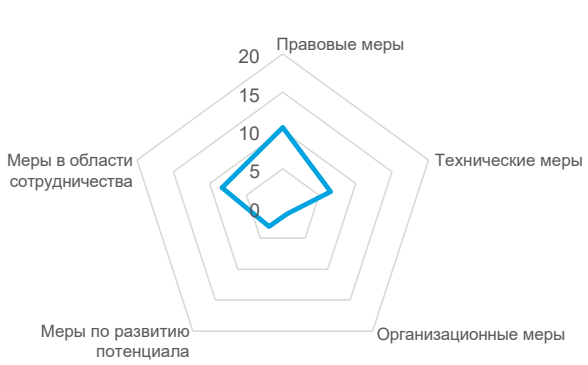
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,25	20,00	20,00	16,25	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Босния и Герцеговина



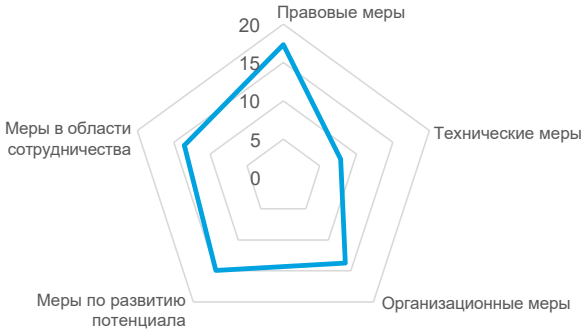
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
29,44	10,41	6,56	1,02	3,12	8,33

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Болгария (Республика)



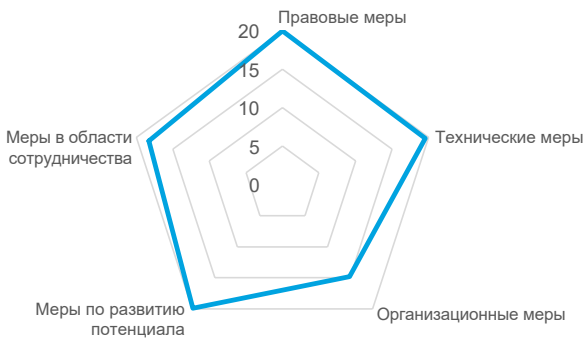
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
67,38	17,34	7,84	13,72	14,92	13,57

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Хорватия (Республика)



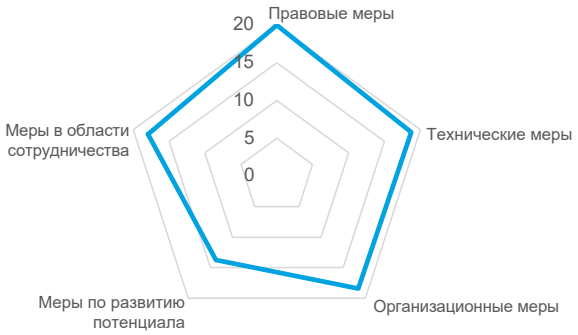
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
развитие потенциала
Области возможного роста
Организационные меры,
технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
92,53	20,00	19,54	14,80	19,89	18,29

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Кипр (Республика)



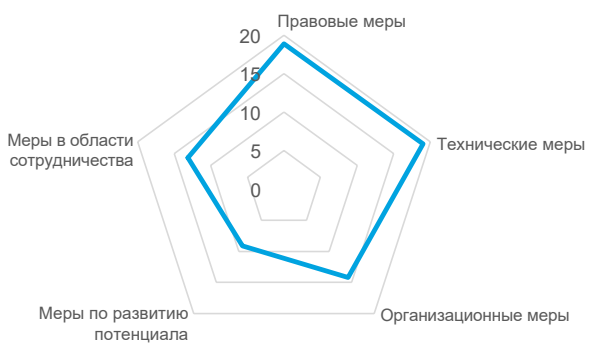
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
88,82	20,00	18,73	18,41	13,73	17,94

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Чешская Республика



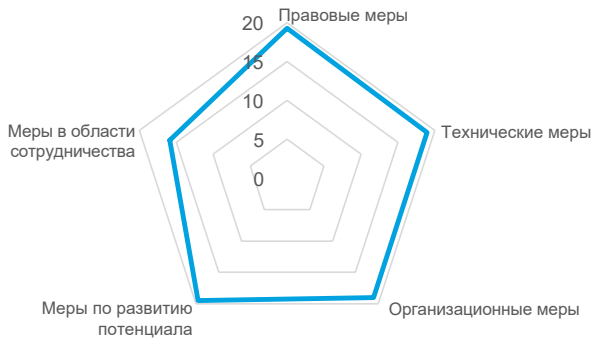
Уровень развития
Развитая страна

Относительно сильные стороны
Технические меры, правовые меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
74,37	18,89	19,00	14,20	9,14	13,14

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Дания



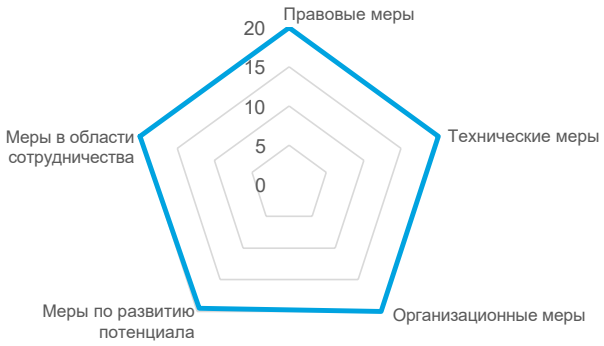
Уровень развития
Развитая страна

Относительно сильные стороны
Развитие потенциала, правовые меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
92,60	19,30	18,94	18,98	19,48	15,89

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Эстония (Республика)



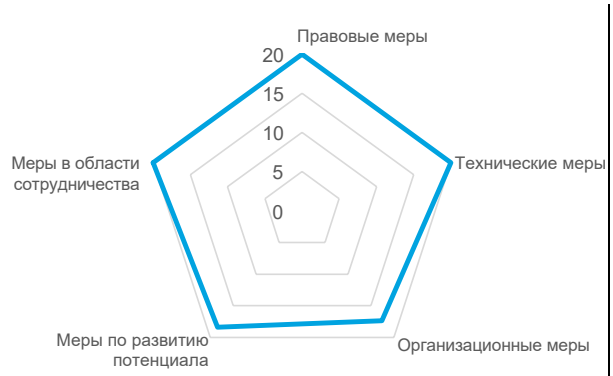
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
99,48	20,00	20,00	20,00	19,48	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Финляндия



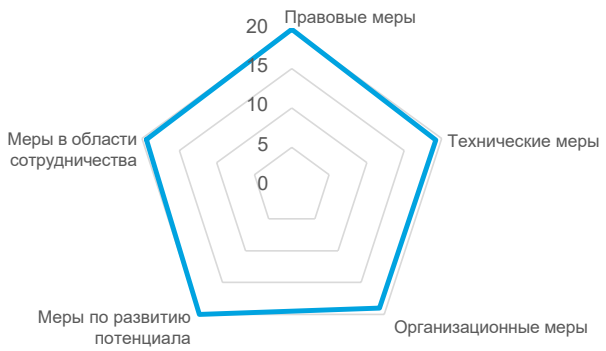
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
92,07	20,00	20,00	14,33	17,74	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Франция



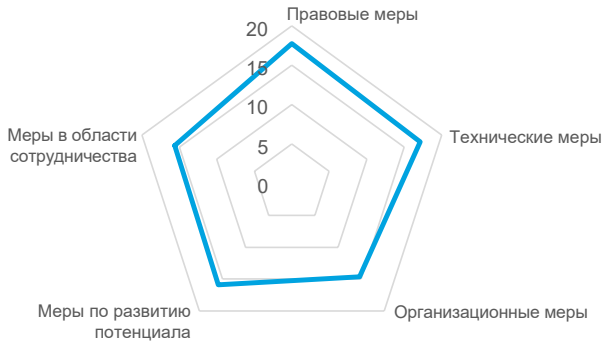
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,60	20,00	19,21	18,98	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Грузия



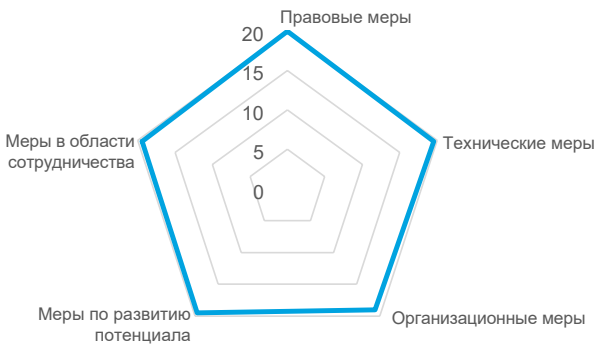
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Меры в области сотрудничества, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
81,07	17,75	17,13	14,67	15,89	15,63

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Германия (Федеративная Республика)



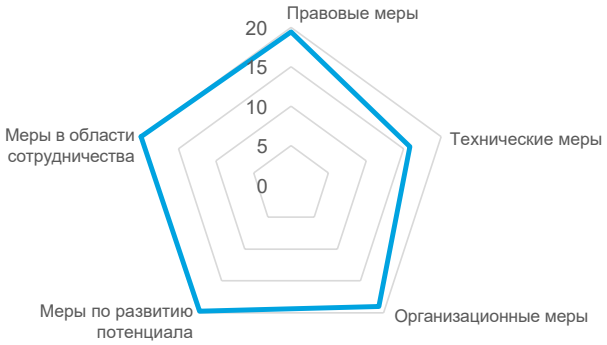
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
развитие потенциала,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,41	20,00	19,54	18,98	19,48	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Греция



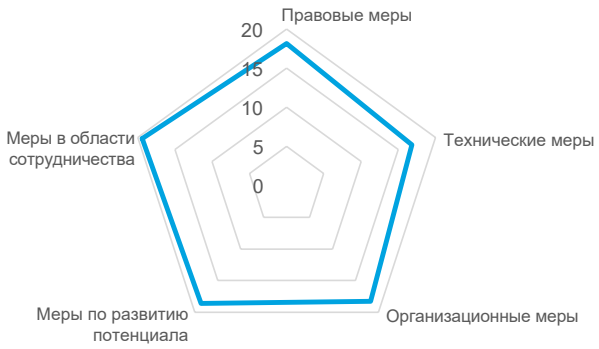
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества,
развитие потенциала,
правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
93,98	19,43	15,83	18,98	19,74	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Венгрия



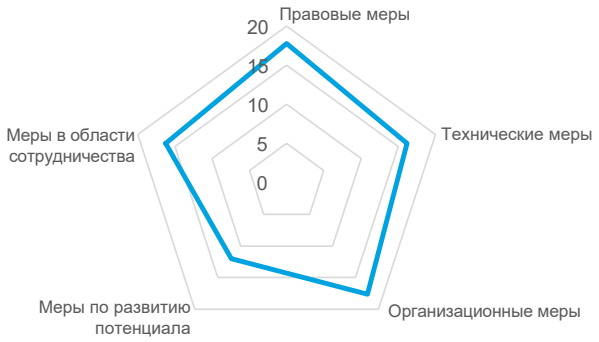
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества, развитие потенциала, правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
91,28	18,16	16,82	18,29	18,60	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Исландия



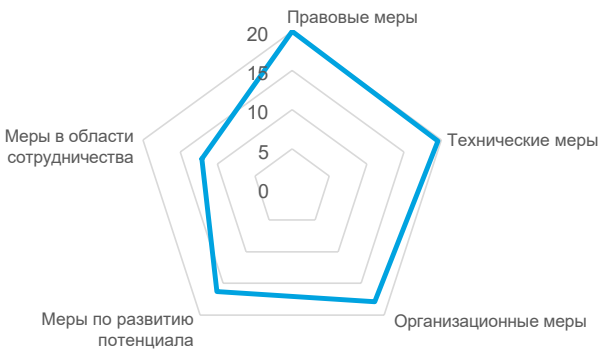
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры, организационные меры
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
79,81	17,78	16,17	17,62	11,99	16,25

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Ирландия



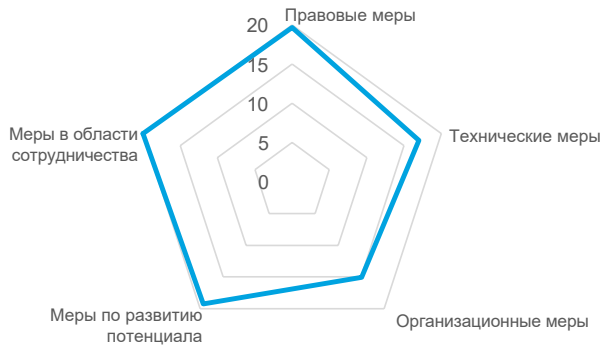
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
85,86	20,00	19,54	17,89	16,32	12,11

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Израиль (Государство)***



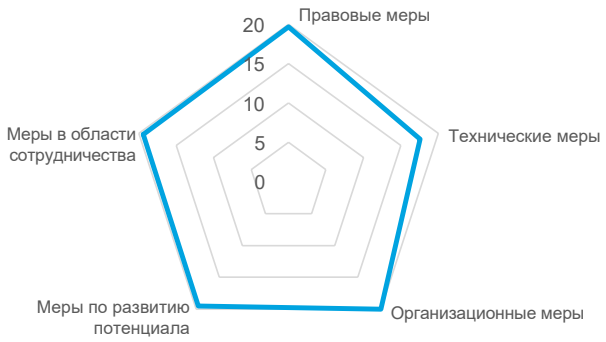
Уровень развития
Развитая страна

Относительно сильные стороны
Технические меры,
развитие потенциала
Области возможного роста
Правовые меры,
организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
90,93	19,68	16,99	15,02	19,24	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Италия



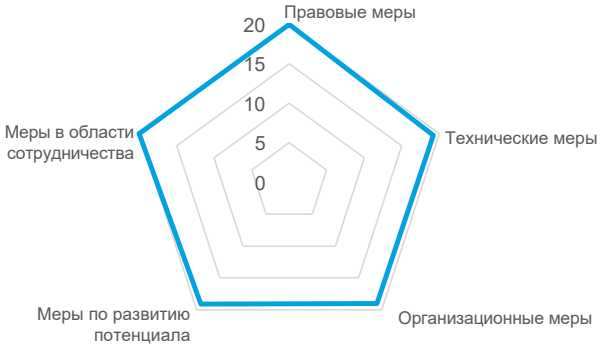
Уровень развития
Развитая страна

Относительно сильные стороны
Организационные меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,13	19,68	17,56	20,00	19,48	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Латвия (Республика)



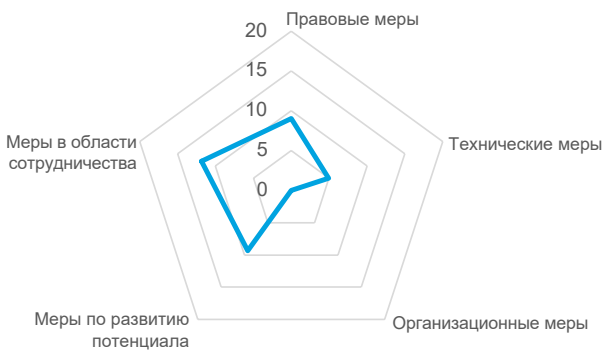
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества,
технические меры,
развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,28	20,00	19,21	18,98	19,09	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Лихтенштейн (Княжество)***



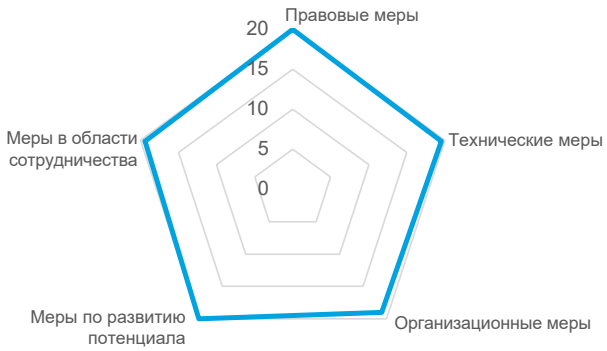
Уровень развития
Развитая страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
35,15	9,04	4,93	0,00	9,34	11,85

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Литва (Республика)



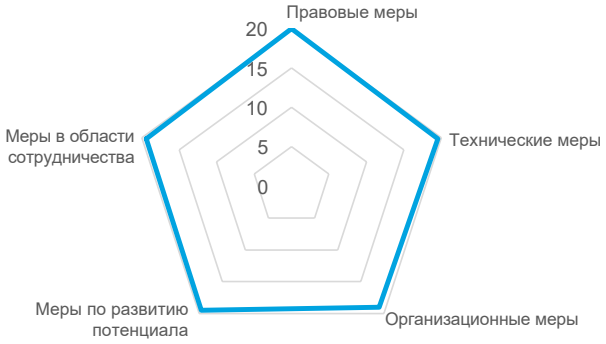
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
развитие потенциала,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,93	20,00	19,54	18,98	20,00	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Люксембург



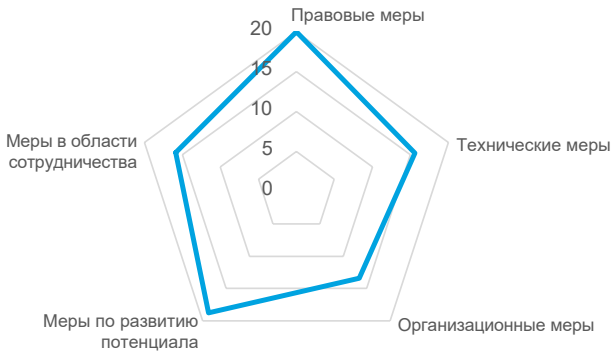
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
развитие потенциала,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,41	20,00	19,54	18,98	19,48	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Мальта



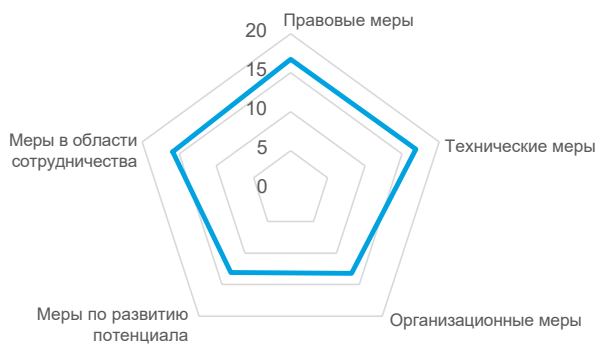
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
83,65	20,00	15,59	13,41	18,76	15,89

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Молдова (Республика)



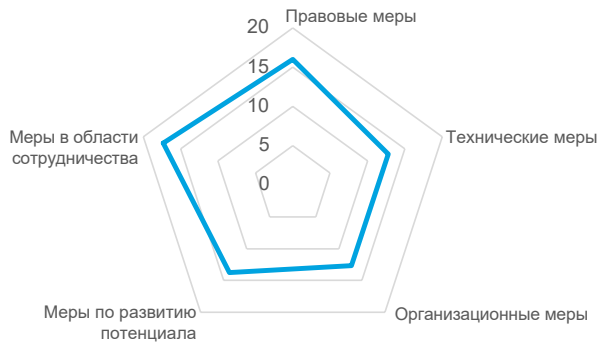
Уровень развития
Развитая страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Технические меры
Области возможного роста
Организационные меры,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
75,78	16,73	16,86	13,21	13,09	15,89

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Монако (Княжество)



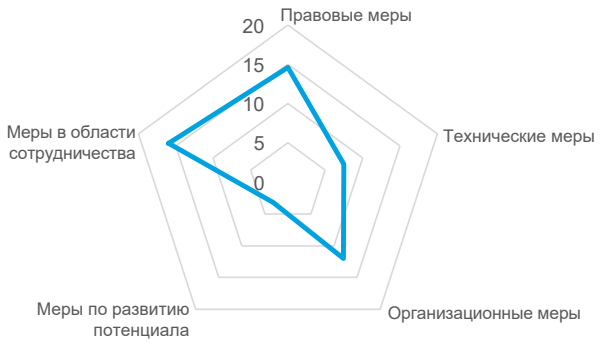
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры,
организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
72,57	16,00	12,77	12,70	13,75	17,34

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Черногория



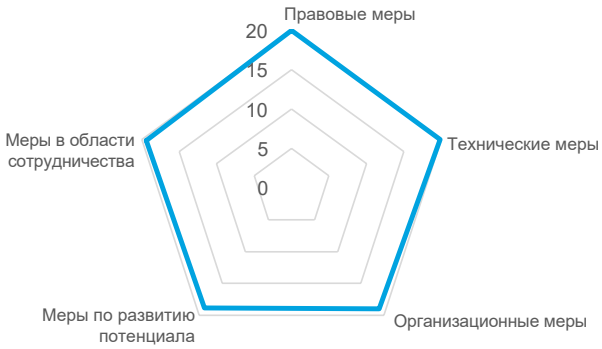
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
53,23	14,61	7,48	12,00	3,18	15,97

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Нидерланды (Королевство)***



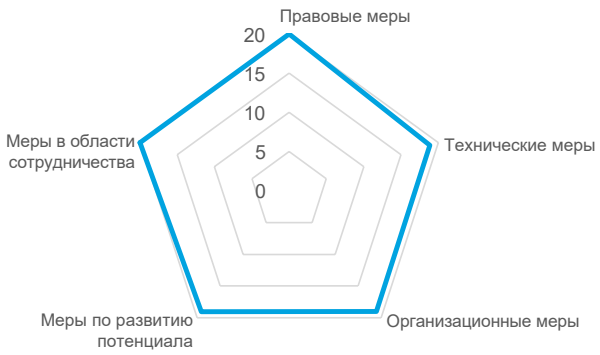
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,05	20,00	19,84	18,98	18,82	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Норвегия***



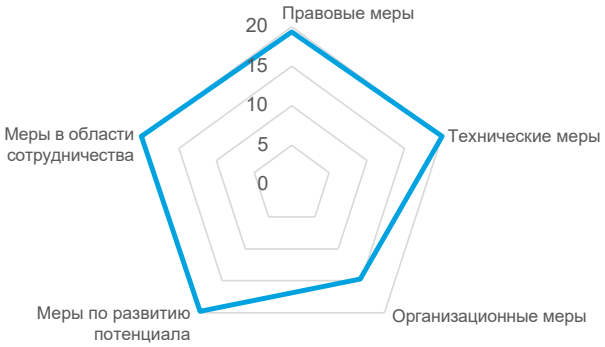
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества
Области возможного роста
Развитие потенциала,
технические меры,
правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
96,89	20,00	18,86	18,98	19,04	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Польша (Республика)



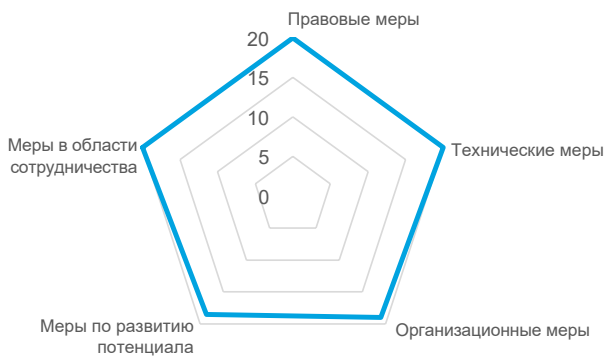
Уровень развития
Развитая страна

Относительно сильные стороны
Технические меры,
меры в области сотрудничества,
правовые меры,
развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
93,86	19,35	20,00	14,74	19,77	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Португалия



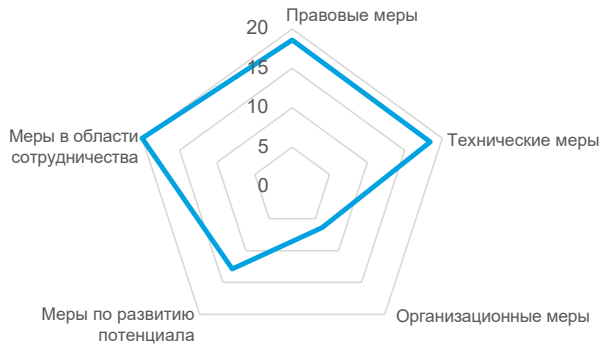
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
технические меры,
меры в области сотрудничества
Области возможного роста
Организационные меры,
развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,32	20,00	20,00	18,98	18,34	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Румыния



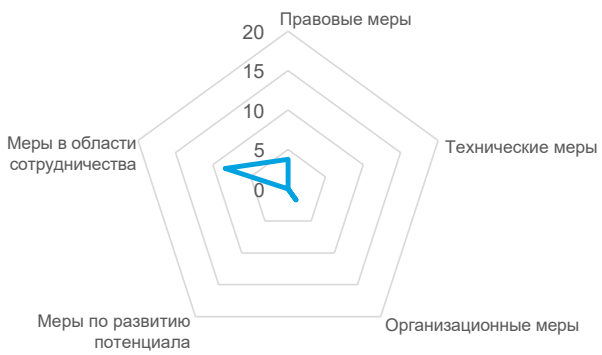
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
76,29	18,60	18,40	6,42	12,88	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сан-Марино (Республика)



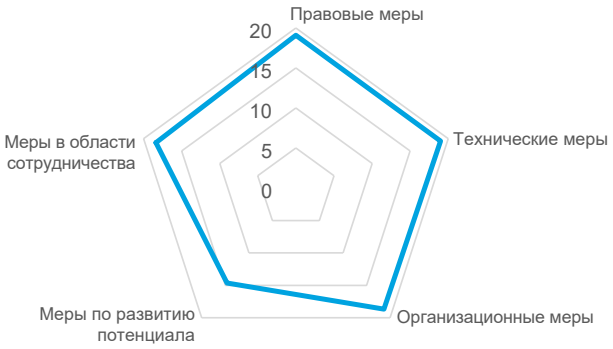
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Технические меры, развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
13,83	3,77	0,00	1,69	0,00	8,37

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Сербия (Республика)



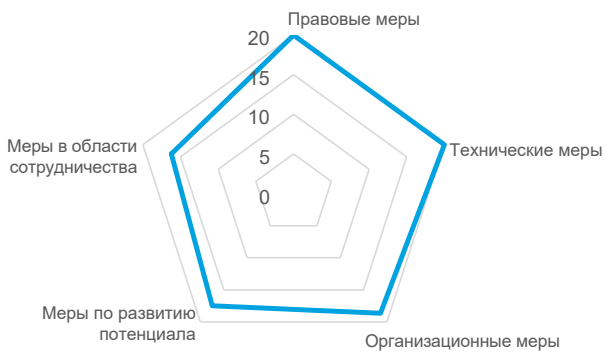
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры, технические меры, организационные меры, меры в области сотрудничества
Области возможного роста
Развитие потенциала

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
89,80	19,10	18,99	18,67	14,66	18,38

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Словацкая Республика



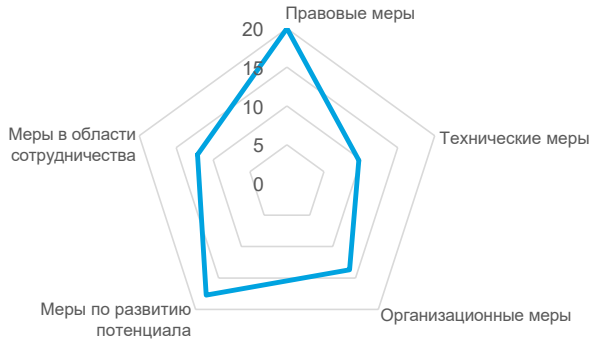
Уровень развития
Развитая страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры,
технические меры
Области возможного роста
Меры в области сотрудничества

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
92,36	20,00	20,00	18,64	17,50	16,22

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Словения (Республика)



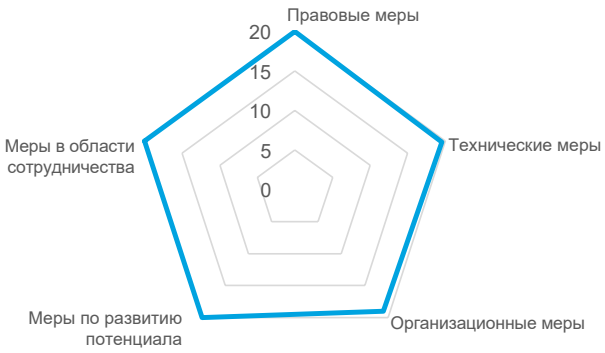
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
73,27	20,00	11,38	13,71	17,72	12,11

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Испания



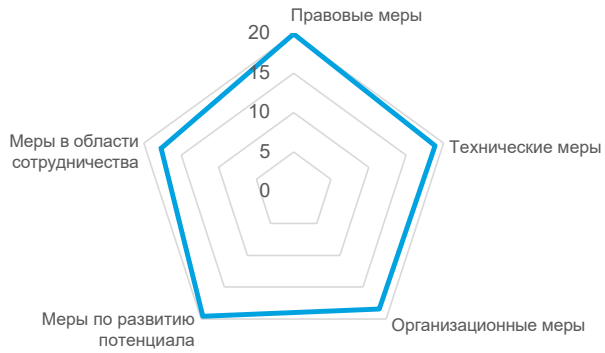
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества,
развитие потенциала,
технические меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
98,52	20,00	19,54	18,98	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Швеция



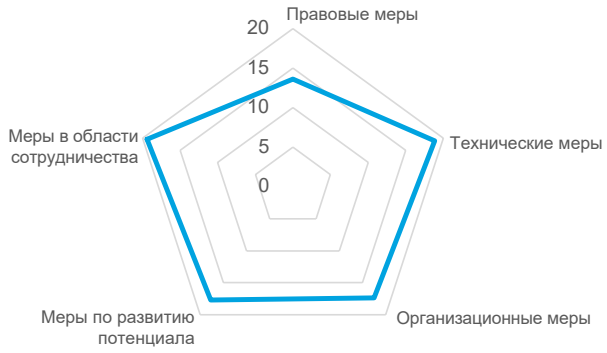
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
94,59	20,00	18,86	18,46	19,57	17,70

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Швейцария (Конфедерация)***



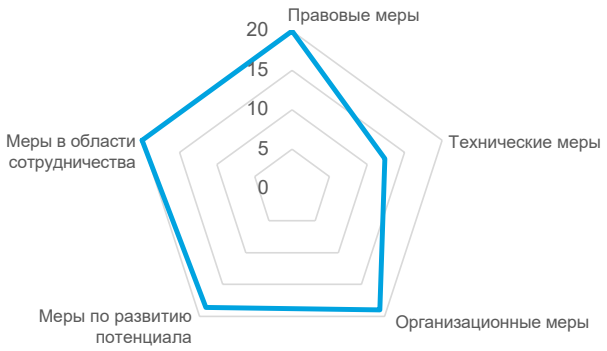
Уровень развития
Развитая страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Технические меры,
меры в области сотрудничества
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
86,97	13,62	18,85	17,40	17,69	19,41

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Северная Македония (Республика)



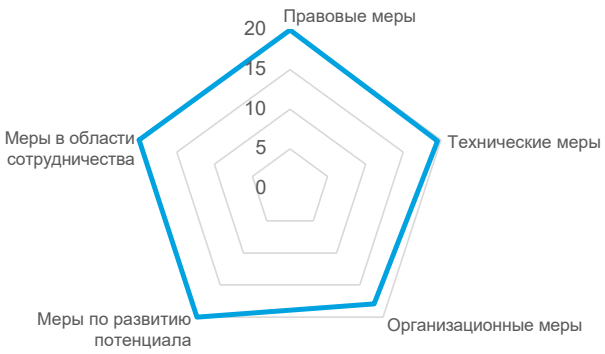
Уровень развития
Развитая страна,
страна, не имеющая выхода к морю

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
89,92	20,00	12,37	18,98	18,57	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Турция



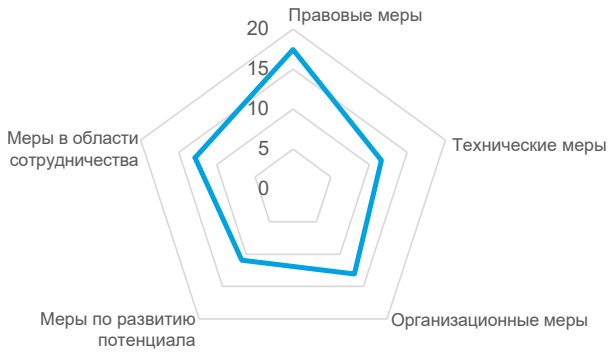
Уровень развития
Развивающаяся страна

Относительно сильные стороны
Правовые меры,
меры в области сотрудничества,
технические меры,
развитие потенциала
Области возможного роста
Организационные меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
97,50	20,00	19,54	17,96	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Украина



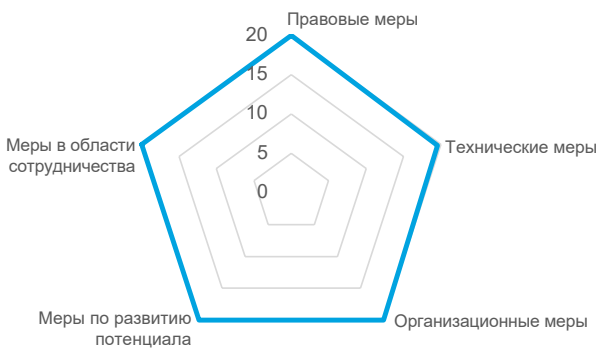
Уровень развития
Развитая страна

Относительно сильные стороны
Меры в области сотрудничества
Области возможного роста
Правовые меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
65,93	17,46	11,60	13,06	10,94	12,87

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

Соединенное Королевство Великобритании и Северной Ирландии



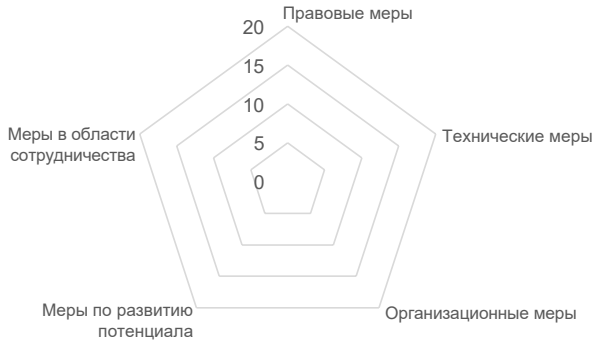
Уровень развития
Развитая страна

Относительно сильные стороны
Правовые меры,
организационные меры,
меры в области сотрудничества,
развитие потенциала
Области возможного роста
Технические меры

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
99,54	20,00	19,54	20,00	20,00	20,00

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

*Ватикан**



Уровень развития
Развитая страна,
страна, не имеющая выхода
к морю

Относительно сильные стороны
Данные отсутствуют
Области возможного роста
Данные отсутствуют

Общая оценка	Правовые меры	Технические меры	Организационные меры	Меры по развитию потенциала	Меры в области сотрудничества
0	0	0	0	0	0

Источник: Глобальный индекс кибербезопасности МСЭ, 4-е издание, 2020 год

** Ответы на вопросник не получены/данные собраны группой GCI.

* Данные отсутствуют.

Глоссарий

Сокращение	Определение на английском языке		Определение на русском языке
CERT	Computer Emergency Response Team, trademarked by Carnegie Mellon University		Группа реагирования на нарушения компьютерной защиты, товарный знак Университета Карнеги–Меллона
CI	Critical Infrastructure		Критически важная инфраструктура
CIRT*	Computer Incident Response Team, *see related terms CSIRTs, CERTs*		Группа реагирования на компьютерные инциденты, *см. соответствующие термины CSIRT, CERT*
CSIRT	Computer Security Incident Response Team		Группа реагирования на инциденты в сфере компьютерной безопасности
DPP	Data and Privacy Protection		Защита данных и неприкосновенности конфиденциальной информации
EU	European Union	ЕС	Европейский союз
GCI-1/2/3/4	The iteration of the Global Cybersecurity Index		Издание Глобального индекса кибербезопасности
GDPR	General Data Protection Regulation (EU)		Общий регламент по защите персональных данных (ЕС)
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
ITU	International Telecommunication Union	МСЭ	Международный союз электросвязи
LDC	Least Developed Countries	НРС	Наименее развитые страны
LLDCs	Landlocked Developed Countries	ЛЛДС	Развитые страны, не имеющие выхода к морю
MLAT	Mutual Legal Assistance Treaty		Договор о взаимной правовой помощи
MSMEs	Micro, small, and medium-sized enterprise	ММСП	Микро-, малые и средние предприятия
NCS	National Cybersecurity Strategy	НСК	Национальная стратегия кибербезопасности
NGO	Non-Government Organization	НПО	Неправительственная организация
ODC	Other Developing Countries		Прочие развивающиеся страны
OT	Operational Technology		Операционная технология
PPP	Public Private Partnership	ГЧП	Государственно-частное партнерство
SIDS	Small Island Development States	СИДС	Малые островные развивающиеся государства
SME	Small and medium-sized enterprises	МСП	Малые и средние предприятия
UN	United Nations	ООН	Организация Объединенных Наций

Приложение A. Методика

A1 Сфера применения и структура GCI

Полномочия на введение Глобального индекса кибербезопасности (GCI) вытекают из Резолюции 130 Полномочной конференции МСЭ (Пересм. Дубай, 2018 год) об усилении роли МСЭ в укреплении доверия и безопасности при использовании информационно- коммуникационных технологий (ИКТ). В частности, странам предлагается "*поддерживать инициативы МСЭ в области кибербезопасности, включая введение Глобального индекса кибербезопасности (GCI), с тем чтобы содействовать осуществлению государственных стратегий и обмену информацией о деятельности, проводимой в отраслях и секторах*". Цель GCI – способствовать формированию глобальной культуры кибербезопасности и превращению ее в один из основных элементов ИКТ.

Таблица A1. Участие в работе над Глобальным индексом кибербезопасности и периоды сбора данных

	GCI-1	GCI-2	GCI-3	GCI-4
Количество стран, предоставивших координаторов	105	136	155	169
Период сбора данных	2013–2014 годы	2016 год	2017–2018 годы	2020 год
Год публикации	2015 год	2017 год	2019 год	2021 год

GCI составлен на основе данных, предоставленных членами МСЭ, в том числе частными лицами, экспертами и организациями отрасли в качестве вносящих вклад партнеров (Австралийский институт стратегической политики, Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Университет Гренобля (Франция), Университет штата Индиана, Интерпол, Арабский региональный центр кибербезопасности МСЭ в Омане, Управление интернета и безопасности Кореи, Национальный регуляторный орган электросвязи (NTRA) Египта, группа Red Team Cyber, Потомакский институт политических исследований, ЮНИКРИ, Технологический университет Ямайки, УНП ООН и Всемирный банк).

Сфера применения GCI

Глобальный индекс кибербезопасности (GCI) – это сводный набор показателей, совершенствующийся в каждом издании, который позволяет отслеживать степень приверженности стран обеспечению кибербезопасности по пяти компонентам Глобальной программы кибербезопасности (ГПК). Его основная задача заключается в оценке:

- типа, уровня и изменения во времени обязательств по обеспечению кибербезопасности в отдельных странах и в сравнении с другими странами;
- хода работы по обязательствам стран в области кибербезопасности в глобальной перспективе;
- хода работы по обязательствам в области кибербезопасности в региональной перспективе;
- разрыва в приверженности обязательствам по обеспечению кибербезопасности (то есть различий между странами с точки зрения их участия в инициативах по кибербезопасности).

Цель GCI – помочь странам определить направления совершенствования в области обеспечения кибербезопасности и побудить их к работе в этих направлениях. Это также позволит повысить общую степень приверженности обязательствам по обеспечению кибербезопасности во всем мире, поможет согласовать практические приемы и будет способствовать формированию культуры кибербезопасности на глобальном уровне. GCI призван проиллюстрировать примеры успешных усилий в области обеспечения кибербезопасности, которые могут быть использованы в качестве примеров передовой практики и руководства к действию для стран со схожими национальными условиями.

A2 Программа сотрудничества в области кибербезопасности МСЭ

Кибербезопасность – это мультидисциплинарная область, и ее освоение затрагивает все секторы, отрасли и заинтересованные стороны как по вертикали, так и по горизонтали. Чтобы ускорить развитие национального потенциала, необходимо приложить определенные усилия в политической, экономической и социальной сферах. Это можно осуществить силами правоохранительных и судебных органов, образовательных учреждений, министерств, предприятий частного сектора, разработчиков технологий, государственно-частных партнерств, а также в рамках внутригосударственного сотрудничества.

Программа многостороннего международного сотрудничества в области обеспечения кибербезопасности МСЭ направлена на достижение синергизма между текущими и будущими инициативами и сосредоточена на следующих пяти компонентах, которые служат неотъемлемыми составляющими национальной культуры кибербезопасности.

Таблица A2. Описание основных компонентов GCI 2020 года

Правовые меры	
	Меры, основанные на существовании нормативно-правовой базы в отношении кибербезопасности и киберпреступности.
	Правовые меры (включая законодательство, регламентарные положения и законы о сдерживании спама) позволяют государству создавать базовые механизмы реагирования посредством расследования и судебного преследования преступлений, а также наложения санкций за несоблюдение или нарушение закона. Нормативно-правовая база устанавливает минимальную поведенческую платформу, на которой могут быть основаны дополнительные меры по обеспечению кибербезопасности. По сути цель состоит в том, чтобы разработать законодательство, достаточное для согласования практики применения на региональном/международном уровне и упрощения международных усилий по борьбе с киберпреступностью.
Технические меры	
	Меры, основанные на существовании технических организаций и структуры, отвечающих за обеспечение кибербезопасности.
	ИКТ могут эффективно развиваться и применяться лишь в атмосфере доверия и безопасности. Поэтому странам необходимо разработать и внедрить общепринятые минимальные критерии безопасности и схемы сертификации для приложений и систем программного обеспечения. Эти усилия необходимо дополнить созданием национального органа по реагированию на киберинциденты, авторитетного государственного органа и национальной структуры для наблюдения, предупреждения инцидентов и принятия соответствующих ответных мер.
Организационные меры	
	Меры, основанные на существовании координационных центров, политики и стратегий повышения кибербезопасности на национальном уровне.
	К организационным мерам относятся определение целей и стратегических планов обеспечения кибербезопасности, а также формальное определение институциональных ролей, обязанностей и ответственности за их выполнение. Эти меры незаменимы для поддержки разработки и реализации эффективной политики обеспечения кибербезопасности. Государство должно установить общие стратегические цели и задачи, а также всеобъемлющий план их достижения, обеспечения выполнения и измерения. Необходимы национальные учреждения для реализации стратегии и оценки результатов. Без национальной стратегии, модели управления и надзорного органа действия в разных секторах вступают в противоречие друг с другом, что препятствует достижению эффективного согласования усилий по повышению кибербезопасности.

Таблица A2. Описание основных компонентов GCI 2020 года (окончание)

Меры по развитию потенциала	
	Меры, основанные на наличии программ исследований и разработок, образования и обучения, подготовки сертифицированных специалистов, а также государственных институтов, способствующих развитию потенциала.
	К мерам по развитию потенциала относятся кампании по повышению осведомленности населения, программы сертификации и аккредитации специалистов по кибербезопасности, курсы профессиональной подготовки по кибербезопасности, образовательные программы или учебные планы и т. д. Этот компонент является неотъемлемой частью первых трех составляющих (правовой, технической и организационной). Несмотря на многочисленные социально-экономические и политические последствия, кибербезопасность чаще всего рассматривается с технической точки зрения. Развитие кадрового и институционального потенциала имеет важное значение для повышения осведомленности, накопления знаний и ноу-хау во всех секторах, для выработки соответствующих решений системного характера и для содействия подготовке квалифицированных специалистов.
Меры в области сотрудничества	
	Меры, основанные на партнерских отношениях, механизмах сотрудничества и сетях обмена информацией.
	Ввиду беспрецедентного уровня взаимосвязи между государствами обеспечение кибербезопасности – это общая ответственность и транснациональная задача. Более широкое сотрудничество позволит разработать гораздо более мощные средства обеспечения кибербезопасности, помогая снизить киберриски и повысить эффективность расследований, гарантируя задержание и судебное преследование злоумышленников.

A3 Основные изменения по каждому компоненту

Правовые меры

Этот компонент позволяет оценить юридические действия по обеспечению кибербезопасности; он был обновлен для лучшего отражения положений национального материального права, связанных с кибербезопасностью.

- Согласно рекомендациям Консультационной группы БРЭ, в Глобальном индексе кибербезопасности больше не учитывается процессуальное право. Вместо этого внесена большая ясность в некоторые вопросы, включая вопросы о краже персональных данных, онлайновых домогательствах и расизме.
- Вопросы, относящиеся к правовым мерам, изначально были разработаны в соответствии с рекомендациями конвенций, таких как Будапештская конвенция о киберпреступности. Однако теперь ответы сосредоточены на освещении только принятых национальных законов, а сведения о ратификации подобных конвенций больше не собираются. Тем не менее, учитывая влияние международных конвенций и их роль в принятии имеющих юридическую силу обязательств, такие международные конвенции, как Будапештская конвенция, теперь оцениваются как международная деятельность в рамках мер в области сотрудничества.
- Поскольку роль онлайновой среды в человеческой деятельности становится все более значимой, для создания вызывающего доверие киберпространства, способствующего достижению разнообразия и охвату цифровыми технологиями, требуется изучение таких вопросов, как защита конфиденциальности, а также таких проблем, как домогательство, запугивание, соблазнение, детская порнография и расизм. В настоящее издание Глобального индекса кибербезопасности добавлены вопросы по этим проблемам.

Технические меры

Технический компонент реструктурирован, чтобы лучше отражать принцип работы CIRT, в том числе:

- группы реагирования на компьютерные инциденты – правительственные и национальные CIRT – объединены в один показатель;
- сертификация CIRT – важный элемент для оценки способности справляться с киберинцидентами. Для оценки уровня зрелости национальных CIRT[1] добавлена схема сертификации SIM3. SIM3 используется в схеме сертификации TF-CSIRT/Trusted Introducer в качестве основы для оценки и выявления "сертифицированных" участников с наивысшим уровнем зрелости. Модели зрелости потенциала в области безопасности для CIRT будут более углубленно изучаться в будущих изданиях Глобального индекса кибербезопасности.

Организационные меры

- Поскольку деятельность по обеспечению кибербезопасности – это процесс, осуществляемый на постоянной основе, странам рекомендуется регулярно (не реже чем каждые пять лет) пересматривать национальные стратегии кибербезопасности, чтобы оценить, остается ли НСК актуальной с учетом меняющейся оценки рисков и отражает ли она национальные цели, а также понять, какие требуются корректировки. На основании этой рекомендации страны, не подтвердившие или не обновившие свои НСК за последние пять лет, получали пониженную оценку показателей НСК.
- Разработка механизмов защиты ребенка в онлайновой среде должна находиться среди жизненно важных приоритетов стран, особенно когда пандемия COVID-19 вынуждает детей учиться в онлайновом формате. Хотя интернет предоставляет значительные преимущества с точки зрения образования и развития детей, следует также помнить о рисках, которым подвергаются дети в онлайновой среде. В большинстве стран реализуются инициативы в поддержку защиты ребенка в онлайновой среде такими средствами, как создание веб-сайтов и социальных сетей со специальными учебными материалами, информирующими играми и руководствами для детей, родителей и педагогов. Чтобы провести различие между мерами индивидуального характера и мерами, интегрированными в более общую определенную стратегию, за последние давались максимальные оценки, в то время как страны, проводящие единичные или нерегулярные инициативы, получали пониженные оценки.

Меры по развитию потенциала

Показатели этого компонента оставались неизменными со второго издания GCI. Рамки настоящего издания расширены, с тем чтобы оно включало в себя больше информации по вопросу о государственной поддержке малых и средних предприятий (МСП), поскольку они играют важную роль в качестве участников цифровой экономики и цепочек поставок; с учетом происходящего перехода к электронной торговле МСП нуждаются в поддержке по управлению киберрисками.

Меры в области сотрудничества

Этот компонент отражает наличие подписанных или ратифицированных соглашений независимо от того, являются ли они юридически обязывающими. Было уточнено, какие именно соглашения относятся к двусторонним и к многосторонним. Будапештская конвенция, которая ранее считалась многосторонним соглашением, теперь относится к международной деятельности.

A4 Методика расчетов

Вопросник, используемый для GCI, позволяет определить значение 20 показателей на основе ответов на 82 вопроса. Таким образом достигается необходимый уровень детализации и повышается точность и качество ответов. Показатели приведены в вопроснике GCI (Приложение B).

[1] CIRT, или CSIRT/CERT, – специальные организационные структуры, отвечающие за координацию и поддержку мер реагирования на события или инциденты, связанные с компьютерной безопасностью, на национальном уровне.

Показатели, используемые для расчета GCI, выбирались с учетом:

- соответствия пяти компонентам GCI;
- соответствия основным целям и концептуальной структуре GCI;
- доступности и качества данных; и
- возможности перекрестной проверки по вторичным данным.

GCI базируется на карте развития кибербезопасности, которую страна может принять во внимание в процессе укрепления своей приверженности обеспечению кибербезопасности. Вопросник построен на основе пяти различных компонентов, помеченных пятью разными цветами. Глубина контура на диаграммах настоящего отчета указывает на более высокий уровень выполнения обязательств в области кибербезопасности.

В этом отчете представлены региональные и общемировые тенденции. Для обеспечения точности страны должны были подкреплять свой ответ загрузкой или указанием URL-адреса подтверждающих документов. В каждом разделе предусмотрено поле для комментариев, чтобы страны могли поделиться передовым опытом, рассказывая о своих достижениях в области кибербезопасности.

Странам предлагались два или три варианта ответов на 82 вопроса по 20 показателям в рамках пяти компонентов, а раздел комментариев использовался для детализации описания стадии реализации в том случае, если элемент списка находится на стадии проекта или реализации.

Возвращенные вопросники прошли две проверки двумя разными валидаторами; если ответ относился к проекту или к стадии реализации или если он не содержал конкретных ответов на все элементы, входящие в вопрос, проставлялась пониженная оценка. Такой трехступенчатый режим оценки позволил избежать необоснованных и предвзятых оценок благодаря таблице конкретных элементов, которые должны присутствовать в ответе для получения положительной или пониженной оценки.

С этой целью в октябре 2019 года Секретариат БРЭ представил четвертое издание вопросника Глобального индекса кибербезопасности и всю сопутствующую документацию собранию Группы Докладчика по Вопросу 3 2-й Исследовательской комиссии, которое утвердило вопросник. В марте 2020 года на собрании ИК2 БРЭ обновило статус Вопроса 3 и предложило странам назначить экспертов по кибербезопасности для участия в процессе расчета весовых коэффициентов.

Общая последовательность операций в рамках процесса GCI

1. Всем Государствам – Членам МСЭ и Государству Палестина направляется письмо-приглашение, в котором им сообщается об инициативе и предлагается назначить координатора, ответственного за сбор всех соответствующих данных и заполнение онлайнового вопросника GCI. В ходе онлайнового обследования МСЭ официально предлагает утвержденному координатору заполнить вопросник.
2. Сбор первичных данных (для стран, не представивших ответы на вопросник):
    - МСЭ разрабатывает первоначальный проект ответов на вопросник, используя общедоступные данные и онлайн-исследования;
    - проект вопросника направляется на рассмотрение координаторам;
    - координаторы вносят уточнения и возвращают проект вопросника;
    - исправленный проект вопросника рассылается во все координационные центры для окончательного утверждения;
    - утвержденный вопросник используется для анализа, оценки и ранжирования.
3. Сбор вторичных данных (для стран, представивших ответы на вопросник):
    - МСЭ выявляет все недостающие ответы, подтверждающие документы, ссылки и т. д.;
    - координатор по мере необходимости вносит уточнения в ответы;

- исправленный проект вопросника рассылается во все координационные центры для окончательного утверждения;
- утвержденный вопросник используется для анализа, оценки и ранжирования.

Примечание. – Если страна не назначила координатора для заполнения вопросника GCI, то МСЭ устанавливает контакт с институциональным координатором, указанным в Общем справочнике МСЭ.

Весовые коэффициенты

В отличие от предыдущих изданий, в которых использовалась шкала от 0 до 1, в этом издании GCI используется шкала от 0 до 100, причем каждый компонент взвешивается по 20 пунктам.

В качестве общего весового коэффициента каждому показателю, субпоказателю и микропоказателю присваивается весовой коэффициент с учетом относительной важности данной группы показателей. Весовой коэффициент может существенно повлиять на итоговую оценку, и разные методы будут по-разному определять место в рейтинге.

В GCI используется подход, основанный на широком участии, с использованием процесса распределения бюджета (ПРБ). При этом предполагается, что весовые коэффициенты, по сути, являются оценочными суждениями и должны учитывать широкий спектр мнений экспертов.

В рамках подхода на основе распределения бюджета экспертам предоставляется определенный "бюджет", который они могут распределять в рамках группы показателей, давая более высокую оценку тем показателям, которые оцениваются как более важные. Экспертам предлагалось дать рекомендации по весовым коэффициентам для компонентов, относящихся к областям их профессиональной компетенции.

Поскольку все ответы стран, лежащие в основе собранных данных, представляли собой данные обследования, проверенные группой МСЭ, статистическое качество данных при взвешивании не учитывалось.

Участие группы экспертов по весовым коэффициентам

В октябре 2020 года было разослано циркулярное письмо с предложением Государствам – Членам МСЭ и членам, представляющим частный сектор, назначить экспертов для данного издания Глобального индекса кибербезопасности. Назначенные эксперты представляли академические организации, аналитические центры, министерства по ИКТ, регуляторные органы и организации по стандартизации.

Также для внесения рекомендаций по весовым коэффициентам были приглашены эксперты, участвовавшие в выпуске предыдущих изданий Глобального индекса кибербезопасности.

В общей сложности в программе приняли участие 84 эксперта, предложившие свои рекомендации по весовым коэффициентам компонентов, относящихся к областям их профессиональной компетенции.

Агрегирование показателей

Группы показателей агрегировались с использованием средневзвешенных арифметических значений. Это означает, что страна, получившая низкие оценки в одной области, может частично компенсировать их, добившись хороших результатов в другой.

В Справочнике ОЭСР по составным индексам отмечается, что "*при геометрическом агрегировании предельная полезность от повышения низкой абсолютной оценки будет намного выше, чем от повышения высокой абсолютной оценки. Следовательно, если производится геометрическое, а не линейное агрегирование, то стране выгоднее решать вопросы, связанные с теми секторами/видами деятельности/альтернативными решениями, по которым она имеет низкие оценки*" (33). Однако для ясности и наглядности более понятным и действенным был сочтен линейный подход.

Анализ чувствительности

Учитывая важность весовых коэффициентов для окончательной оценки страны, был проведен анализ чувствительности, в который входили:

- включение/исключение отдельных показателей;
- разные схемы взвешивания (схема с равными весовыми коэффициентами, метод распределения бюджета, взвешивание по диаметрально противоположным рекомендациям экспертов);
- разные системы агрегирования (со средневзвешенными коэффициентами, аддитивные).

Рейтинги

Рейтинг стран определялся по их окончательной оценке с использованием метода компактного ранжирования. Равные оценки приводят к одинаковому рейтингу. Страна, следующая за двумя или более странами с одинаковым рейтингом, получает следующий порядковый номер.

Приложение B. Вопросник Глобального индекса кибербезопасности (4-е издание)

Настоящий вопросник разработан и рассмотрен на собрании группы Докладчика Исследовательской комиссии МСЭ-D по Вопросу 3/2 "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности". Это собрание было созвано с целью добиться утверждения Государствами-Членами выпуска 4-го издания Глобального индекса кибербезопасности МСЭ.

Вопросник состоит из пяти разделов; в каждом разделе ответы на вопросы следует давать в форме "да/нет", поставив отметку в клетке перед соответствующим вариантом. Вопросник заполняется в онлайновом режиме. Каждый респондент получил от МСЭ по электронной почте официальное сообщение, содержащее индивидуальный URL и логин для ввода ответов. Респонденты также могут загружать соответствующие документы (и URL) по каждому вопросу в качестве справочной информации. Предполагается, что информация, предоставленная респондентами данного вопросника, не будет носить конфиденциальный характер.

Таблица B1. Вопросник GCI: правовые меры

1 Нормы материального права в области киберпреступности

Пояснение. 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.

1.1 Имеются ли у вас нормы материального права о противозаконном поведении в сети?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.1 Имеются ли у вас нормы материального права о противозаконном доступе к устройствам, компьютерным системам и данным?

Пояснение. Доступ – способность и средства осуществлять связь или иное взаимодействие с системой, использовать ресурсы системы для обработки информации, получать сведения об информации, содержащейся в системе, или управлять компонентами и функциями системы (NICCS).

Компьютерная система или **система** – любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, выполняет автоматизированную обработку данных (COE – Конвенция о киберпреступности).

Компьютерные данные – любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию (COE – Конвенция о киберпреступности).

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.2 Имеются ли у вас нормы материального права о противозаконном вмешательстве (посредством ввода, изменения или уничтожения данных) в устройства, данные и компьютерные системы?

Пояснение. Вмешательство в компьютерную систему – умышленное несанкционированное создание серьезных помех функционированию компьютерной системы. Сюда могут относиться ввод, передача, повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.

Вмешательство в данные – умышленное несанкционированное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.3 Имеются ли у вас нормы материального права о противозаконном перехвате данных в устройствах и компьютерных системах?

Пояснение. Противозаконный перехват – осуществляемый с использованием технических средств умышленный несанкционированный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную или другую электронную систему, из нее или внутри такой системы.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.4 Имеются ли у вас нормы материального права о краже идентичности и хищении данных в онлайновой среде?

Пояснение. Кража идентичности в онлайновой среде – хищение персональных данных, таких как имена, адреса, дата рождения, контактная информация или банковские реквизиты. Это может происходить в результате фишинга, несанкционированного доступа к учетным записям в интернете, извлечения информации из социальных сетей или противозаконного доступа к базам данных.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Имеются ли у вас положения о подлоге с использованием компьютерных технологий (пиратство/нарушение авторского права)?

Пояснение. Несанкционированный ввод, изменение или стирание компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, в целях совершения обмана или злого умысла.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Имеются ли у вас нормы материального права о безопасности в онлайновой среде?

Пояснение. Безопасность в онлайновой среде – достижение максимальной защищенности в интернете от различных рисков для безопасности личной или персональной информации или информации, связанной с имуществом, а также усиление самозащиты пользователей от киберпреступлений.

1.3.1 Имеются ли у вас положения/правовые меры в отношении преступлений, связанных с материалами расистского и ксенофобского характера в онлайновой среде?

Пояснение. Меры по предотвращению различных форм онлайновых агрессивных высказываний и других форм нетерпимости в отношении расы, цвета кожи, религии, происхождения или национальной или этнической принадлежности, сексуальной ориентации или гендерной идентичности, ограниченных физических возможностей, социального статуса или других характеристик.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3.2 Имеются ли у вас положения/правовые меры, направленные против преследования и нарушения уважения к достоинству/неприкосновенности личности в онлайновой среде?

Пояснение. Киберпреследование или запугивание – сообщения по электронной почте, прямые сообщения или оскорбительные веб-сайты, имеющие целью запугивание или иное преследование отдельного лица или группы лиц посредством персонализированных нападок.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3.3 Имеются ли у вас положения/правовые меры, направленные на защиту ребенка в онлайновой среде?

Пояснение. Законодательство, в котором четко прописано, что все без исключения преступления, какие могут совершаться против ребенка в реальном мире, могут совершаться и в интернете или любой другой электронной сети. Необходимо разработать новые или пересмотреть существующие законы, с тем чтобы установить противозаконность определенных видов поведения, характерных только для интернета, таких как дистанционное склонение детей к совершению или просмотру сексуальных действий или их заманивание для встречи в реальном мире с сексуальными целями (Руководящие указания для директивных органов по защите ребенка в онлайновой среде, разработанные МСЭ).

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Имеются ли какие-либо регламентарные положения в области кибербезопасности, относящиеся к следующим вопросам?

Пояснение. Регламентарное положение – это правило, основанное на определенной части законодательства и предназначенное для ее исполнения. Исполнение регламентарных положений обычно осуществляется регуляторным органом, созданным для реализации целей или положений законодательства или уполномоченным на это.

Регламентарные положения в сфере кибербезопасности определяют принципы, которым должны следовать различные заинтересованные стороны и которые проистекают из законов, относящихся к защите данных, уведомлению о нарушениях, требованиям сертификации/стандартизации в области кибербезопасности, осуществлению мер по обеспечению кибербезопасности, требованиям в области кибербезопасности для взрослых, защите конфиденциальности частной информации, защите ребенка в онлайновой среде, цифровым подписям и электронным транзакциям, а также к ответственности поставщиков услуг интернета, и являются частью исполнения этих законов.

2.1 Защита персональных данных/конфиденциальности частной информации

Пояснение. Нормативно-правовые положения о защите персональных данных от несанкционированного доступа, изменения, разрушения или использования. Конфиденциальность частной информации в интернете – это степень конфиденциальности и безопасности личных данных, обнародованных в интернете. Это широкий термин, обозначающий множество факторов, способов и технологий, применяемых для защиты конфиденциальных данных, частной информации, коммуникаций и предпочтений; примером таких законодательных положений может служить Закон о защите данных.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Уведомления о случаях утечки данных

Пояснение. Законодательные и регламентарные положения, касающиеся уведомления о случаях утечки данных, обязывают пострадавшую организацию уведомить о такой утечке соответствующие инстанции, своих клиентов и другие стороны, а также принять меры к устранению причиненного ущерба. Такие законы, как правило, принимаются в ответ на растущее число случаев взлома баз данных, содержащих информацию, позволяющую установить личность пользователей.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3 Требования проверки кибербезопасности

Пояснение. Проверка безопасности – это систематически и периодически проводимая оценка безопасности информационной системы. Стандартная проверка может включать оценку безопасности физической конфигурации и среды системы, программного обеспечения, процессов обработки информации, а также методов работы пользователей.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.4 Применение стандартов

Пояснение. Существование одобренной (или утвержденной) государством системы (или систем) для применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственных учреждениях) и в рамках критически важной инфраструктуры (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, ETCИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.5 Выявление и защита критически важных государственных информационных инфраструктур

Пояснение. Критически важная инфраструктура – это основные системы, имеющие решающее значение для обеспечения защищенности, безопасности, в том числе экономической, а также для охраны здоровья населения страны. К таким системам, среди прочего, относятся системы обороны, банковские и финансовые системы, системы электросвязи, энергетические системы и т. д. Приведите любые ссылки или документы, которые определяют критически важные инфраструктуры, или документы/новостные материалы, подтверждающие эти определения.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в области правовых норм, относящихся к кибербезопасности, которые связаны с вашей страной.

Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы.

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

Таблица B2. Вопросник GCI: технические меры

1 Национальные/правительственные CIRT/CSIRT/CERT

Пояснение. CIRT/CSIRT/CERT – группы реагирования на компьютерные инциденты, укомплектованные персоналом специальные организационные структуры, отвечающие за координацию и поддержку мер реагирования на события или инциденты, связанные с компьютерной безопасностью, на национальном или государственном уровне.

ПРИМЕЧАНИЕ. – Иногда проводится различие между правительственными и национальными CIRT как отдельными/разными структурами – правительственные CIRT обслуживают правительственные учреждения, а национальные CIRT – национальные субъекты, включая частные предприятия и граждан. Иногда их считают одной и той же структурой.

1.1 Имеется ли национальная/государственная CIRT/CSIRT/CERT?

Пояснение. Учрежденная решением правительства или являющаяся частью правительственных или национальных структур.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Занимается ли ваша национальная или правительственная CIRT/CSIRT/CERT следующими видами деятельности

1.2.1 Разработка и реализация мероприятий по повышению осведомленности в вопросах кибербезопасности

Пояснение. Работа по организации широких информационно-пропагандистских кампаний в целях распространения в масштабах страны информации о безопасном поведении в кибер- и онлайн-пространстве.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.2 Проведение регулярных учений по кибербезопасности, таких как CyberDrills

Пояснение. Запланированное мероприятие, в ходе которого организация имитирует нарушение киберпространства для развития или проверки таких навыков и умений, как предотвращение, выявление подобных нарушений, смягчение их последствий, реагирование на них, а также восстановление после таких нарушений. Проводятся ли такие учения периодически или систематически?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.3 Распространение общедоступных информационных бюллетеней

Пояснение. Информационные бюллетени CIRT – донесение до сведения широкой общественности информации о возникающих киберугрозах и рекомендуемых действиях.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.4 Содействие обеспечению защиты ребенка в онлайновой среде

Пояснение. CIRT/CSIRT/CERT обеспечивает поддержку инициатив по защите ребенка в онлайновой среде путем проведения кампаний по повышению осведомленности, информирования о происшествиях, связанных с детьми, предоставления учебных материалов по этим вопросам и др.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) с Форумом групп реагирования на инциденты и обеспечения безопасности (FIRST)?

Пояснение. Полноправный или ответственный за взаимодействие член Форума групп реагирования на инциденты и обеспечения безопасности (www.first.org).

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.4 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) с региональной группой CERT?

Пояснение. Формальная или неформальная связь с какой-либо группой CERT внутри или за пределами страны в рамках региональной группы CERT. Примеры региональных групп CERT: APCERT, AFRICACERT, EGC, OIC и OAS.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.5 Был ли уровень развития вышеупомянутых групп CIRT, CSIRT или CERT сертифицирован по схеме сертификации TI в соответствии с TF-CSIRT – SIM3?

Пояснение. SIM3 – основа сертификации CIRT.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Отраслевые группы CIRT/CSIRT/CERT

Пояснение. 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, научные и образовательные учреждения, экстренные службы и финансовый сектор. Отраслевая CERT обслуживает клиентов только из определенной отрасли.

2.1 Существуют ли отраслевые группы CIRT/CSIRT/CERT в вашей стране?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Занимаются ли ваши отраслевые CIRT/CSIRT/CERT следующими видами деятельности?

2.2.1 Подготовка и проведение мероприятий по повышению осведомленности по кибербезопасности в отрасли

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2.2 Активное участие в национальных учениях CyberDrill

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2.3 Распространение информации о случившихся в отрасли инцидентах среди отраслевых предприятий

Пояснение. Распространение информации о возникающих киберугрозах и рекомендуемых действиях.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Национальная система для применения стандартов кибербезопасности

Пояснение. Одобрена государственная система (или системы) применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственные органы) и в управлении критически важной 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, ETCИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.

3.1 Имеется ли система для применения/принятия стандартов кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.2 Распространяется ли эта система на международные или другие соответствующие стандарты?

Пояснение. МСЭ-Т, ИСО/МЭК, NIST, ANSI/ISA и др.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4 Защита ребенка в онлайновой среде

Пояснение. Это показатель наличия в стране национального агентства, занимающегося вопросами защиты ребенка в онлайновой среде; телефонного номера для сообщений о проблемах, связанных с пребыванием детей в онлайновой среде; любых технических механизмов и средств подачи сообщений, которые помогают защитить детей в онлайновой среде; и любой деятельности государственных и негосударственных учреждений по распространению знаний и оказанию поддержки с предоставлением телефонного номера, адреса электронной почты, веб-форм и т. п. для защиты детей в онлайновой среде, по которым заинтересованные стороны могут сообщать об инцидентах или проблемах, связанных с защитой ребенка в онлайновой среде (COP).

4.1 Имеются ли какие-либо механизмы и средства подачи сообщений, которые помогают защитить детей в онлайновой среде?

Пояснение. Горячие линии, телефоны доверия и т. п.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в технических областях, относящихся к кибербезопасности, которые связаны с вашей страной.

Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы.

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

Таблица B3. Вопросник GCI: организационные меры

1 Национальная стратегия кибербезопасности

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

1.1 Имеется ли в вашей стране национальная стратегия/политика в области кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Предусматривает ли она защиту критически важных национальных информационных инфраструктур, в том числе в секторе электросвязи?

Пояснение. Любые физические или виртуальные информационные системы, которые контролируют, обрабатывают, передают, получают или хранят электронную информацию любого вида, включая данные, голос или видео, имеющие жизненно важное значение для функционирования критически важных инфраструктур – настолько важное, что неработоспособность или разрушение таких систем приведет к катастрофическим последствиям для национальной безопасности, национальной экономической безопасности или здоровья и безопасности населения.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Включает ли она упоминание об устойчивости национальной системы кибербезопасности?

Пояснение. Национальный план обеспечения устойчивости кибербезопасности гарантирует наличие у страны возможности своевременно и эффективно противостоять последствиям любой угрозы (стихийной или антропогенной), переносить их, приспосабливаться к ним и восстанавливаться, в том числе путем сохранения и восстановления своих собственных основных служб и функций с помощью внешних служб.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Производится ли пересмотр и обновление национальной стратегии кибербезопасности на постоянной основе?

Пояснение. Установлено управление жизненным циклом стратегии; стратегия обновляется в соответствии с изменениями в национальной, технологической, социальной, экономической и политической сферах, которые могут повлиять на ситуацию с кибербезопасностью в стране.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Открыта ли стратегия кибербезопасности для консультаций с национальными экспертами в области кибербезопасности в той или иной форме?

Пояснение. Стратегия открыта для консультаций со всеми заинтересованными сторонами, включая операторов критически важных инфраструктур, поставщиков услуг интернета, научные учреждения и др.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Имеется ли установленный план действий/дорожная карта по осуществлению управления в области кибербезопасности?

Пояснение. Стратегический план, определяющий общие результаты в области национальной кибербезопасности, включая необходимые для его реализации шаги и этапы.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Имеется ли национальная стратегия защиты ребенка в онлайновой среде?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Ответственный орган

Пояснение. 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. Ответственные органы могут функционировать в рамках правительства и иметь полномочия принуждать другие учреждения и национальные органы к осуществлению политики и внедрению стандартов.

2.1 Имеется ли орган, ответственный за координацию в области кибербезопасности на национальном уровне?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.1.1 Осуществляет ли этот орган контроль в области защиты важнейшей государственной информационной инфраструктуры?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Имеется ли национальный орган, контролирующий развитие национального потенциала в области кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3 Имеется ли орган, осуществляющий надзор за реализацией инициатив по защите ребенка в онлайновой среде на национальном уровне?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Показатели кибербезопасности

Пояснение. 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.

3.1 Проводятся ли какие-либо проверки кибербезопасности на национальном уровне?

Пояснение. Проверка безопасности – систематическая оценка безопасности информационной системы, заключающаяся в измерении степени ее соответствия набору установленных критериев. Всесторонняя проверка, как правило, предусматривает оценку безопасности физической конфигурации и среды системы, программного обеспечения, процессов обработки информации, а также методов работы пользователей. Регуляторные органы могут требовать проведения периодической оценки состояния безопасности критически важных инфраструктур, находящихся в частной собственности, и представления отчетов о результатах.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.2 Существуют ли показатели для оценки рисков, связанных с киберпространством, на национальном уровне?

Пояснение. Это процесс, включающий выявление, анализ и оценку рисков.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.3 Имеются ли показатели для оценки уровня развития кибербезопасности на национальном уровне?

Пояснение. Это подход к измерению уровня развития кибербезопасности в государстве.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в области организационных мер, относящихся к кибербезопасности, которые связаны с вашей страной.

Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы.

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

Таблица B4. Вопросник GCI: меры по развитию потенциала

1 Кампании по повышению осведомленности населения в области кибербезопасности

Пояснение. 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. Сюда относятся такие действия, как создание порталов и веб-сайтов для повышения осведомленности, распространение вспомогательных материалов и другие соответствующие мероприятия.

1.1 Проводятся ли кампании по повышению осведомленности населения, ориентированные на определенный сектор, такой как МСП, компании частного сектора и госучреждения?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Проводятся ли кампании по повышению осведомленности населения, ориентированные на гражданское общество?

Пояснение. НПО, общественные организации.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Проводятся ли кампании по повышению осведомленности населения, ориентированные на граждан?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.4 Проводятся ли кампании по повышению осведомленности населения, ориентированные на пожилых людей?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.5 Проводятся ли кампании по повышению осведомленности населения, ориентированные на лиц с особыми потребностями?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.6 Проводятся ли кампании по повышению осведомленности населения с участием родителей, педагогов и детей (связанные с СОР)?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Подготовка специалистов по кибербезопасности

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

Сюда также относится подготовка по вопросам кибербезопасности для сотрудников правоохранительных, судебных и других юридических органов. Это специализированная профессионально-техническая подготовка, которая может периодически проводиться для сотрудников полиции, правоохранительных органов, судей, адвокатов, поверенных, юристов, помощников юристов и других лиц, работающих в сфере права и правоприменения. 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.

2.1 Осуществляет ли ваше правительство разработку или проведение курсов профессиональной подготовки по кибербезопасности?

Пояснение. Содействие проведению курсов по кибербезопасности для работников (технической сферы, сферы социальных наук и т. п.) и сертификации специалистов предприятий государственного или частного сектора.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Имеется ли в вашей стране программа аккредитации специалистов по кибербезопасности?

Пояснение. Учреждения, проводящие аккредитацию специалистов по кибербезопасности, или любые другие соответствующие механизмы.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для специалистов по кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3.1 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников правоохранительных органов??

Пояснение. Официальный процесс просвещения специалистов в области правоприменения (сотрудников полиции и правоохранительных органов) по вопросам компьютерной безопасности.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3.2 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для сотрудников судебных и других юридических органов?

Пояснение. Профессиональная или техническая подготовка по кибербезопасности, которая может периодически проводиться для сотрудников полиции, правоохранительных органов, судей, адвокатов, поверенных, юристов, помощников юристов и других лиц, работающих в сфере права и правоприменения.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников МСП/частных компаний?

Пояснение. Учебные занятия по освоению передового опыта/развитию потенциала в области кибербезопасности для защиты своего бизнеса и т. п. путем правильного использования онлайновых услуг.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3.4 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для других должностных лиц из государственного сектора и правительственных учреждений?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Осуществляет ли ваше правительство/ваша организация разработку или поддержку каких-либо образовательных программ или учебных планов в области кибербезопасности...

Пояснение. Наличие 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.

3.1 В начальной школе?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.2 В средней школе?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.3 В высшей школе?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4 Научно-исследовательские программы в области кибербезопасности

Пояснение. 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. Научно-исследовательские программы в области кибербезопасности включают, помимо прочего, анализ вредоносного программного обеспечения, исследования в области криптографии, уязвимости систем, а также моделей и концепций безопасности. Программы развития кибербезопасности – это программы разработки аппаратного или программного обеспечения, которые включают, в частности, брандмауэры, системы предотвращения вторжения, сети-приманки, а также модули обеспечения безопасности аппаратного обеспечения. Для улучшения координации деятельности различных учреждений и совместного использования ресурсов необходим общий национальный орган.

4.1 Проводится ли научно-исследовательская деятельность в области кибербезопасности на общенациональном уровне?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4.1.1 Имеются ли программы НИОКР по кибербезопасности в частном секторе?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4.1.2 Имеются ли программы НИОКР по кибербезопасности в государственном секторе?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4.1.3 Вовлечены ли в научно-исследовательскую деятельность высшие учебные заведения, такие как академии и университеты?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

5 Национальная отрасль кибербезопасности

Пояснение. 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.

5.1 Имеется ли национальная отрасль кибербезопасности??

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

6 Имеются ли какие-либо правительственные механизмы, стимулирующие...

Пояснение. 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. Стимулы повышают спрос на связанные с кибербезопасностью услуги и продукты, что способствует улучшению защиты от киберугроз.

6.1 создание потенциала в области кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

6.2 развитие отрасли кибербезопасности?

Пояснение. Поддержка новых компаний в сфере услуг по обеспечению кибербезопасности в научной и других областях.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передового опыта/достижений/текущих разработок, связанных с мерами по созданию потенциала в области кибербезопасности, которые связаны с вашей страной.

Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы.

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

Таблица B5. Вопросник GCI: меры в области сотрудничества

1 Двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами

Пояснение. 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 или международной организацией, 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). Этот показатель служит также для определения того, осуществляется ли обмен информацией о выявленных угрозах. Создание потенциала – это обмен профессиональными инструментами, расширение круга экспертов и др.

1.1 Имеются ли у вас двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?

Пояснение. Под обменом информацией понимается практика обмена неконфиденциальной информацией.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?

Пояснение. Возможность поощрять проведение в рамках сотрудничества учебных занятий для укрепления навыков, компетенций и способностей национальных специалистов по кибербезопасности в целях обеспечения согласованности совместных действий против киберугроз.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Предусматривает(ют) ли это (эти) соглашение(я) взаимную правовую помощь?

Пояснение. Оказание двумя или более странами взаимной помощи по сбору и обмену информацией в целях обеспечения применения норм публичного или уголовного права.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Участие правительства в международных механизмах, связанных с деятельностью в сфере кибербезопасности

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

2.1 Участвует ли ваше правительство/ваша организация в международных механизмах, связанных с деятельностью в сфере кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Многосторонние соглашения по кибербезопасности

Пояснение. 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).

3.1 Имеются ли у вашего государства многосторонние соглашения о сотрудничестве в области кибербезопасности?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.1.1 Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?

Пояснение. Под обменом информацией понимается практика обмена неконфиденциальной информацией.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.1.2 Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?

Пояснение. Возможность поощрять проведение в рамках сотрудничества учебных занятий для укрепления навыков, компетенций и способностей национальных специалистов по кибербезопасности в целях обеспечения согласованности совместных действий против киберугроз.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4 Партнерские отношения с частным сектором (ГЧП)

Пояснение. 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 (то есть официальные партнерства в целях сотрудничества или обмена информацией, опытом, технологиями и/или ресурсами) на национальном или международном уровнях.

4.1 Участвует ли ваше правительство в ГЧП с местными компаниями?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4.2 Участвует ли ваше правительство в ГЧП с иностранными компаниями в вашей стране?

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

5 Межведомственные партнерства

Пояснение. Этот показатель эффективности касается официальных партнерств между различными правительственными органами данного государства (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.

5.1 Имеются ли межведомственные партнерства/соглашения между различными правительственными органами, касающиеся кибербезопасности?

Пояснение. Сотрудничество между министерствами или специализированными учреждениями.

□ *Да*

□ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок, относящихся к мерам в области сотрудничества в рамках деятельности в области кибербезопасности, которые связаны с вашей страной.

Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы.

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

Канцелярия Директора
Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)
Place des Nations
CH-1211 Geneva 20
Switzerland

Эл. почта: bdtdirector@itu.int
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

Канцелярия заместителя Директора и региональное присутствие
Департамент координации операций на местах (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Эл. почта: bdtdeputydir@itu.int
Тел.: +41 22 730 5131
Факс: +41 22 730 5484

Департамент цифровых сетей и цифрового общества (DNS)

Эл. почта: bdt-dns@itu.int
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

Департамент центра цифровых знаний (DKH)

Эл. почта: bdt-dkh@itu.int
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

Департамент партнерских отношений в интересах цифрового развития (PDD)

Эл. почта: bdt-pdd@itu.int
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

Африка

Эфиопия

Региональное отделение МСЭ
Gambia Road
Leghar Ethio Telecom Bldg., 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Эл. почта: itu-ro-africa@itu.int
Тел.: +251 11 551 4977
Тел.: +251 11 551 4855
Тел.: +251 11 551 8328
Факс: +251 11 551 7299

Камерун

Зональное отделение МСЭ
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroun

Эл. почта: itu-yaounde@itu.int
Тел.: + 237 22 22 9292
Тел.: + 237 22 22 9291
Факс: + 237 22 22 9297

Сенегал

Зональное отделение МСЭ
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar – Yoff
Senegal

Эл. почта: itu-dakar@itu.int
Тел.: +221 33 859 7010
Тел.: +221 33 859 7021
Факс: +221 33 868 6386

Зимбабве

Зональное отделение МСЭ
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Эл. почта: itu-harare@itu.int
Тел.: +263 242 369015
Тел.: +263 242 369016

Северная и Южная Америка

Бразилия

Региональное отделение МСЭ
SAUS Quadra 6 Ed. Luis Eduardo Magalhães
Bloco E, 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia – DF
Brazil

Эл. почта: itubrasilia@itu.int
Тел.: +55 61 2312 2730-1
Тел.: +55 61 2312 2733-5
Факс: +55 61 2312 2738

Барбадос

Зональное отделение МСЭ
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Эл. почта: itubridgetown@itu.int
Тел.: +1 246 431 0343
Факс: +1 246 437 7403

Чили

Зональное отделение МСЭ
Merced 753, Piso 4
Santiago de Chile
Chile

Эл. почта: itusantiago@itu.int
Тел.: +56 2 632 6134/6147
Факс: +56 2 632 6154

Гондурас

Зональное отделение МСЭ
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Эл. почта: itutegucigalpa@itu.int
Тел.: +504 2235 5470
Факс: +504 2235 5471

Арабские государства

Египет

Региональное отделение МСЭ
Smart Village, Building B 147
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Эл. почта: itu-ro-arabstates@itu.int
Тел.: +202 3537 1777
Факс: +202 3537 1888

Азиатско-Тихоокеанский регион

Таиланд

Региональное отделение МСЭ
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210
Thailand

Эл. почта: itu-ro-asiapacific@itu.int
Тел.: +66 2 574 9326 – 8
+66 2 575 0055

Индонезия

Зональное отделение МСЭ
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Эл. почта: itu-ro-asiapacific@itu.int
Тел.: +62 21 381 3572
Тел.: +62 21 380 2322/2324
Факс: +62 21 389 5521

Индия

Зональное отделение и Центр инноваций МСЭ
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Эл. почта: itu-ro-southasia@itu.int

СНГ

Российская Федерация

Региональное отделение МСЭ
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Эл. почта: itu-ro-cis@itu.int
Тел.: +7 495 926 6070

Европа

Швейцария

Отделение для Европы МСЭ
Place des Nations
CH-1211 Geneva 20
Switzerland

Эл. почта: eurregion@itu.int
Тел.: +41 22 730 5467
Факс: +41 22 730 5484

Международный союз
электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-32732-3 SAP id

Опубликовано в Швейцарии
Женева, 2024 г.
Фотографии представлены: Shutterstock