Программа МСЭ-D в области кибербезопасности

Глобальный индекс кибербезопасности – GCIv5

Эталонная модель (методика)

Содержание

Стр.

Содержание 2

История вопроса и справочная информация 3

Сфера охвата 3

Концептуальная структура 4

Методика вычислений 5

Общая последовательность процесса GCI 5

ПРИЛОЖЕНИЕ A – Определения основных составляющих и показателей 7

Правовые меры 7

1.1 Законодательство в области киберпреступности 7

1.2 Нормативные положения в области кибербезопасности 7

Технические меры 7

1.1 Национальные/правительственные группы реагирования на компьютерные инциденты 7

1.2 Отраслевые группы CIRT/CSIRT/CERT 8

1.3 Национальная система для применения стандартов кибербезопасности 8

Организационные меры 8

1.1 Национальная стратегия/политика кибербезопасности 8

1.2 Ответственный орган 8

1.3 Показатели кибербезопасности 9

1.4 Стратегии и инициативы по защите ребенка в онлайновой среде (COP) 9

Меры по развитию потенциала 9

1.1 Кампании по повышению осведомленности населения в области кибербезопасности 9

1.2 Подготовка специалистов по кибербезопасности 9

1.3 Образовательные программы по кибербезопасности в рамках национальных образовательных стандартов 10

1.4 Программы исследований и разработок (НИОКР) в области кибербезопасности 10

1.5 Национальная отрасль кибербезопасности 10

1.6 Государственные механизмы стимулирования 10

Меры в области сотрудничества 10

1.1 Двусторонние соглашения в области кибербезопасности 10

1.2 Многосторонние соглашения в области кибербезопасности 11

1.3 Договоры о взаимной правовой помощи в области кибербезопасности 11

1.4 Государственно-частные партнерства 11

1.5 Межведомственные партнерства 11

История вопроса и справочная информация

Глобальный индекс кибербезопасности (GCI), впервые опубликованный в 2015 году, помогает странам повысить уровень своей приверженности обеспечению кибербезопасности путем выявления сильных сторон и точек роста в отношении кибербезопасности и освещения передового опыта. На основании собранной информации в GCI представлены обязательства, которые Государства-Члены могут выполнить в своих национальных условиях. Кроме того, GCI способствует распространению передового опыта и формированию глобальной культуры кибербезопасности.

Сфера охвата и структура GCI закреплены в Резолюции 130 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ, в которой формулируется задача усиления роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий. В частности, Государствам-Членам 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*". Конечная цель заключается в содействии формированию глобальной культуры кибербезопасности и превращению ее в один из основных элементов информационно-коммуникационных технологий.

Предыдущие издания Глобального индекса кибербезопасности отвечают рекомендациям Резолюции 45 (Пересм. Кигали, 2022 г.) МСЭ-D, в которой четко определяется работа в рамках Глобального индекса кибербезопасности (GCI) и БРЭ рекомендуется "учитывать результаты GCI для ориентирования инициатив, связанных с кибербезопасностью, уделяя особое внимание разрывам, выявленным в процессе определения GCI".

Предыдущие издания GCI:

Название издания	GCIv1	GCIv2	GCIv3	GCI 2020 (GCIv4)
Номер издания	1	2	3	4
Количество стран-участников	105 стран	136 стран	155 стран	169 стран
Период сбора данных	2013–2014 гг.	2016 г.	2017–2018 гг.	2020 г.
Год публикации	2015 г.	2017 г.	2019 г.	2021 г.
Примечание	В партнерстве с ABI Research			

Вопросник GCI с соответствующими показателями, субпоказателями и микропоказателями обновляется в период между подготовкой изданий в консультации с Вопросом Исследовательской комиссии МСЭ-D "*Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности среди Членов МСЭ*".

Поскольку Государства-Члены демонстрируют постоянный интерес к GCI, МСЭ занимается подготовкой пятого издания (GCIv5) в консультации с Группой экспертов по GCI, в соответствии с рекомендацией Резолюции 45 (Пересм. Кигали, 2022 г.).

Сфера охвата

Глобальный индекс кибербезопасности (GCI) представляет собой составной индекс, объединяющий различные показатели в области кибербезопасности в меры, основанные на пяти основных составляющих Глобальной программы кибербезопасности (ГПК). Эти основные составляющие образуют пять ключевых компонентов GCI. Основными целями GCI является измерение:

- видов, уровней и процесса трансформации обязательств стран в области кибербезопасности;
- прогресса в соблюдении обязательств в области кибербезопасности с глобальной точки зрения;

- прогресса в соблюдении обязательств в области кибербезопасности с точки зрения региональных перспектив;
- разрыва в соблюдении обязательств в области кибербезопасности, т. е. различий между странами с точки зрения уровня их участия в инициативах по обеспечению кибербезопасности.

Целью Глобального индекса кибербезопасности является содействие странам в определении требующих улучшения аспектов кибербезопасности, что способствует повышению общего уровня кибербезопасности во всем мире. В GCI также собраны примеры передового опыта, который страны могут перенять, чтобы усовершенствовать свои методы обеспечения кибербезопасности и повысить степень согласованности подходов.

Концептуальная структура

Глобальный индекс кибербезопасности основан на следующих пяти основных составляющих, представляющих собой всеобъемлющие аспекты обязательств стран в области кибербезопасности:

Правовые меры: законодательные инструменты, включая законы, нормативные положения и политику, определяющие права, обязанности и меры защиты, предоставляемые в отношении ключевых вопросов, связанных с кибербезопасностью, например, в отношении запрета определенной криминальной деятельности или минимальных регуляторных требований.

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

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

Меры по развитию потенциала: развитие потенциала является неотъемлемой частью правовых, технических и организационных мер. Понимание связанных с кибербезопасностью технологий, рисков и последствий может способствовать разработке более совершенного законодательства, политики, стратегий и более эффективному распределению ролей и обязанностей. Развитие потенциала включает в себя развитие знаний и навыков как среди основного населения, так и среди специалистов, чья работа косвенно или напрямую связана с кибербезопасностью.

Меры в области сотрудничества: усилия по обеспечению кибербезопасности более успешны в том случае, когда они опираются на все затрагиваемые секторы и дисциплины, и для их реализации необходим целостный подход с участием многих заинтересованных сторон. Сотрудничество укрепляет диалог и координацию, что позволяет сформировать более широкую область применения кибербезопасности. Сотрудничество может включать в себя такие виды деятельности, как реализация совместных инициатив, обмен информацией, проведение профессиональной подготовки и другие мероприятия, объединяющие специалистов, должностных лиц и других субъектов, стремящихся повысить уровень кибербезопасности.

Методика вычислений

Пятое издание вопросника GCI состоит из пяти основных составляющих: правовые, технические, организационные меры, меры по развитию потенциала и сотрудничеству, которые включают в общей сложности 20 показателей, 64 субпоказателя и 28 микропоказателя, составленных на основе 83 вопросов. Вопросы подобраны таким образом, чтобы соблюсти баланс между значимой детализацией в отношении обязательств в области кибербезопасности, при этом не теряя из виду общую перспективу. Показатели можно найти в вопроснике GCI **Error! Reference source not found.**(Приложение A).

Показатели отбираются с учетом:

- актуальности в отношении основных составляющих Глобальной программы кибербезопасности;
- соответствия сфере охвата и концептуальной структуре Глобального индекса кибербезопасности;
- способности Государств-Членов предоставить точные ответы на вопросы;
- возможности осуществления перекрестной проверки с помощью вторичных данных.

В настоящем издании предложены три варианта ответов (да, частично, нет), чтобы исключить субъективность в оценке и любую возможную предвзятость в отношении определенных типов ответов. Кроме того, простая трехчастная концепция позволяет быстрее проводить более сложную оценку, поскольку она не подразумевает пространные ответы, что ускоряет и упрощает предоставление данных и последующий анализ. Респондент должен только подтвердить наличие или отсутствие конкретных заранее определенных решений в области кибербезопасности.

В целях обеспечения точности страны должны будут предоставить сведения, подтверждающие их ответ, с помощью функции загрузки подтверждающих документов и адресов URL. К каждой основной составляющей будет добавлен раздел комментариев, чтобы страны могли поделиться передовым опытом, рассказывающем о последствиях их эволюции в области обеспечения кибербезопасности.

Пятое и все последующие издания GCI будут структурированы в зависимости от уровней обязательств в соответствии с Резолюцией 45 ВКРЭ (Всемирной конференции по развитию электросвязи), прошедшей в Кигали, Руанда, в июне 2022 года, на которой Государства-Члены рекомендовали GCI принять многоуровневый подход, заключающейся в разбивке стран на группы вместо составления их рейтинга, с тем чтобы обеспечить более значимую оценку сильных сторон стран, а также областей, требующих улучшения. Таким образом, на собраниях Группы экспертов по методике будет поставлена задача по определению подходящей структуры уровней.

Общая последовательность процесса GCI

1 Вопросник GCI пересматривается с учетом отзывов, полученных от Государств-Членов и Группы экспертов по GCI. Вопросник представляется собранию 2-й Исследовательской комиссии для дальнейшего обсуждения.

2 В соответствии с Резолюцией 45 (Пересм. Кигали, 2022 г.) МСЭ-D Глобальный индекс кибербезопасности будет и далее составляться на основе рекомендаций Группы экспертов по

GCI в отношении аспектов, связанных с методикой, структурой, вопросами и весовыми коэффициентами.

3 Формируется состав Группы, работающей по переписке, которая представляет собой рабочую группу Группы экспертов по GCI и включает специалистов и желающих присоединиться представителей Государств-Членов для предоставления рекомендаций и отзывов в отношении вопросника.

4 Секретариат БРЭ вносит соответствующие изменения на основе консультаций с Группой, работающей по переписке, до того, как руководство БРЭ одобрит вопросник или представит его, в частичном виде или полностью, для получения дополнительных отзывов от Группы, работающей по переписке.

5 Утвержденный вопросник направляется для перевода на все шесть (6) официальных языков ООН.

6 В рамках Группы экспертов по GCI проходят еще два собрания рабочей группы для проведения консультаций по уровням и распределению весовых коэффициентов.

7 Директор БРЭ направляет письмо с приглашением в адрес всех Государств – Членов МСЭ и Государства Палестина принять участие в обследовании GCI. Письма предназначены для информирования стран о GCI и содержат просьбу назначить координатора, ответственного за сбор всех соответствующих страновых данных и заполнение вопросника GCI.

8 Назначенным координаторам официально предлагается представить ответы на вопросник с помощью онлайнового портала.

9 Секретариат БРЭ проводит сбор вторичных данных для стран, ответивших на вопросник, который включает:

- выявление любых недостающих ответов, подтверждающих документов, ссылок и т. д.;
- работу координатора по уточнению ответов там, где это необходимо;
- направление исправленного проекта вопросника каждому координатору для итогового утверждения;
- использование подтвержденного вопросника для анализа, подсчета баллов и распределения по уровням.

10 Секретариат БРЭ проводит сбор первичных данных для стран, не ответивших на вопросник, который включает:

- осуществляемую МСЭ подготовку первоначальных ответов на вопросник с использованием общедоступных данных и изучения источников в интернете;
- направление проекта заполненного вопросника координаторам на рассмотрение;
- работу координаторов по уточнению ответов и возвращение проекта заполненного вопросника;
- направление исправленного проекта заполненного вопросника каждому координатору для окончательного утверждения;
- использование подтвержденного вопросника для анализа, подсчета баллов и распределения по уровням.

11 Составляется отчет, содержащий краткое изложение основных тенденций и передового опыта с учетом рекомендаций в отношении уровней и весовых коэффициентов, подготовленных Группой экспертов по GCI.

Примечание. – Если страна не предоставит координатора по вопроснику GCI, МСЭ установит контакт с институциональным координатором, указанным в Общем справочнике МСЭ.

ПРИЛОЖЕНИЕ А

Определения основных составляющих и показателей

Правовые меры

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

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

1.1 Законодательство в области киберпреступности

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

1.2 Нормативные положения в области кибербезопасности

Нормативное положение – это правило или принцип, регулирующий поведение или практику; в частности, соответствующая директива, которую составляет и ведет какой-либо орган власти[1]. Нормативное положение основано на правилах и предназначено для выполнения определенного законодательного акта. Нормативные положения в области кибербезопасности определяют законы, касающиеся защиты данных, уведомления о нарушениях, требований сертификации/стандартизации в области кибербезопасности, реализации мер по обеспечению кибербезопасности, требований проверки кибербезопасности, защиты конфиденциальности, защиты ребенка в онлайновой среде, цифровых подписей и электронных транзакций, а также ответственности поставщиков услуг интернета.

Технические меры

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

1.1 Национальные/правительственные группы реагирования на компьютерные инциденты

CIRT (Группа реагирования на компьютерные инциденты), CERT (Группа реагирования на нарушения компьютерной защиты) и CSIRT (Группа реагирования на инциденты в сфере компьютерной безопасности) являются конкретными организационными структурами, отвечающими за координацию и поддержку при реагировании на инциденты в области компьютерной безопасности или инциденты на национальном уровне. Они несут ответственность на национальном уровне за

---

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation.

предоставление возможностей для выявления киберугроз, защиты, реагирования и управления ими, а также повышения безопасности киберпространства в государстве. Эти возможности должны дополняться сбором собственных разведывательных данных вместо использования вторичных сведений из отчетов об инцидентах в отношении безопасности, поступающих от подразделений CIRT или из других источников.

1.2 Отраслевые группы CIRT/CSIRT/CERT

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

1.3 Национальная система для применения стандартов кибербезопасности

Первостепенное значение имеет создание государственной системы (или систем) применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственные органы) и в управлении критической инфраструктурой (даже если она эксплуатируется частным сектором). Эти стандарты, среди прочего, включают стандарты, разработанные следующими организациями: ИСО, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETCИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.

Организационные меры

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

1.1 Национальная стратегия/политика кибербезопасности

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

1.2 Ответственный орган

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

1.3 Показатели кибербезопасности

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

1.4 Стратегии и инициативы по защите ребенка в онлайновой среде (СОР)

Национальная стратегия защиты ребенка в онлайновой среде должна включать план действий по созданию безопасной онлайновой среды для детей во всем мире. Необходимо ввести в действие свод норм, устанавливающих набор правил и задач, благодаря которым становится очевидно, что любое преступление, которое может быть совершено против ребенка в физическом пространстве, также может mutatis mutandis быть совершено в интернете или любой другой электронной сети.

Меры по развитию потенциала

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

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

1.1 Кампании по повышению осведомленности населения в области кибербезопасности

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

1.2 Подготовка специалистов по кибербезопасности

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

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

1.3 Образовательные программы по кибербезопасности в рамках национальных образовательных стандартов

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

1.4 Программы исследований и разработок (НИОКР) в области кибербезопасности

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

1.5 Национальная отрасль кибербезопасности

Благоприятная экономическая, политическая и социальная среда, способствующая обеспечению кибербезопасности, стимулирует развитие частного сектора, ориентированного на обеспечение кибербезопасности. Проведение кампаний по повышению осведомленности общественности, развитие трудовых ресурсов и потенциала, а также 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.

1.6 Государственные механизмы стимулирования

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

Меры в области сотрудничества

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

1.1 Двусторонние соглашения в области кибербезопасности

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

1.2 Многосторонние соглашения в области кибербезопасности

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).

1.3 Договоры о взаимной правовой помощи в области кибербезопасности

Сюда также может входить ратификация международных соглашений, содержащих положения, касающиеся взаимной правовой помощи и кибербезопасности.

1.4 Государственно-частные партнерства

Государственно-частные партнерства (ГЧП) – это совместные предприятия с участием государственного и частного секторов. Они могут принимать форму долгосрочного договора между частным субъектом и государственным органом на обеспечение принадлежащего государству актива или предоставление государственной услуги, при котором частный субъект несет значительный риск и управленческую ответственность, а его вознаграждение зависит от результативности[2]. Этот показатель эффективности служит для определения количества официально признанных национальных или отраслевых ГЧП, осуществляющих обмен информацией и активами (кадрами, процессами, инструментами) в области кибербезопасности между государственным и частным секторами (т. е. официальные партнерства в целях сотрудничества или обмена информацией, опытом, технологиями и/или ресурсами) на национальном или международном уровнях.

1.5 Межведомственные партнерства

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

---

[2] https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships.