

1

Глобальный обзор существующих инструментов оценки национального потенциала кибербезопасности (GOAT)

**ГЛОБАЛЬНЫЙ ФОРУМ**

**ПО КИБЕРКОМПЕТЕНТНОСТИ**

**Авторы**

Настоящий документ подготовлен Рабочей группой A – Целевой группой по стратегии и оценкам Глобального форума по киберкомпетентности (GFCE) в качестве проекта согласно плану ее работы на 2020 год. В состав проектной группы вошли:

* Кэролин Вайссер Харрис, Глобальный центр развития потенциала в области кибербезопасности (GCSCC);
* Иэн Уоллес, председатель Рабочей группы A по вопросам стратегии и политики GFCE;
* Джеймс Бурман, Центр кибербезопасности для Океании (OCSC);
* Орхан Османи и Марван Бен Ракед, Международный союз электросвязи (МСЭ);
* Мелисса Хэтэуэй и Франческа Спидальери, Потомакский институт политических исследований (PIPS);
* Раду Серрано, Академия электронного государственного управления (eGA);
* Керри-Энн Барретт, Организация американских государств (ОАГ).

Проектная группа выражает признательность Австралийскому институту стратегической политики (ASPI), Агентству Европейского союза по кибербезопасности (ENISA), корпорации MITRE и Всемирному банку за их комментарии и вклад, а также представителю секретариата GFCE Кэтлин Бей за оказанную ею поддержку в области дизайна, материально-технического обеспечения и решения организационных вопросов. Также выражаем благодарность МСЭ за рассмотрение и редактирование данного документа и его перевод на арабский, французский, русский и испанский языки.

Информация и мнения, изложенные в настоящем документе, принадлежат авторам и могут не совпадать с официальной точкой зрения или позицией GFCE, его Секретариата, или его членов и партнеров. Ни GFCE, ни его члены не несут ответственности за последствия использования информации, содержащейся в данной публикации.



**Содержание**

[Введение 4](#_Toc79468196)

Инструменты оценки

[Борьба с киберпреступностью: инструмент оценки развития потенциала 5](#_Toc79468197)

[Киберзрелость стран Азиатско-Тихоокеанского региона 10](#_Toc79468198)

[Индекс киберготовности 2.0 (CRI) 15](#_Toc79468199)

[Модель зрелости потенциала стран в области кибербезопасности (CMM) 20](#_Toc79468200)

[Система разработки и реализации стратегии кибербезопасности (CSDI) 27](#_Toc79468201)

[Глобальный индекс кибербезопасности (GCI) 32](#_Toc79468202)

[Система оценки потенциала стран (NCAF) 37](#_Toc79468204)

[Индекс национальной кибербезопасности (NCSI) 42](#_Toc79468205)

[Обзор инструментов 48](#_Toc79468206)

# Введение

Мировое сообщество предпринимает все более активные попытки понять положение дел в области кибербезопасности разных стран в целях выявления пробелов в этой области и принятия более обоснованных решений по соответствующим мерам и инвестициям, направленным на укрепление потенциала кибербезопасности. Научно-исследовательские институты, региональные организации и компании разработали системы, модели и индексы и применяют их по всему миру, создавая базу знаний о киберзрелости разных стран и их готовности к отражению все возрастающих киберугроз для органов государственного управления, промышленности, бизнеса и граждан.

Положительные отзывы, полученные на сессии по [оценке потенциала кибербезопасности](https://thegfce.org/report-on-the-cyber-capacity-assessments-session/), организованной в рамках виртуального собрания GFCE в апреле 2020 года, подчеркнули необходимость повышения осведомленности о существующих инструментах оценки потенциала кибербезопасности и предоставления подробных сведений о соответствующих методиках, результатах их применения и их влиянии, чтобы помочь сообществу GFCE (бенефициарам, спонсорам и исполнителям) определить подходящие инструменты и подходы, нацеленные на удовлетворение актуальных потребностей и устранение пробелов в знаниях.

Соответственно цель настоящего документа состоит в том, чтобы оказать помощь в процессе принятия решений, предоставляя всесторонний обзор различных инструментов, используемых в них подходов, их преимуществ и результатов, а также информацию о порядке действий и контактную информацию на тот случай, если страна пожелает получить такую оценку.

Целевая группа по стратегии и оценкам GFCE специально отобрала инструменты, предназначенные для оценки потенциала кибербезопасности страны. Исходя из этого критерия в настоящий документ были включены следующие инструменты:

* + Борьба с киберпреступностью: инструмент оценки развития потенциала, Всемирный банк;
  + Киберзрелость стран Азиатско-Тихоокеанского региона, Австралийский институт стратегической политики (ASPI);
  + Индекс киберготовности 2.0 (CRI), Потомакский институт политических исследований (PIPS);
  + Модель зрелости потенциала стран в области кибербезопасности (CMM), Глобальный центр развития потенциала в области кибербезопасности (GCSCC);
  + Система разработки и реализации стратегии кибербезопасности (CSDI), корпорация MITRE;
  + Глобальный индекс кибербезопасности (GCI), Международный союз электросвязи (МСЭ);
  + Система оценки потенциала стран (NCAF), Агентство Европейского союза по кибербезопасности (ENISA);
  + Индекс национальной кибербезопасности (NCSI), Академия электронного государственного управления (eGA).

По мере определения других инструментов, соответствующих вышеуказанному критерию, они будут добавляться в данный документ.

Для целей составления настоящего документа организациям, ответственным за каждый из инструментов, был разослан вопросник, в котором запрашивалась следующая информация:

* исполнитель (исполнители) и контактная информация;
* темы;
* показатели;
* методика, способы сбора данных и контроля качества;
* результаты и способы их представления;
* влияние и преимущества;
* роль в координации деятельности по развитию потенциала кибербезопасности и в процессе поиска партнеров для GFCE.

# Борьба с киберпреступностью: инструмент оценки развития потенциала

## Всемирный банк

Инструмент Всемирного банка *Борьба с киберпреступностью: инструмент оценки развития потенциала* (Инструмент оценки) был разработан в рамках проекта "Борьба с киберпреступностью" для оказания помощи развивающимся странам в определении приоритетных областей в целях содействия распределению их ограниченных ресурсов по развитию потенциала.

Инструмент оценки отличается от других систем оценки тем, что представляет собой инструмент самодиагностики, охватывающий следующие девять параметров: 1) неправовая база; 2) правовая база; 3) материальное право; 4) процессуальное право; 5) электронные доказательства; 6) юрисдикция; 7) гарантии; 8) международное сотрудничество; и 9) развитие потенциала.

Инструмент оценки может использоваться как для самостоятельной деятельности, проводимой страной в собственных целях, так и в качестве важного инструмента комплексной оценки, позволяющего оперативным целевым группам оценивать готовность страны к борьбе с киберпреступностью.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | Последнее обновление опубликовано в 2017 году. Мы ведем работу по обновлению текущей версии инструмента оценки, которую планируется завершить к июлю 2021 года. |
| Как называется инструмент оценки? | Борьба с киберпреступностью: инструмент оценки развития потенциала. |
| Как называется организация, обслуживающая инструмент? | Всемирный банк |
| Кто осуществляет оценку? | Инструмент доступен как глобальный общественный ресурс. Любой желающий может зайти на сайт (см. ниже), загрузить и использовать этот инструмент. Он предназначен для самооценки. |
| Ссылки на инструмент и любая дополнительная информация | <https://www.combattingcybercrime.org/> |
| К кому следует обращаться для обсуждения организации оценки? | Г‑н Дэвид Сатола (David Satola), ведущий юрисконсульт и вице-президент по правовым вопросам Всемирного банка |
| Географический охват | Глобальный |
| Кто может пользоваться инструментом? | * Директивные органы * Законодательные органы * Правоохранительные органы * Представители гражданского общества в развивающихся странах * Все заинтересованные лица |
| Какие темы охвачены? | Концептуально оценка организована по следующим девяти параметрам:   * **неправовая база,** охватывающая национальные стратегии, политику и другие вопросы неправового характера, такие как сотрудничество с частным сектором; * **правовая база,** охватывающая национальные законы и факт присоединения страны к какому-либо договору; * **материальное право,** касающееся незаконной деятельности; |
|  | * **процессуальное право**, касающееся главным образом вопросов ведения следствия; |
|  | * **электронные доказательства** с упором на допустимость цифровых доказательств и обращение с ними в контексте киберпреступности; * **юрисдикция** с упором на способ определения юрисдикции преступления; |
|  | * **гарантии** с упором на следующие три элемента: "надлежащая правовая процедура", защита данных и свобода выражения мнения; * **международное сотрудничество** с упором, во-первых, на процедуру экстрадиции и, во-вторых, на формальный и неформальный уровни взаимной правовой помощи (ВПП); * **развитие потенциала,** как институционального (например, академии подготовки сотрудников правоохранительных органов), так и кадрового, с упором на потребности в обучении сотрудников правоохранительных органов, прокуратуры и судебных органов. |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки   * Меры по укреплению доверия (CBM) и соответствующие нормы * Кибердипломатия   ☒ Международное право в киберпространстве Управление инцидентами и защита критической информационной инфраструктуры (CIIP) ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью   * Регистрация и анализ инцидентов * Учения по кибербезопасности   ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты  * Открытые интернет-стандарты * Интернет вещей |
| Тип показателей | Как количественные, так и качественные показатели |
| Сколько показателей используется и как они применяются? | Инструмент оценки состоит из **115**показателей, сгруппированных по девяти параметрам: неправовая база; правовая база; материальное право; процессуальное право; электронные доказательства; юрисдикция; гарантии; международное сотрудничество и развитие потенциала.  В оценочной таблице девять параметров распределены по четырем уровням. На**уровне 1** обозначается каждая предметная область (параметр). На **уровне 2** устанавливается общая структура каждого из вопросов, которые задаются на **уровне 3** и могут дополнительно уточняться на **уровне 4**.Последний столбец (показатель) предусматривает ответ "да/нет" или выбор одного из набора возможных вариантов ответа. |
| Методика – тип используемой оценки | **В зависимости от ситуации:** группа по борьбе с киберпреступностью проводит первоначальную оценку страны-заказчика в рамках кабинетного исследования, а затем представляет результаты, проверяет и подтверждает оценки совместно с ответственными государственными органами этой страны. |
| Метод сбора первичных данных | * Общедоступная информация * Неопубликованные документы * Анкеты и опросы * Наблюдения * Документы и записи * Собеседование |
| Проводится ли сбор вторичных данных? | Да. После первоначального кабинетного исследования группа посещает страну‑заказчика и консультируется с ответственными государственными органами для проверки и подтверждения первоначальной оценки.   * Наблюдения * Документы и записи |
| Какие механизмы применяются для обеспечения точности собранных данных? | Члены группы по борьбе с киберпреступностью, возглавляемой ведущим юрисконсультом по ИКТ Всемирного банка, обычно обладают опытом/знаниями в области борьбы с киберпреступностью и занимаются во Всемирном банке решением различных вопросов, связанных с ИКТ. Кроме того, первоначальная оценка, проводимая членами группы, проверяется и утверждается ответственными государственными органами страны-заказчика, что гарантирует точность собранных данных. |
| Каковы основные результаты оценки? | В каждом случае составляется отчет об оценке развития потенциала кибербезопасности для каждой страны-заказчика. |
| Формат представления результатов оценки | * Отчет об оценке развития потенциала кибербезопасности (PDF) * Инструмент визуализации (графические диаграммы в формате Excel) |
| Можно ли публиковать результаты оценки? | Да. Однако вопрос о публикации результатов оценки остается на усмотрение страны-заказчика. |
| Как получить доступ к предыдущим отчетам? | Вопрос о предоставлении доступа к предыдущим отчетам остается на усмотрение страны-заказчика. |
| Каковы имеющиеся доказательства оказанного влияния? | Группа провела оценки развития потенциала в области борьбы с киберпреступностью для стран Африки и Азиатско-Тихоокеанского региона, включая Намибию, Эфиопию, Кению, Федеративные Штаты Микронезии и Мьянму. Кроме того, группа получила новые запросы на проведение оценки от 22 стран (Бенин, Бурунди, Демократическая Республика Конго, Гамбия, Либерия, Мали, Нигер, Нигерия, Республика Конго, Сьерра-Леоне, Танзания, Уганда, Замбия, Буркина-Фасо, Кабо-Верде, Коморские Острова, Марокко, Камерун, Мавритания, Руанда и Сенегал).  Кроме того, одна из наших партнерских организаций, Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), приняла Инструмент оценки в качестве своей единственной методики оценки готовности к борьбе с киберпреступностью.  Наконец, группа представила Инструмент оценки на следующих мероприятиях: ежегодное собрание GFCE в Сингапуре (2018 год) и собрания рабочих групп в Гааге (2018 и 2019 годы); ежегодное собрание Совета Европы (СЕ) в Страсбурге (2019 год); ежегодные конференции Международной ассоциации прокуроров (МАП) в Южно-Африканской Республике (2018 год) и Аргентине (2019 год); совместное заседание Совета Европы и Африканского союза (АС) по наращиванию потенциала в области борьбы с киберпреступностью в Африке (2018 год) и Коллоквиум по международному праву в Гонконге (Китай, 2019 год). |
| Какие преимущества дает проведение оценки? | Инструмент оценки позволяет проводить эффективную и универсальную оценку готовности страны к борьбе с киберпреступностью, обеспечивая объективность, полноту и доступность. Сочетание этих трех качеств Инструмента оценки предоставляет директивным и законодательным органам, а также лицам, принимающим решения, возможность выбрать наилучшее решение по распределению ресурсов.   * **Объективность** достигается за счет того, что ответ на каждый вопрос в Инструменте оценки по возможности предусматривает однозначный ответ "да/нет" или, в крайнем случае, четкий выбор из небольшого числа вариантов. * **Полнота** достигается за счет "взвешивания" каждого критерия. В Инструменте оценки используются около 115 показателей, сгруппированных по девяти темам (или параметрам). * **Простота для понимания** достигается благодаря графическому представлению результата оценки в виде единой радиальной диаграммы. Диаграмма помогает стране определить, соответствует ли ее текущая практика передовой международной. Каждый параметр на общей радиальной диаграмме также можно детализировать до уровня, характеризующего эффективность по каждому из подкритериев. |
| Имеется ли процесс расчета весовых коэффициентов? | Да. Однако конкретный процесс расчета весовых коэффициентов не раскрывается пользователям для предотвращения манипуляций с Инструментом оценки. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Нет. Подсчет баллов и ранжирование результатов не предусмотрено. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Имеются ли национальные стратегии и политика в области кибербезопасности? **(Неправовая база)** * Имеется ли внутреннее законодательство по киберпреступности? Присоединялась ли страна к каким-либо международным договорам по противодействию киберпреступности? **(Правовая база)** * Предусмотрено ли в стране уголовное преследование за традиционные преступления, совершаемые с использованием компьютеров или связанные с компьютерами, или за киберпреступления нового типа? **(Материальное право)** * Существуют ли процессуальные законы, регулирующие процесс расследования киберпреступлений и судебного преследования за них? **(Процессуальное право)** * Введены ли в стране правила, касающиеся допустимости электронных доказательств и обращения с ними? **(Электронные доказательства)** * Как страна определяет юрисдикцию киберпреступления? **(Юрисдикция)** * Обеспечивает ли страна "надлежащую правовую процедуру" (защиту данных и свободу выражения мнения) для своих граждан? **(Гарантии)** * Применяла ли страна процедуры экстрадиции или формальные/неформальные принципы ВПП на международном уровне? **(Международное сотрудничество)** * Существуют ли институты или программы по развитию потенциала в области борьбы с киберпреступностью для сотрудников правоохранительных органов, прокуроров и судей? **(Развитие потенциала)** |
| На каких этапах жизненного цикла стратегии проводится оценка? | * На начальном этапе * На этапе обзора и анализа * На этапе разработки стратегии * На этапе реализации * На этапе мониторинга и оценки   Первое применение Инструмента оценки обеспечивает исходный уровень, а периодическое обновление результатов с помощью этого инструмента облегчает контроль достижений. |
| Как оценка помогает согласовать другие виды деятельности? | Инструмент оценки служит для определения приоритетных областей страны по девяти параметрам, что в свою очередь способствует целенаправленному распределению ограниченных ресурсов для разработки национальной стратегии по наращиванию ее потенциала кибербезопасности. Следовательно, Инструмент оценки может использоваться как для самостоятельной деятельности страны, так и в качестве важного инструмента комплексной проверки, позволяющего оперативным целевым группам оценивать готовность страны к борьбе с киберпреступностью. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | Инструмент оценки вносит вклад в процесс поиска партнеров для GFCE, составляя прочную и объективную основу для планирования и осуществления деятельности по наращиванию потенциала кибербезопасности. |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | Как указано выше, преимущества Инструмента оценки были продемонстрированы при успешном проведении оценок развития потенциала кибербезопасности в ряде стран-заказчиков и признаны нашей партнерской организацией УНП ООН, которая теперь использует Инструмент оценки в качестве своей единственной методики оценки готовности к борьбе с киберпреступностью. |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | * Инструмент оценки был проверен и одобрен нашими партнерскими организациями, в том числе Советом Европы, МСЭ, УНП ООН, Конференцией Организации Объединенных Наций по торговле и развитию (ЮНКТАД), Верховной прокуратурой Республики Корея (KSPO) и GCSCC (Оксфордский университет). * Независимая группа экспертов внесла свой вклад в определение веса каждого показателя в Инструменте оценки. |

# Киберзрелость стран Азиатско-Тихоокеанского региона

## Австралийский институт стратегической политики (ASPI)

*Киберзрелость стран Азиатско-Тихоокеанского региона* – это ежегодный отчет, публикуемый Австралийским институтом стратегической политики (ASPI), в котором рассматриваются тенденции в области киберзрелости стран Азиатско-Тихоокеанского региона. В нем исследуется широкий географический и экономический срез региона, куда входят 25 стран Южной, Северной и Юго-Восточной Азии, южной части Тихого океана и Северной Америки.

Методика измерения киберзрелости заключается в оценке различных аспектов кибервозможностей государств. Данная модель была доработана благодаря взаимодействию с экспертами и заинтересованными сторонами в Азиатско-Тихоокеанском регионе, что позволяет ей эффективно оценивать изменения в подходах государств и их технологические достижения. Зрелость в этом контексте демонстрируется наличием, эффективным внедрением и функционированием связанных с киберпространством структур, политики, законодательства и организаций. Эти показатели киберзрелости охватывают общегосударственную политику и законодательные структуры, меры реагирования на финансовые киберпреступления, военную организацию, бизнес и мощь цифровой экономики, а также уровни осведомленности о киберпреступности в обществе.

Информационная научно-исследовательская база, лежащая в основе каждой из этих групп показателей, построена исключительно на основе общедоступной информации; другими словами, выводы отчета основаны исключительно на материалах из открытых источников.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | 2017 год |
| Как называется инструмент оценки? | Киберзрелость стран Азиатско-Тихоокеанского региона |
| Как называется организация, обслуживающая инструмент? | [Австралийский институт стратегической политики (ASPI)](https://www.aspi.org.au/) |
| Кто осуществляет оценку? | [Австралийский институт стратегической политики (ASPI)](https://www.aspi.org.au/) |
| Ссылки на инструмент и любая дополнительная информация | <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017> |
| К кому следует обращаться для обсуждения организации оценки? | Г‑жа Даниэль Кейв, заместитель директора Международного центра киберполитики, ASPI;  г‑н Том Урен, старший аналитик Международного центра киберполитики, ASPI;  г‑н Барт Хогевен, руководитель отдела наращивания потенциала кибербезопасности, ASPI |
| Географический охват | Региональный |
| Кто может пользоваться инструментом? | Все. Отчет находится в открытом доступе. |
| Какие темы охвачены? | 1. Государственное управление  Тема государственного управления относится к организационному подходу государства к вопросам киберсферы, включая состав государственных органов, занимающихся этими вопросами; законодательные намерения и возможности государства; а также участие государства в решении таких вопросов международной киберполитики, как управление интернетом, применение международного права и разработка норм или принципов. Эти показатели служат руководством для взаимодействия дипломатического корпуса, правительства, органов по экономическому развитию, правоохранительных органов и частного сектора в странах Азиатско-Тихоокеанского региона.  2. Борьба с финансовой киберпреступностью  Финансовая киберпреступность – критически важная проблема для всех государств Азиатско-Тихоокеанского региона. Последствия киберпреступлений для простых людей в регионе значительны и связаны с существенными финансовыми потерями. Оценка способности государства бороться с финансовой киберпреступностью может служить ориентиром для участия в правоприменительной деятельности, в том числе посредством обмена информацией и оказания помощи в развитии потенциала со стороны государственного и частного секторов.  3. Военное применение  Эта тема касается военной организационной структуры государства (если таковая имеется), связанной с киберпространством, и известных взглядов государства на использование киберпространства его вооруженными силами. Это может служить ориентиром для взаимодействия между вооруженными силами государств, а также для дипломатического и военно-политического взаимодействия. Использование киберпространства в военных целях, особенно национальные потенциалы, – деликатная тема для всех стран Азиатско-Тихоокеанского региона, поэтому данная область требует тщательного рассмотрения, чтобы государства стремились или соглашались взаимодействовать друг с другом.  4. Цифровая экономика и бизнес  Понимает ли государство важность киберпространства и цифровой экономики и то, насколько, по его мнению, они важны в экономическом плане, – один из показателей киберзрелости. Данный показатель может служить ориентиром для взаимодействия по наращиванию потенциала, развития региональных деловых связей и взаимодействия между государством и бизнесом по вопросам кибербезопасности.  5. Социальная вовлеченность  Осведомленность общества и его участие в решении проблем кибербезопасности, таких как управление интернетом, цензура в интернете и киберпреступность, указывают на зрелость общественного дискурса между государством и его гражданами. Образовательные программы по вопросам ИКТ и киберпространства также могут указывать на высокий уровень понимания технических вопросов и проблем.  Доля населения, имеющего доступ к интернету, указывает на тип бизнеса и личного участия в киберпространстве, качество инфраструктуры ИКТ и уровень доверия граждан государства к цифровой торговле. Этот показатель может служить ориентиром для органов по развитию, стремящихся построить региональную экономику, и предприятий, желающих развивать торговлю в регионе. |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки  ☒ CBM и соответствующие нормы  ☒ Кибердипломатия  ☒ Международное право в киберпространстве Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью   * Регистрация и анализ инцидентов * Учения по кибербезопасности   ☒ Защита критической информационной инфраструктуры |
|  | Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве   * Подготовка по вопросам киберпреступности * Предупреждение киберпреступности |
|  | Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов |
|  | Стандарты  * Открытые интернет-стандарты * Интернет вещей |
| Тип показателей | Количественные и качественные показатели |
| Сколько показателей используется и как они применяются? | "Мера киберзрелости" состоит из 10 показателей.  Эти показатели имеют весовые коэффициенты в соответствии с их важностью для киберзрелости государства. Группа экспертов по кибербезопасности и заинтересованных сторон из государственных учреждений и предприятий частного сектора оценила их по шкале от 1 до 10, где 1 означает "совсем не важно", а 10 – "чрезвычайно важно".  Затем эти экспертные оценки для каждой категории были усреднены для получения весового коэффициента, который можно использовать при вычислении общей оценки.  На последнем этапе каждая страна оценивалась по 10 параметрам по шкале от 0 до 10 (10 – наивысший уровень зрелости). Оценки основывались на качественных и количественных исследованиях обширной информации из открытых источников и, где это возможно, на сравнении с исследованиями и результатами, полученными в 2014, 2015 и 2016 годах.  Общая оценка каждой страны представляла собой сумму оценок по каждому фактору, взвешенных по средней расчетной значимости. Для облегчения интерпретации общие оценки преобразовывались в процент от наивысшей возможной оценки с учетом присвоенных весов:  ,  где – взвешенная оценка, *S* – оценка и *w* – весовой коэффициент. |
| Методика – тип используемой оценки | Сравнительная с ранжированием |
| Метод сбора первичных данных | Информация из открытых источников |
| Проводится ли сбор вторичных данных? | * Собеседования * Анкеты и опросы * Наблюдения * Оперативные группы |
| Какие механизмы применяются для обеспечения точности собранных данных? | Посольствам и высоким комиссиям стран, охваченных отчетом, предлагается проверить профиль их страны на наличие фактологических ошибок. |
| Каковы основные результаты оценки? | * Профили отдельных стран * Региональный сравнительный рейтинг * Обзор региональных тенденций * Оценка возможностей международного взаимодействия |
| Формат представления результатов оценки | Отчет |
| Можно ли публиковать результаты оценки? | Да. Результаты публикуются в отчете. |
| Как получить доступ к предыдущим отчетам? | <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016>  <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015>  <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2014> |
| Каковы имеющиеся доказательства оказываемого влияния? | См. ответ на вопрос о свидетельствах, ниже. |
| Какие преимущества дает проведение оценки? | См. ответ на вопрос об этапах жизненного цикла стратегии, на которых проводится оценка, ниже. |
| Имеется ли процесс расчета весовых коэффициентов? | Да. См. ответ на вопрос о показателях и их применении, выше. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Да. См. ответ на вопрос о показателях и их применении, выше. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | Каковы региональные тенденции в области киберзрелости в Азиатско‑Тихоокеанском регионе?  Как страны Азиатско-Тихоокеанского региона сопоставляются по пяти направлениям политики, составляющим киберзрелость?  Какие возможности для международного взаимодействия имеются у стран Азиатско-Тихоокеанского региона? |
| На каких этапах жизненного цикла стратегии проводится оценка? | Азиатско-Тихоокеанский регион рассматривается в сравнительной перспективе.  Отчеты лучше всего подходят для разработки национальной киберстратегии на начальном этапе, этапе обзора, а также на этапе мониторинга и оценки (M&E).  При разработке регионального подхода или создании региональной картины инструмент подходит для определения повестки дня, стратегического анализа и сравнения национальных практик.  Годовой цикл отчета делает его ценным для контроля и оценки, а также анализа тенденций. |
| Как оценка помогает согласовать другие виды деятельности? | Отчет представляет собой авторитетный источник анализа, основанного на фактах и свидетельствах, полезный для лиц, определяющих политику на национальном и региональном уровнях, в государственном и частном секторах. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | Отчет предоставляет потенциальные отправные точки для переговоров между получателями и поставщиками услуг по наращиванию потенциала кибербезопасности. |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | Как правило, этот отчет отражается в СМИ:   * <https://www.zdnet.com/article/only-us-tops-australia-in-asia-pacific-cyber-maturity-aspi/> * <https://www.theaustralian.com.au/commentary/opinion/threat-posed-by-evil-nations-and-criminals-in-cyberland-is-rising/news-story/fdebd93f3dc0206afe0705e6f6ec045c> * [https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in- asiapacific-region-379580.vov](https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in-%20asiapacific-region-379580.vov) * <https://theaseanpost.com/article/cyberattack-malaysia-imminent-or-imagined>   На отчет ссылаются в выступлениях, в том числе ведущие (австралийские) политики:   * <https://www.rusi.org.au/resources/Documents/2015_10_05%20Brodtman.pdf>   Отчет используется в качестве источника в других политических и научных публикациях, например:   * <https://www.austcyber.com/resources/sector-competitiveness-plan/executive-summary> * <https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Maurer_Tim_Web.pdf> * <https://www.standards.org.au/getmedia/952ea009-ffc2-490a-905f-8f731fa84a52/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx> |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | Будучи признанным аналитическим центом, ASPI руководствуется своим уставом, в котором закреплены принципы независимости и беспристрастности. Кроме того, отчет составляется на основе открытых и проверяемых источников. Наблюдения или выводы не подлежат утверждению какими бы то ни было государственными органами или источниками финансирования и соответствуют общепринятым стандартам аналитической строгости. |
| Дополнительная информация | Предыдущий отчет был опубликован в декабре 2017 года в ожидании нового цикла финансирования и переоценки потенциальных результатов исследований. |

# Индекс киберготовности 2.0 (CRI)

## Потомакский институт политических исследований (PIPS)

*Индекс киберготовности 2.0* (CRI) представляет собой комплексную, сравнительную, основанную на опыте методику оценки ответственного подхода и зрелости стран в отношении защиты своей национальной цифровой инфраструктуры и услуг, от которых зависит их экономический рост и национальная устойчивость. CRI 2.0 основан на индексе киберготовности 1.0 2013 года – первой методической системе оценки киберготовности. Инструмент оценки CRI помогает странам выявить имеющиеся пробелы, укрепить положение дел в области кибербезопасности и лучше управлять киберрисками на национальном уровне.

С 2013 года CRI применялся более чем к 100 странам, и было подготовлено 14 подробных отчетов.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | Мы регулярно добавляем новые вопросы и показатели к каждому из семи основных элементов инструмента. |
| Как называется инструмент оценки? | Индекс киберготовности 2.0. |
| Как называется организация, обслуживающая инструмент? | [Потомакский институт политических исследований (PIPS)](https://www.potomacinstitute.org/academic-centers/cyber-readiness-index) |
| Кто осуществляет оценку? | Члены группы киберготовности (г‑жа Мелисса Хэтэуэй  и г‑жа Франческа Спидальери) |
| Ссылки на инструмент и любая дополнительная информация | * Веб-сайт PIPS: <https://www.potomacinstitute.org/academic-centers/cyber-readiness-index> * Портал Cybil: <https://cybilportal.org/tools/cyber-readiness-index-2-0/> |
| К кому следует обращаться для обсуждения организации оценки? | * Мелисса Хэтэуэй, старший научный сотрудник PIPS и главный исследователь CRI: hathawayglobal@icloud.com * Франческа Спидальери, соисследователь CRI: francescaspidalieri@gmail.com |
| Географический охват | Глобальный |
| Кто может пользоваться инструментом? | * Руководство стран * Национальные/региональные правительства * Министерства/государственные учреждения * Учреждения по кибербезопасности/лица, определяющие политику * Высшие учебные заведения * Специалисты по кибербезопасности * Отдельные исследователи |
| Какие темы охвачены? | В CRI 2.0 используются более 70 уникальных показателей в рамках семи основных элементов, которые позволяют выделить зрелые виды деятельности и определить области, нуждающиеся в совершенствовании, по следующим категориям.  **1. Национальная стратегия:** публикация национальной стратегии; назначение компетентного органа; определение ключевых государственных и коммерческих структур, ответственных за реализацию; механизмы защиты критической инфраструктуры; определение критически важных служб; определение национальных стандартов по непрерывности предоставления услуг.  **2. Реагирование на инциденты:** публикация плана реагирования на инциденты; выявление межотраслевых взаимозависимостей; данные, свидетельствующие о выполнении и обновлении плана; публикация оценки киберугроз; создание группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT); финансовые и людские ресурсы.  **3. Электронная преступность и правоохранительная деятельность:** ратификация международного договора о киберпреступности; усилия по сокращению уровня электронной преступности; институциональная способность бороться с киберпреступностью; готовность пересмотреть существующие законы и механизмы; усилия по очистке зараженной инфраструктуры; обучение сотрудников правоохранительных органов и развитие потенциала.  **4. Обмен информацией:** политика обмена информацией; институциональная структура для обмена информацией с государственными учреждениями и/или промышленными предприятиями; свидетельства наличия механизмов межсекторальной координации и координации между заинтересованными сторонами; готовность правительства к рассекречиванию разведывательной информации и соответствующие процессы.  **5. Инвестиции в научные исследования и разработки, образование и потенциал:** механизмы государственного стимулирования инноваций и инвестиций в области кибербезопасности; финансовые и людские ресурсы для научных исследований и разработок и передачи технологий; программы на получение степени в области кибербезопасности; спонсорская поддержка кампаний по повышению осведомленности и образовательных программ в области кибербезопасности.  **6. Дипломатия и торговля:** определение кибербезопасности как важного элемента внешней политики и международных переговоров по экономическому развитию; создание специального подразделения кибердипломатии в министерстве иностранных дел страны; участие в международных, многонациональных и региональных соглашениях по кибербезопасности и обеспечение их соблюдения.  **7. Оборона и реагирование на кризисные ситуации:** создание национальной военной и/или гражданской организации по киберзащите; данные, свидетельствующие о проведении киберучений национального уровня с участием коммерческих и/или международных партнеров; установление стандартов ответственного поведения государства в киберпространстве; создание механизмов оперативной помощи.  Полное описание каждого элемента см. в подробной методике: https://www.potomacinstitute.org/images/CRIndex2.0.pdf |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки  ☒ CBM и соответствующие нормы  ☒ Кибердипломатия  ☒ Международное право в киберпространстве Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью  ☒ Регистрация и анализ инцидентов  ☒ Учения по кибербезопасности  ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты |
| Тип показателей | Данные, собираемые в рамках CRI 2.0, носят качественный характер, и каждый показатель оценивается по четырем ключевым категориям: 1) заявления/стратегии/политика; 2) организация/компетентный орган; 3) ресурсы; и 4) реализация. |
| Сколько показателей используется и как они применяются? | В CRI 2.0 используются более 70 показателей в рамках семи основных элементов, позволяющих оценить зрелость страны в области кибербезопасности и выделить системы, которые являются полностью действующими, частично действующими или такими, по которым недостаточно сведений.  Все показатели CRI 2.0 имеют общую структуру, и вопросы, которые ставятся в одной версии методики, сопоставимы с аналогичными вопросами предыдущих или будущих версий. Каждому показателю присваивается одинаковый вес, а затем этот показатель описывается в отчете по стране в рамках более широкого контекста, основанного на потребностях, возможностях, приоритетах и целях данной страны. |
| Методика – тип используемой оценки | Для оценки киберзрелости и разработки подробных профилей стран в CRI 2.0 используются первичные источники, включая национальные стратегии, политику, законодательство, официальные заявления руководства, национальные оценки и отчеты и т. д.   Страны не сравниваются друг с другом. |
| Метод сбора первичных данных | * Информация из открытых источников * Неопубликованные или официальные конфиденциальные документы * Собеседования/наблюдения * Документы и записи |
| Проводится ли сбор вторичных данных? | Да. Сбор вторичных данных проводится для подтверждения, исправления или расширения информации, собранной в ходе анализа первичных источников и собеседования с официальными лицами страны и специалистами. |
| Какие механизмы применяются для обеспечения точности собранных данных? | Все исследования основываются на первичных источниках и официальной документации, а затем подтверждаются официальными лицами и/или специалистами страны. |
| Каковы основные результаты оценки? | Подробные отчеты по странам публикуются на веб-сайте PIPS на всех шести языках ООН и общедоступны.  Эти отчеты помогают правительствам разработать собственные подходы и политику в области кибербезопасности и составить действенный приоритетный план, необходимый для укрепления позиций страны в области кибербезопасности. Это позволяет им определить меры, которые необходимо принять для снижения рисков, независимо от имеющегося внутреннего опыта. |
| Формат представления результатов оценки | * Подробные отчеты по странам * Инструмент визуализации (лепестковая диаграмма и диаграмма "кружки́ Харви") * Презентация PowerPoint, по просьбе страны |
| Можно ли публиковать результаты оценки? | Да. Все отчеты CRI по странам общедоступны на веб-странице CRI PIPS: <https://www.potomacinstitute.org/academic-centers/cyber-readiness-index> |
| Как получить доступ к предыдущим отчетам? | См. выше. |
| Каковы имеющиеся доказательства оказанного влияния? | CRI оказал непосредственное влияние на политику в области киберготовности и на мышление руководства следующих стран и организаций: Австралия, Азербайджан, Бангладеш, Босния и Герцеговина, Болгария, Канада, Китай, Чешская Республика, Египет, Эстония, Франция, Грузия, Германия, Исландия, Индия, Индонезия, Израиль, Италия, Япония, Иордания, Кыргызстан, Литва, Мексика, Нидерланды, Новая Зеландия, Оман, Филиппины, Польша, Румыния, Саудовская Аравия, Сербия, Словакия, Южно-Африканская Республика, Швеция, Швейцария, Украина, Соединенное Королевство; Африканский форум групп реагирования на компьютерные инциденты (Africa CERT), Группа реагирования на нарушения компьютерной защиты Азиатско-Тихоокеанского региона (APCERT), МСЭ, Межамериканский банк развития (МАБР), Организация Североатлантического договора (НАТО), Совет Северных стран, Организация американских государств ( ОАГ) и Всемирный банк.  CRI продолжает оказывать глобальное влияние, и Мелисса Хэтэуэй, главный специалист по CRI, способствует просвещению по этим вопросам руководителей государств. Ее регулярно приглашают на международные встречи и дискуссии на высшем уровне, она представлена в многочисленных международных публикациях и продолжает информировать руководителей государств о практичности использования CRI 2.0 в качестве инструмента планирования/сравнительного анализа и обеспечения участия различных заинтересованных сторон в усилиях стран и процессах в области кибербезопасности, а также увеличения финансирования для наращивания их потенциала в этой области. |
| Какие преимущества дает проведение оценки? | Оценка CRI 2.0 помогает странам выявить разрыв между нынешним положением их дел в области кибербезопасности и национальными кибервозможностями, требуемыми для поддержки цифрового будущего этих стран. Инструмент также можно использовать для оценки положения страны на кривой зрелости с общегосударственной и общенациональной точек зрения. Взятые вместе, эти показатели помогают правительствам оценить и согласовать свои инициативы в области цифровой и национальной безопасности. С помощью собранных данных CRI также позволяет выявить передовой опыт, который страны могут внедрить для облегчения усилий по обеспечению киберготовности в различных отраслях и секторах и содействия этим усилиям. CRI 2.0 указывает средства, включая политику, законодательство, нормативные акты, стандарты, рыночные стимулы и другие инициативы, которые могут использовать руководители государств для защиты своих инвестиций в цифровые технологии и решения проблемы экономических потерь, связанных с кибербезопасностью.  Такая оценка помогает руководителям государств осознать, что для полной реализации потенциала цифровой экономики в отношении экономического роста, повышения производительности и эффективности труда, повышения квалификации кадров и улучшения доступа к бизнесу и информации необходимо согласовать стратегии экономического развития с приоритетами национальной безопасности. Она показывает, как ИКТ могут обеспечить экономический рост, но лишь при условии проведения правильной политики, внедрения надлежащих процессов и технологий для обеспечения защиты и безопасности киберинфраструктуры и киберуслуг, от которых зависит цифровое будущее и экономический рост страны. |
| Имеется ли процесс расчета весовых коэффициентов? | Да. В своей внутренней базе данных мы присваиваем весовой коэффициент 5,0 показателям полностью действующих систем, 3,0 – показателям систем, действующих частично, и 1,0 – если определенные элементы системы засекречены или отсутствуют достаточные свидетельства их существования или реализации. Расчет весовых коэффициентов используется не для ранжирования стран, а лишь для построения лепестковых диаграмм и других способов визуализации. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | CRI 2.0 дает оценку зрелости по каждому из основных элементов, но не ранжирует страны. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Согласованы ли краткосрочные и долгосрочные цели страны, включая цифровую повестку дня, промышленную политику, экономические цели и приоритеты национальной безопасности, с ее национальной стратегией кибербезопасности? * Какие виды киберугроз могут помешать достижению этих целей? * Каковы наиболее важные цифровые ресурсы страны (например, компании, услуги, инфраструктура и активы), нарушение работы которых может иметь серьезные последствия для экономики и национальной безопасности? * Существуют ли четкие рамки подотчетности и ответственности для обеспечения достижения целей страны и реализации мер по снижению рисков? * Являются ли вопросы кибербезопасности и устойчивости ключевой частью процесса планирования? * Какие шаги может предпринять страна, чтобы стать более устойчивой в отношении цифровых технологий?   CRI 2.0 также может использоваться в качестве эталона для определения странами разрыва между текущим положением дел в области кибербезопасности в стране и национальными кибервозможностями, необходимыми для устранения недостатков и поддержки их будущих приоритетов в сфере экономики и безопасности. Руководство стран может использовать CRI 2.0 для облегчения усилий по обеспечению киберготовности в различных отраслях и секторах экономики и содействия этим усилиям, тем самым уделяя постоянное внимание взаимосвязи между цифровой и промышленной стратегиями и своими приоритетами в области национальной безопасности. |
| На каких этапах жизненного цикла стратегии проводится оценка? | Методика CRI должна быть частью жизненного цикла всей стратегии, и этот инструмент оценки может использоваться до и/или после разработки национальной стратегии кибербезопасности, в том числе на следующих этапах: начальном, отбора и анализа, разработки стратегии, реализации, мониторинга и оценки, обновления стратегии. |
| Как оценка помогает согласовать другие виды деятельности? | CRI 2.0 связывает экономический рост и развитие с национальной политикой в области безопасности и таким образом помогает странам лучше согласовать национальную стратегию кибербезопасности со стратегиями цифрового развития и экономического роста страны. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | CRI 2.0 может подтверждать или дополнять другие инструменты оценки, предлагаемые сообществом GFCE, включая CMM Оксфордского университета и GCI МСЭ. |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | Помимо использования всеми вышеперечисленными странами и международными организациями для определения их политики и стратегий, методика CRI цитировалась или использовалась в многочисленных статьях, докладах, брифингах, отчетах и производных публикациях. Например, ОАГ и МАБР использовали методику и базу данных CRI 2.0 для подтверждения и проверки своего международного отчета об уровне киберпотенциала и киберготовности государств-членов ([Cybersecurity: Are We Ready in Latin America and the Caribbean?](https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean)). Команда CRI активно сотрудничала с МСЭ в вопросах обмена данными, согласования усилий и усиления воздействия, а также участвовала в работе над двумя основополагающими проектами МСЭ по кибербезопасности – разработке второго издания Глобального индекса кибербезопасности (GCI) МСЭ и подготовке силами многих партнеров под эгидой МСЭ [Руководства по разработке национальной стратегии кибербезопасности](https://www.potomacinstitute.org/divisions/34-science-and-technology-policy/cyber-readiness/cyber-readiness-news/200-the-cyber-readiness-index-contributes-to-the-international-telecommunications-union-s-national-cybersecurity-strategy-guide-2).  Дополнительные сведения по CRI 2.0 можно найти в публикациях в СМИ, приведенных в разделе новостей по киберготовности: <https://www.potomacinstitute.org/academic-centers/cyber-readiness-index> |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | Отчеты по странам основаны на данных из первичных источников и независимо проверены нашей экспертной группой. |

# Модель зрелости потенциала стран в области кибербезопасности (CMM)

## Глобальный центр развития потенциала в области кибербезопасности (GCSCC), Оксфордский университет и партнеры

*Модель зрелости потенциала стран в области кибербезопасности* (CMM), разработанная Глобальным центром развития потенциала в области кибербезопасности (GCSCC) при Оксфордском университете, служит для оценки потенциалов стран в области кибербезопасности по пяти параметрам, тем самым позволяя странам проводить самооценку, лучше планировать инвестиции и национальные стратегии кибербезопасности и устанавливать приоритеты в сфере развития потенциала. С 2015 года проведено свыше 110 обзоров потенциала кибербезопасности (CMM) более чем в 80 странах.

GCSCC и его партнеры определяют потенциал кибербезопасности в широком смысле как охватывающий политику, стратегию, социальные и культурные факторы, образование и обучение, нормативно-правовую базу, а также кибертехнологии и стандарты. В соответствии с этим определением подход Центра к исследованиям носит междисциплинарный характер, так что потенциал кибербезопасности рассматривается во всех его измерениях с различных научных точек зрения.

Модель CMM разрабатывалась с намерением исследовать нюансы наращивания потенциала в этих нескольких измерениях; определить виды деятельности, позволяющие обеспечить и повысить потенциал; выявить передовой опыт; определить условия, при которых можно добиться роста потенциала, и понять, как измерения (параметры) связаны друг с другом и зависят друг от друга. CMM также обеспечивает структуру, которая позволяет сравнивать потенциал кибербезопасности в разных странах и в разные периоды времени. Используемая методика служит для сбора информации от различных групп участников и заинтересованных сторон, чтобы отразить широкий взгляд на потенциал кибербезопасности в каждой стране.

### Обзор

|  |  |  |
| --- | --- | --- |
| Дата последнего обновления инструмента | Март 2021 года | |
| Как называется инструмент оценки? | Модель зрелости потенциала стран в области кибербезопасности (CMM), редакция 2021 года | |
| Как называется организация, обслуживающая инструмент? | [Глобальный центр развития потенциала в области кибербезопасности (GCSCC)](https://gcscc.ox.ac.uk/)  [Центр кибербезопасности для Океании (OCSC)](https://ocsc.com.au/)  [Центр развития потенциала кибербезопасности для юга Африки (C3SA)](http://www.c3sa.uct.ac.za/) | |
| Кто осуществляет оценку? | Глобальный центр развития потенциала в области кибербезопасности (GCSCC), Центр кибербезопасности для Океании (OCSC), Центр развития потенциала кибербезопасности для юга Африки (C3SA), Организация американских государств (OAГ), Всемирный банк, компания NRD Cyber Security  Партнеры по реализации  Международный союз электросвязи (МСЭ); Глобальный форум по киберкомпетентности (GFCE); Организация электросвязи Содружества (ОЭС); Сетевой информационный центр Азиатско-Тихоокеанского региона (APNIC); Азиатско-Тихоокеанское сообщество электросвязи (АТСЭ); Норвежский институт международных отношений (NUPI); компания German Corporation for International Cooperation GmbH (GIZ), Германия | |
| Ссылки на инструмент и любая дополнительная информация | <https://gcscc.ox.ac.uk/the-cmm> | |
| К кому следует обращаться для обсуждения организации оценки? | [GCSCC](mailto:GCSCC), все страны, г‑жа Кэролин Вайссер Харрис: [carolin.weisser@cs.ox.ac.uk](mailto:carolin.weisser@cs.ox.ac.uk)  [OCSC](https://ocsc.com.au/), регион Океании, г‑н Джеймс Бурман: [james.boorman@ocsc.com.au](mailto:james.boorman@ocsc.com.au)  [C3SA](http://www.c3sa.uct.ac.za/), Африканский регион, г‑жа Нтабисенг Пуле: [npule@researchictafrica.net](mailto:npule@researchictafrica.net) | |
| Географический охват | Глобальный |
| Кто может пользоваться инструментом? | Все.  CMM является общедоступным документом. Для проведения обзора CMM рекомендуется сотрудничать с одним из разработчиков, знакомым с [методикой CMM](https://gcscc.ox.ac.uk/cmm-review-process). |
| Какие темы охвачены? | CMM оценивает потенциал кибербезопасности по пяти параметрам, имеющим решающее значение для создания потенциала страны в области кибербезопасности.    **Параметр 1(*политика и стратегия в области кибербезопасности*)** позволяет исследовать возможности страны по разработке и реализации стратегии кибербезопасности и повышению устойчивости кибербезопасности за счет повышения ее потенциала в области реагирования на инциденты, киберзащиты и защиты критической инфраструктуры. Этот параметр оценивает эффективность стратегии и политики по обеспечению национального потенциала кибербезопасности при сохранении преимуществ использования киберпространства, жизненно важных для государственного управления, международного бизнеса и общества в целом.  **Параметр 2 (*культура кибербезопасности и общество*)** позволяетрассмотреть важные элементы культуры ответственной кибербезопасности, такие как понимание рисков, связанных с кибербезопасностью в обществе, уровень доверия к интернет-услугам, электронному правительству и услугам электронной коммерции, а также понимание пользователями способов защиты персональной информации в онлайновой среде. Более того, этот параметр позволяет определить наличие механизмов отчетности, действующих в качестве каналов связи для передачи пользователями сообщений о кибепреступлениях. Кроме того, он оценивает роль СМИ и социальных сетей в формировании ценностей, отношений и поведения в сфере кибербезопасности.  **Параметр 3 (*наращивание знаний и потенциала в области кибербезопасности*)** позволяетоценить доступность, качество и популярность программ для различных групп заинтересованных сторон, включая органы государственного управления, предприятия частного сектора и население в целом, и относится к программам повышения осведомленности о кибербезопасности, официальным образовательным программам по кибербезопасности и программам профессиональной подготовки.  **Параметр 4 (*нормативно-правовая база*)** позволяет исследовать способность органов государственного управления разрабатывать и принимать национальные законы, прямо или косвенно относящиеся к кибербезопасности, с особым акцентом на нормативные требования по кибербезопасности, законодательство, связанное с киберпреступностью, и другие соответствующие законы. Возможность обеспечить соблюдение таких законов изучается по потенциалу правоохранительных органов, прокуратуры, регуляторных и судебных органов. Кроме того, в рамках этого параметра рассматриваются такие вопросы, как формальные и неформальные механизмы сотрудничества в области борьбы с киберпреступностью.  **Параметр 5 (*стандарты и технологии*)** относится к эффективному и повсеместному использованию технологий кибербезопасности для защиты людей, организаций и национальной инфраструктуры. В частности, этот параметр позволяет конкретно изучить вопросы внедрения стандартов кибербезопасности и передового опыта, развертывания процессов и средств контроля, а также разработки технологий и продуктов для снижения рисков кибербезопасности. |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки  ☒ CBM и соответствующие нормы  ☒ Кибердипломатия   * Международное право в киберпространстве  Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью  ☒ Регистрация и анализ инцидентов  ☒ Учения по кибербезопасности  ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты |
| Тип показателей | Качественные показатели |
| Сколько показателей используется  и как они применяются? | CMM охватывает около 600 показателей для оценки зрелости по пяти параметрам, имеющим решающее значение для создания потенциала страны в области кибербезопасности: *политика и стратегия в области кибербезопасности; культура кибербезопасности и общество; наращивание знаний и потенциала в области кибербезопасности; нормативно-правовая база; а также стандарты и технологии.*  Каждый ***параметр*** CMM включает набор ***факторов***, которые описывают и определяют, что значит обладать потенциалом кибербезопасности. Большинство факторов разбиты на несколько ***аспектов***. Каждому фактору/аспекту соответствует ряд ***показателей*** в рамках пяти ***стадий*** зрелости: *начальная, формирующаяся, устоявшаяся, стратегическая* и *динамичная.* Эти показатели описывают шаги и действия, которые необходимо предпринять для достижения или поддержания данной стадии зрелости в иерархии аспектов/факторов/параметров.  Для того чтобы страна могла продемонстрировать степень своей зрелости в рамках данного аспекта/фактора, ей необходимо подтвердить каждый показатель; в противном случае нельзя считать, что она перешла к следующему этапу оценки. |
| Методика – тип используемой оценки | Развертывание CMM – это многоэтапный процесс с участием нескольких заинтересованных сторон, состоящий из трех основных этапов:   1. проведение группой по осуществлению кабинетных исследований с учетом обстановки; 2. обсуждения в течение трех-четырех дней в адаптированных оперативных группах внутри страны с участием ключевых заинтересованных сторон, таких как научные круги, органы уголовного судопроизводства, правоохранительные органы, специалисты по информационным технологиям и представители организаций государственного сектора, владельцы критической инфраструктуры, лица, определяющие политику, специалисты по информационным технологиям из органов государственного управления и предприятий частного сектора (включая финансовые учреждения), компании по электросвязи, банковский сектор, а также представители гражданского общества и международные партнеры; 3. подробный отчет CMM с описанием контекста кибербезопасности внутри страны, суммированием результатов по каждому фактору и аспекту CMM, указанием этапов зрелости потенциала кибербезопасности и рекомендациями по повышению потенциала кибербезопасности страны. Отчет проходит рецензирование Техническим советом GCSCC и передается в органы государственного управления для представления замечаний.   Дополнительную информацию можно получить на веб-странице: <https://gcscc.ox.ac.uk/cmm-review-process> |
| Метод сбора первичных данных | * Адаптированные оперативные группы (сбор основных первичных данных) * Анкеты и опросы (региональные исследования ОАГ) * Собеседования (необязательно в целях получения дополнительных фактических данных) |
| Проводится ли сбор вторичных данных? | Да (в рамках кабинетного исследования до/после оперативных групп CMM)   * Информация из открытых источников * Неопубликованные документы * Документы и записи * Анкеты и опросы |
| Какие механизмы применяются для обеспечения точности собранных данных? | * Каждое обсуждение в адаптированной оперативной группе CMM относится к одному или нескольким параметрам, что позволяет собирать фактические данные по каждому параметру как минимум дважды. Это также позволяет провести триангуляцию и получить разные ответы на один и тот же вопрос от разных заинтересованных сторон. * С предварительного согласия собрания адаптированных оперативных групп CMM протоколируются, и некоторые из тех, кто осуществляет оценку, используют анонимные стенограммы этих собраний для анализа ответов на вопросы с учетом всех собранных данных. * Кабинетное исследование подтверждает данные, поступившие от адаптированных оперативных групп CMM. * Отчет CMM проходит рецензирование Техническим советом GCSCC и передается в органы государственного управления для представления замечаний. * Некоторые из тех, кто осуществляет оценку, используют инструмент структурированного кодирования полей (SFC), который позволяет вводить и кодировать ответы, полученные из кабинетных исследований и от оперативных групп CMM, чтобы проверять показатели на каждом этапе обзора. Эти методы получили развитие с появлением инструмента SFC, что свидетельствует о постоянном стремлении к совершенствованию методики обзора CMM. |
| Каковы основные результаты оценки? | Отчет, основанный на фактических данных, который передается органам государственного управления. |
| Формат представления результатов оценки | * Письменный отчет с рекомендациями (PDF) * Резюме для заказчика (необязательно) * Заключительный семинар с участием заказчика и основных заинтересованных сторон (необязательно) * Инструмент визуализации (OAГ: <https://www.cybersecurityobservatory.org>) |
| Можно ли публиковать результаты оценки? | Да.  Органы государственного управления оставляют за собой право распространять и/или публиковать отчет или любую его часть. |
| Можно ли получить доступ к предыдущим отчетам, и если да, то как? | Все оценки CMM со ссылками на опубликованные отчеты можно найти на следующих веб-сайтах:   * <https://gcscc.ox.ac.uk/cmm-reviews> * <https://cybilportal.org/tools/portal-of-cybersecurity-capacity-maturity-model-cmm-review-reports/>   (Информацию о статусе отчета можно получить на [портале Cybil](https://cybilportal.org/), выполнив поиск по ключевым словам "CMM+название страны") |
| Каковы имеющиеся доказательства оказанного влияния? | Независимая оценка выборки внедрений CMM в феврале 2020 года показала, что:   * обзор CMM способствовал повышению осведомленности о кибербезопасности и наращиванию потенциала; * обзор CMM способствовал расширению сотрудничества в органах государственного управления; * некоторые страны (например, Северная Македония, Литва и Грузия) назвали CMM основой разработки своей стратегии и политики; * обзор CMM повысил внутреннее доверие в органах государственного управления к повестке дня в области кибербезопасности; * обзор CMM помог определить роли и обязанности внутри органов государственного управления, а также привел к увеличению финансирования программ наращивания потенциала кибербезопасности; * обзор CMM помог обеспечить общение и сотрудничество с бизнес‑сообществом и обществом в целом.   Обзор CMM был проведен более 120 раз, программы CMM развернуты более чем в 85 странах, ведется работа с национальными правительствами во всех регионах мира. В частности:   * Организацией американских государств (ОАГ) проведены два региональных исследования (в [2016 и 2020 годах](https://www.cybersecurityobservatory.org/%23/final-report)); * проведено более 25 обзоров в сотрудничестве со Всемирным банком и Корейским агентством по интернету и безопасности (KISA) по их глобальным программам развития потенциала кибербезопасности [этапа I](https://cybilportal.org/projects/global-cybersecurity-capacity-program-i/) и [этапа II](https://cybilportal.org/projects/global-cybersecurity-capacity-program-ii/) и в рамках [Обзоров национального потенциала кибербезопасности (CMM) для Содружества](https://cybilportal.org/projects/national-cybersecurity-capacity-cmm-reviews-for-the-commonwealth/) и портфеля программ ЭКОВАС; * создана группа реагирования на нарушение компьютерной защиты (CERT) и проведена оценка потенциала стран Тихоокеанского региона силами МСЭ, АТСЭ, APNIC и других партнеров; * обеспечено развитие потенциала кибербезопасности в странах Содружества силами ОЭС.   Данные обзора CMM использовались в следующих научных статьях:   * Creese, S., Shillair, R., Bada, M., Reisdorf, B. C., Roberts, T. and Dutton, W. H. (2019). ‘The Cybersecurity Capacity of Nations’, pp. 165‑179 in Graham, M. and Dutton, W. H. (eds), *Society and the Internet: How Networks of Information and Communication are Changing our Lives*, 2nd edition. Oxford: Oxford University Press. * Dutton, W. H., Creese, S., Shillair, R. and Bada, M. (2019). ‘Cyber Security Capacity: Does It Matter?’. *Journal of Information Policy*, 9: 280‑306. [doi:10.5325/jinfopoli.9.2019.0280](https://www.jstor.org/stable/10.5325/jinfopoli.9.2019.issue-2019) * Creese, S., Dutton, W. H., Esteve-González, P. and Shillair, R. (2021). ‘Cybersecurity Capacity Building: Cross-National Benefits and International Divides’. Paper to be presented at the TPRC Conference, Washington D.C., February 2021. Доступна на веб-сайте SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658350> |
| Какие преимущества дает проведение оценки? | Цель обзора CMM – собрать данные о состоянии потенциала страны в области кибербезопасности и по всем параметрам CMM определить, какой из пяти стадий зрелости в отношении кибербезопасности она достигла. Эти данные используются для составления основанного на фактах отчета, который направляется органам государственного управления с рекомендациями:   * по оценке зрелости потенциала страны в области кибербезопасности; * детальному анализу набора практических мер, направленных на сокращение и устранение недостатков в отношении зрелости потенциала кибербезопасности; * определению приоритетов для инвестиций и будущего наращивания потенциала; * экономическому обоснованию инвестиций и соответствующего ожидаемого повышения уровня национальной кибербезопасности. |
| Имеется ли процесс расчета весовых коэффициентов? | Нет. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Да – оценка зрелости, но не рейтинг.  CMM предполагает пять стадий зрелости, варьирующихся от *начальной* до *динамичной*. Для начальной стадии характерен особый подход к развитию потенциала, а для динамичной – стратегический подход и способность адаптироваться к меняющимся условиям среды. Та или иная стадия означает, что страна находится в определенном положении с точки зрения зрелости потенциала кибербезопасности.  CMM обеспечивает фактические данные, которые требуются для определения достигнутой стадии зрелости по тому или иному фактору/аспекту. Чтобы достичь уровня зрелости по любому параметру CMM, необходимо достигнуть соответствия всем показателям по каждому фактору/аспекту этого параметра. Таким образом CMM прямо указывает, какие области требуют дальнейшего развития для достижения следующей стадии зрелости, а также данные, необходимые для подтверждения этого уровня зрелости потенциала. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Каков существующий потенциал кибербезопасности страны? * Какие существуют пробелы в кибербезопасности страны? * Каков статус реализации стратегии и политики? * Какие участники задействованы и каковы их роли и обязанности? * Какие шаги может предпринять страна для повышения уровня кибербезопасности? |
| На каких этапах жизненного цикла стратегии проводится оценка? | Начальный/обзор и анализ/мониторинг и оценка. |
| Как оценка помогает согласовать другие виды деятельности? | Поскольку адаптированные оперативные группы CMM объединяют в одном месте широкий круг внутренних заинтересованных сторон, а также (по возможности) международных партнеров, обзор CMM идеально подходит для координации с другими мероприятиями, проводимыми до него, после него и параллельно с ним. Формат адаптированных оперативных групп CMM также позволяет при необходимости собирать исходные данные во время собраний, предназначенных для других оценок. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | Обзор потенциала кибербезопасности стоит на первом месте в списке мероприятий GFCE для определения национальной стратегии и является частью его начального этапа наряду с обзором национального потенциала реагирования на инциденты и национальными оценками рисков. Благодаря многостороннему подходу, комплексному характеру и прозрачности обзор CMM идеально подходит для объединения различных заинтересованных сторон внутри страны, спонсоров и исполнителей, а также для обеспечения общей платформы планирования и реализации деятельности по наращиванию потенциала кибербезопасности. |
| Имеются ли общедоступные тематические исследования или свидетельства преимуществ инструмента? | Тематические исследования CMM: региональные отчеты по Северной Македонии, Гане, Самоа, Грузии и ОАГ: <https://gcscc.ox.ac.uk/case-studies>  Тематическое исследование по Сенегалу: ежегодное собрание GFCE в Сингапуре, "*Национальные стратегии*. *Откровенные беседы"*:<https://thegfce.org/national-strategies-interviews-behind-the-cover>  Всемирный банк: Глобальная программа развития потенциала в области кибербезопасности. Извлеченные уроки и рекомендации по усилению программы: <https://cybilportal.org/publications/global-cybersecurity-capacity-program-lessons-learned-and-recommendations-towards-strengthening-the-program/>  Кибербезопасность в островных тихоокеанских государствах: <https://t.co/smxYhtrqBz?amp=1> |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | Большинство исполнителей – это научно-исследовательские институты, получившие от своего ученого совета этическое разрешение на сбор данных для такой оценки.  Каждый отчет CMM проходит рецензирование Техническим советом GCSCC, состоящим из старших ученых и специалистов по кибербезопасности. |
| Дополнительная информация | Как используются обзоры CMM в исследованиях по наращиванию потенциала кибербезопасности: <https://gcscc.ox.ac.uk/our-approach>  Отчет по кибербезопасности OAГ/МАБР за 2020 год: риски, прогресс и дальнейшие шаги в странах Латинской Америки и Карибского бассейна: <https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean>  OAГ/МАБР, 2016 год. Кибербезопасность: готовы ли мы в странах Латинской Америки и Карибского бассейна? <https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean>  GFCE – оценка национального потенциала кибербезопасности с использованием модели зрелости: <https://thegfce.org/wp-content/uploads/2020/04/Assessnationalcybersecuritycapacityusingamaturitymodel.pdf>  Инициатива GFCE: повышение уровня кибербезопасности в Сенегале и Западной Африке: <https://cybilportal.org/projects/progressing-cybersecurity-in-senegal-and-west-africa-gfce-initiative/>  Инициатива GFCE: оценка и развитие потенциала кибербезопасности: <https://cybilportal.org/projects/assessing-and-developing-cybersecurity-capability-gfce-initiative/> |

# Система разработки и реализации стратегии кибербезопасности (CSDI)

## Корпорация MITRE

Система разработки и реализации стратегии кибербезопасности (CSDI) корпорации MITRE включает четырехэтапную модель, предназначенную для решения следующих задач: 1) оценка киберрисков/  
возможностей в национальном контексте; 2) оценка текущего потенциала по восьми ключевым направлениям и стратегическим принципам (потенциал для наращивания потенциала); 3) разработка и определение приоритетности стратегических целей и инвестиций на основе оценки пробелов в потенциале; и 4) составление дорожных карт по реализации стратегии для обеспечения долгосрочной устойчивости.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | Сентябрь 2020 года |
| Как называется инструмент оценки? | Система разработки и реализации стратегии кибербезопасности (CSDI) |
| Как называется организация, обслуживающая инструмент? | Корпорация MITRE |
| Кто осуществляет оценку? | Корпорация MITRE |
| Ссылки на инструмент и любая дополнительная информация | [https://cybilportal.org/tools/national-cyber-strategy-development-implementation- framework/](https://cybilportal.org/tools/national-cyber-strategy-development-implementation-%20framework/) |
| К кому следует обращаться для обсуждения организации оценки? | Гэри Банди: [gbundy@mitre.org](mailto:gbundy@mitre.org)  Синтия Райт: [cawright@mitre.org](mailto:cawright@mitre.org)  Джоанна Ваззана: jvazzana@mitre.org |
| Географический охват | Региональный, национальный или корпоративный |
| Кто может пользоваться инструментом? | Все |
| Какие темы охвачены? | Оценка проводилась по следующим восьми направлениям (областям):   1. гражданское право, регулирование и подотчетность; 2. политика и стандарты; 3. обеспечение ресурсами с учетом рисков; 4. устойчивые операции; 5. реагирование на инциденты; 6. предупреждение киберпреступности и судебное преследование; 7. развитие трудовых ресурсов в области кибербезопасности; 8. осведомленность общественности/культура кибербезопасности.   В каждой из этих областей ключевыми факторами считаются участие нескольких заинтересованных сторон и партнерство, а подходы к реализации, в частности в отношении развития трудовых ресурсов, сосредоточены на установлении эффективных государственно-частных партнерств. В оценки также включаются стратегические принципы, наиболее важными из которых являются приверженность руководства и участие заинтересованных сторон. |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки   * CBM и соответствующие нормы * Кибердипломатия   Международное право в киберпространстве Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью   * Регистрация и анализ инцидентов * Учения по кибербезопасности   ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты |
| Тип показателей | Используются в основном качественные показатели, которые сосредоточены на механизмах управления, политике, процессах и обеспечении ресурсами. Как правило, они не носят конкретно технического характера (то есть не ориентированы на конкретную сетевую архитектуру или практическое тестирование системы). |
| Сколько показателей используется и как они применяются? | Используются более 100 показателей, сгруппированных по соответствующим областям потенциала. |
| Методика – тип используемой оценки | Анализ, основанный на исследованиях, и опрос/собеседование с заинтересованными сторонами. |
| Метод сбора первичных данных | * Информация из открытых источников * Собеседования * Анкеты и опросы * Документы и записи |
| Проводится ли сбор вторичных данных? | Семинары-практикумы для заинтересованных сторон |
| Какие механизмы применяются для обеспечения точности собранных данных? | * Внутренняя проверка качества * Анкеты рассылаются как можно более широкому кругу заинтересованных сторон для дополнения/подтверждения сведений * Опрос с автоматизированной оценкой результатов |
| Каковы основные результаты оценки? | Объединение результатов исследований по открытым источникам, анализа угроз/возможностей, администрируемой оценки и последующих собеседований приводит к созданию интуитивно понятной лепестковой диаграммы для содействия формулированию целей с учетом рисков и приоритизации инвестиций в восьми областях потенциала кибербезопасности, а также подробного отчета с приоритетными рекомендациями. |
| Формат представления результатов оценки | * Отчет * Инструмент визуализации |
| Можно ли публиковать результаты оценки? | Да, с одобрения запрашивающей оценку структуры. |
| Как получить доступ к предыдущим отчетам? | По запросу, направленному в орган государственного управления или организацию, для которых проводилась оценка. |
| Каковы имеющиеся доказательства эффективности? | В каждой стране, с которой MITRE поддерживает устойчивые отношения, подвергшиеся оценке органы государственного управления и/или организации внесли изменения в соответствии с приоритетами, определенными в ходе этого мероприятия, в стратегические цели, структуры/механизмы управления, процессы оперативной координации, каналы связи и процессы реагирования на инциденты, подходы к развитию трудовых ресурсов и/или темы программ повышения осведомленности общественности. |
| Какие преимущества дает проведение оценки? | Подвергшиеся оценке страны, организации и/или вспомогательные структуры достигают глубокого понимания стратегического контекста своих рисков/возможностей и факторов развития потенциала, потребностей и недостатков в форме, облегчающей определение приоритетов – ключевого аспекта инвестиций в развитие потенциала.  В ходе последующих семинаров-практикумов по разработке и реализации стратегии они определяют роли и обязанности основных заинтересованных сторон; передовой опыт в области управления; возможности в области партнерства; подходы к обеспечению ресурсами; пробелы и неясности в законодательстве и политике; а также основные (предварительные) требования – все это формулируется в контексте их уникальной картины угроз и потребностей в отношении развития потенциала.  Кроме того, поскольку оценка ориентирована на общегосударственный или общеорганизационный подход, а семинары-практикумы проводятся с использованием проверенных инструментов конструктивного участия, она способствует привлечению заинтересованных сторон и их вовлечению в процесс, что важно для эффективной реализации программы. |
| Имеется ли процесс расчета весовых коэффициентов? | Все области потенциала кибербезопасности при его оценке имеют равный вес. Однако для конкретных подвергшихся оценке стран/организаций одни области потенциала кибербезопасности будут важнее других в зависимости от стратегического контекста, текущего уровня потенциала и имеющихся людских/финансовых ресурсов. Этот подход специально предназначен для определения областей, которые должны "перевешивать" для каждой подвергшейся оценке организации, на основе ее уникальных потребностей в плане рисков/возможностей. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Построенная лепестковая диаграмма (один выходной инструмент в дополнение к подробному анализу и отчету с рекомендациями) имеет четырехбалльную шкалу. Однако это не модель зрелости: пробелы в потенциале оцениваются в контексте не объективного набора критериев, а желаемых конечных состояний страны/организации. Такой подход помогает гарантировать, что страны/организации не будут гнаться за показателями, менее важными для стратегического контекста стоящих перед ними угроз, и позволяет исполнителям адаптировать инвестиционные стратегии к потребностям, наиболее актуальным для целей экономики и безопасности. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Какова картина киберугроз/возможностей? * В свете этой картины каковы цели в отношении создания и защиты возможностей и услуг ИКТ/кибервозможностей и услуг/цифровых возможностей и услуг? * Какие заинтересованные стороны участвуют в этом процессе и каковы их роли? * Каковы пробелы в потенциале в свете наших стратегических целей? * Как следует расставить приоритеты в прилагаемых усилиях с учетом этих пробелов? * Решение каких задач поможет в достижении поставленных приоритетных целей? * Как можно спланировать инициативы по их достижению? * Какие из возможных инициатив принесут наибольшую отдачу от инвестиций с точки зрения результатов и осуществимости? * Какие ресурсы можно задействовать? * Кто наши потенциальные партнеры по осуществлению избранных инициатив? * Как мы разрабатываем и выполняем дорожную карту по реализации? * Как можно повысить участие заинтересованных сторон и степень общественной поддержки? |
| На каких этапах жизненного цикла стратегии проводится оценка? | Начальном/обзора и анализа/разработки стратегии/ реализации. |
| Как оценка помогает согласовать другие виды деятельности? | Показывая перспективу общегосударственного уровня или уровня организации, привязанную к определенной картине угроз/возможностей, этот подход обеспечивает заинтересованным сторонам общую основу для определения, общих целей, установления приоритетов, распределения ресурсов и достижения этих целей. Дифференцируя пробелы в потенциале по ключевым областям, она помогает организациям сосредоточиться на наиболее важных для них областях при обеспечении видимости других областей, в которых могут возникнуть возможности для наращивания потенциала, таких как ресурсы программы помощи, способные повысить потенциал без отвлечения дефицитных внутренних ресурсов. Наконец, поскольку этот подход реализуется в системе с участием многих заинтересованных сторон, он способствует сосредоточению внимания на каналах связи, обмене информацией и прозрачных процессах, что гарантирует информированность заинтересованных сторон и партнеров о главных приоритетах (и их принятие) и текущей деятельности. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | Она уточняет приоритетные области потребностей, соответствующие контакты с заинтересованными сторонами, другие текущие/доступные программы и имеющиеся людские/финансовые ресурсы. |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | Все выполненные до сих пор оценки проводились по запросу стран/организаций или Государственного департамента США. Ни одна из них не опубликована, хотя правительства Ботсваны, Ганы, Украины и Эквадора выразили признательность в публичных выступлениях, публикациях в социальных сетях и/или на межправительственных встречах на высшем уровне.  Самым ярким свидетельством может быть то, что федеральные агентства США и страны-партнеры продолжают запрашивать наши рекомендации, доверяют им и действуют в соответствии с ними и что за четыре года, в течение которых мы используем эту систему, количество стран, с которыми мы работаем напрямую, увеличилось с трех до более двух десятков, и каждая страна постоянно обращается к нам за советами и помощью. На региональном уровне мы взаимодействуем более чем с 90 странами, и их число продолжает расти, причем в каждом случае появляются новые запросы на конкретную помощь. |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | MITRE – это научно-исследовательская организация, финансируемая из федерального бюджета, с жесткими требованиями внутреннего контроля качества и открытым уставом, которая прямо обязуется оказывать свободное от конфликта интересов беспристрастное обслуживание на благо общества. |
| Дополнительная информация | Эта система была разработана при поддержке Отдела по координации вопросов кибербезопасности Государственного департамента США, и ее усовершенствование стало возможным благодаря двустороннему и региональному взаимодействию под эгидой Государственного департамента. Использование этой оценки вне рамок мероприятий, проводимых под руководством Госдепартамента США, не обязательно подразумевает поддержку правительства США или приверженность его политике; однако в нашей модели и наших рекомендациях подразумевается почитание ценностей США, включая свободу информации, приверженность свободному и открытому интернету, верховенство закона и права человека. |

# Глобальный индекс кибербезопасности (GCI)

## Международный союз электросвязи (МСЭ)

Глобальный индекс кибербезопасности (GCI) помогает странам определить области, в которых можно повысить кибербезопасность, а также побуждает их принять меры для повышения своего рейтинга в этой сфере, что в свою очередь повышает общий уровень кибербезопасности во всем мире. Сфера охвата и структура GCI закреплены в Резолюции 130 (Пересм. Дубай, 2018 год) Полномочной конференции МСЭ, в которой формулируется задача усиления роли МСЭ в укреплении доверия и безопасности при использовании ИКТ. Вопросник GCI, из которого выводятся показатели, субпоказатели и микропоказатели, создается и утверждается путем консультаций в рамках Вопроса 3/2 (Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности), порученного 2‑й Исследовательской комиссии Сектора развития электросвязи МСЭ (МСЭ-D). Обследование проводится посредством онлайновой платформы, с помощью которой собираются подтверждающие данные.

Вопросник GCI четвертого издания (2019–2020 годы) позволяет измерить 20 общих показателей с помощью 82 вопросов. 20 показателей отражают пять основных составляющих Глобальной программы кибербезопасности (ГПК) МСЭ: *правовые меры, технические меры, организационные меры, развитие потенциала и сотрудничество.* В октябре 2019 года, перед началом обследования, Бюро развития электросвязи МСЭ (БРЭ) представило 2‑й Исследовательской комиссии МСЭ-D вопросник GCIv4 и соответствующие документы по GCI. В марте 2020 года БРЭ сообщило 2‑й Исследовательской комиссии о положении дел с ответами на вопросник; проинформировало участников о следующих шагах в процессе анализа данных, а также сообщило, что разработка весовых коэффициентов будет осуществлена путем привлечения группы экспертов, сформированной в процессе открытых консультаций с Государствами – Членами МСЭ, Членами Секторов и партнерами БРЭ. В октябре 2020 года Группа экспертов по определению весовых коэффициентов представила рекомендации по весовым коэффициентам показателей, субпоказателей и микропоказателей GCIv4, а также предложения по внесению изменений в вопросник GCI для его будущих изданий. В настоящее время проводится проверка ответов на вопросник для окончательного утверждения приславшими их странами. Ожидается, что окончательный отчет будет опубликован в 2021 году.

### Обзор

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Дата последнего обновления инструмента | Последнее обновление публикации состоялось в марте 2019 года. Мы находимся в процессе сбора данных и завершения проверки предоставленной информации для отчета по GCIv4. | | | | | |
| Как называется инструмент оценки? | Глобальный индекс кибербезопасности (GCI) | | | | | |
| Как называется организация, обслуживающая инструмент? | Международный союз электросвязи (МСЭ) | | | | | |
| Кто осуществляет оценку? | Международный союз электросвязи (МСЭ) | | | | | |
| Ссылки на инструмент и любая дополнительная информация | * Веб-сайт МСЭ: [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-%20cybersecurity-index.aspx) * Портал Cybil: [https://cybilportal.org/projects/itu-global-cybersecurity-index-gci- programme/](https://cybilportal.org/projects/itu-global-cybersecurity-index-gci-%20programme/) | | | | | |
| К кому следует обращаться для обсуждения организации оценки? | Группа GCI: [gci@itu.int](mailto:gci@itu.int) | | | | | |
| Географический охват | Глобальный | | | | | |
| Кто может пользоваться инструментом? | * Государства-Члены: министерства/учреждения * Агентства по кибербезопасности/лица, определяющие политику * Академические организации * Специалисты по кибербезопасности * Любые заинтересованные лица   Для академических организаций и организаций, желающих сотрудничать в рамках GCI, может потребоваться членство в МСЭ. | | | | | |
| Какие темы охвачены? | GCI охватывает следующие темы.  **Правовые меры**   * Материальное право в отношении киберпреступности * Нормы кибербезопасности   **Технические меры**   * Национальные/правительственные группы реагирования на инциденты (CERT/CIRT/CSRIT) * Отраслевые CERT/CIRT/CSRIT * Национальная программа применения стандартов кибербезопасности * Защита детей в онлайновой среде (COP)   **Организационные меры**   * Национальные стратегии кибербезопасности (NCS) * Ответственные/национальные учреждения * Показатели кибербезопасности   **Меры по развитию потенциала**   * Кампании по повышению осведомленности общественности * Подготовка по вопросам кибербезопасности для специалистов * Национальные образовательные программы и учебные планы * Программы исследований и разработок в области кибербезопасности * Национальная индустрия кибербезопасности * Государственные механизмы стимулирования для поддержки развития кибербезопасности   **Меры в области сотрудничества**   * Двусторонние соглашения * Участие в международных механизмах (форумах) * Многосторонние соглашения * Государственно-частные партнерства * Межведомственные партнерства   Полное описание каждой меры см. в опубликованных отчетах по адресу: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> | | | | | |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки  ☒ CBM и соответствующие нормы  ☒ Кибердипломатия  ☒ Международное право в киберпространстве Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью  ☒ Регистрация и анализ инцидентов  ☒ Учения по кибербезопасности  ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты | | | | | |
| Тип показателей | Для GCI осуществляется сбор качественных данных с использованием двоичной системы для оценки наличия или отсутствия определенных видов деятельности, отделов или показателей. | | | | | |
| Сколько показателей используется и как они применяются? | GCI не придерживается какого-либо заранее установленного набора показателей. В каждое издание вопросника вносятся изменения, и он пересматривается с учетом отзывов, полученных от координаторов стран и членов МСЭ. Поэтому количество показателей может уменьшаться или увеличиваться, и фиксированного количества показателей для каждой темы не существует. См., например, приведенную ниже таблицу с подробной информацией о количестве показателей в каждом издании на сегодняшний день. | | | | | |
|  | **GCIv1** | **GCIv2** | **GCIv3** | **GCIv4** |  |
| 17 показателей и 17 основных вопросов | 25 показателей и 157 вопросов | 25 показателей и 50 основных вопросов | 20 показателей и 82 основных вопроса |
| Методика – тип используемой оценки | В GCI используются как первичные, так и вторичные методы оценки. Группа GCI собирает данные по неучаствующим странам и передает им результаты на утверждение, а также проверяет и утверждает ответы, представленные координаторами Государств – Членов МСЭ. | | | | | |
| Метод сбора первичных данных | * Информация из открытых источников * Неопубликованные документы * Анкеты и опросы * Документы и записи | | | | | |
| Проводится ли сбор вторичных данных? | Да. Сбор вторичных данных для стран, ответивших на вопросник GCI, проводится следующим образом.   * МСЭ проводит проверку, выявляя недостающие ответы, подтверждающие документы и ссылки, используя информацию из открытых источников, неопубликованные документы, анкеты и опросы, а также общедоступные документы и записи. * Проверенные ответы отправляются обратно координатору по стране, который при необходимости уточняет ответы. * МСЭ утверждает окончательные поправки координатора по стране и возвращает документ каждому координатору для окончательного утверждения. * Впоследствии утвержденные ответы на вопросник используются для целей анализа, оценки и ранжирования. | | | | | |
| Какие механизмы применяются для обеспечения точности собранных данных? | Координаторы GCI, назначенные министерствами, обычно обладают опытом/знаниями в области кибербезопасности и работают в различных министерствах на должностях, связанных с обеспечением кибербезопасности. Кроме того, соответствующие ссылки и запрашиваемые и утвержденные документы берутся с официальных общедоступных веб-сайтов органов государственного управления, а иногда предоставляются конфиденциальные официальные документы. Мы обращаемся к опытным специалистам в областях, связанных с обеспечением кибербезопасности, от которых требуем неоднократного выполнения процесса проверки по каждой стране, и передаем эту информацию странам до тех пор, пока не будет получено окончательное подтверждение для гарантии точности. | | | | | |
| Каковы основные результаты оценки? | В каждом издании публикуются окончательный отчет и результаты. | | | | | |
| Формат представления результатов оценки | Отчет | | | | | |
| Можно ли публиковать результаты оценки? | Да. Результаты могут публиковаться. GCI – это открытый материал, предназначенный для повышения осведомленности во всем мире. Все предыдущие отчеты доступны по адресу: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> | | | | | |
| Как получить доступ к предыдущим отчетам? | Получить доступ к предыдущим отчетам и загрузить их можно по адресу: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> | | | | | |
| Каковы имеющиеся доказательства оказанного влияния? | Участие в GCI все большего числа Государств-Членов свидетельствует о постоянно растущем интересе к индексу:   |  |  |  |  | | --- | --- | --- | --- | | **GCIv1 (2015 год)** | **GCIv2 (2017 год)** | **GCIv3 (2018 год)** | **GCIv4 (2019–2020 годы)** | | 105 стран | 134 страны | 155 стран | В настоящее время 163 страны |   Многие страны обращаются к МСЭ с просьбой о поддержке в укреплении их позиций в области кибербезопасности, в частности в области разработки и совершенствования национальных стратегий, создании CERT и в деятельности по наращиванию потенциала. Страны с низким и средним рейтингом (на основе диапазонов оценок, которые остаются неизменными с течением времени) получают целевую помощь, что ведет к неуклонному сокращению числа таких стран. | | | | | |
| Какие преимущества дает проведение оценки? | Оценки помогают выявить пробелы в работе по повышению кибербезопасности в отдельных странах и регионах, а также повысить осведомленность о кибербезопасности во всем мире. Оценка также помогает определить страны, наиболее нуждающиеся в поддержке по улучшению положения их дел в области кибербезопасности.  На основании собранной информации в GCI выявляются практические методы, которые могут внедрить Государства-Члены и которые соответствуют их национальным условиям. Также GCI способствует распространению передового опыта и формированию глобальной культуры кибербезопасности. | | | | | |
| Имеется ли процесс расчета весовых коэффициентов? | Да. Вес показателя в GCI оценивается членами Группы экспертов GCI в зависимости от важности показателя по пяти составляющим GCA; от соответствия основным целям и концептуальной структуре GCI и от доступности и качества данных. Группа экспертов по определению весовых коэффициентов дает объективные рекомендации по весовым коэффициентам после собрания Группы, которое проводится для каждого издания GCI. | | | | | |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Да. Весовые коэффициенты показателей, определенные каждым экспертом, усредняются для получения итогового весового коэффициента по каждому показателю. В рамках применяемой функции страна, ответившая "ДА" с документальным подтверждением, получает полное количество баллов по показателю, а страна, не представившая доказательств или ответившая "НЕТ", – нулевую оценку. Общие оценки нормализуются и ранжируются. | | | | | |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Каковы текущие глобальные тенденции и закономерности в политике кибербезопасности? * Как Государства-Члены могут определить сильные и слабые места в мерах по обеспечению кибербезопасности? * Какова степень выполнения странами обязательств в области кибербезопасности и какие страны обеспечивают передовой опыт в области кибербезопасности? |
| На каких этапах жизненного цикла стратегии проводится оценка? | Начальном/обзора и анализа/разработки стратегии/реализации/мониторинга и оценки. |
| Как оценка помогает согласовать другие виды деятельности? | Оценка GCI помогает определить относительную силу и слабость обязательств Государств‑Членов в области кибербезопасности, информируя государства, где им может потребоваться дополнительная поддержка в развитии потенциала или где они могут оказать поддержку другим. Например, с помощью оценки GCI МСЭ может определить потребности в области обучения по вопросам кибербезопасности в системах образования государств-членов.   |  |  |  |  | | --- | --- | --- | --- | | **Год** | **Высокая** | **Средняя** | **Низкая** | | **2018–2019** | 54 | 53 | 87 | | **2016–2017** | 30 | 60 | 104 | | **2014–2015** | 19 | 52 | 122 | |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | Каждый год многие страны запрашивают помощь в создании CERT и разработке национальных стратегий кибербезопасности по итогам оценки GCI, количества присвоенных баллов и места в рейтинге.  Например:  **Бенин** в результате повышения осведомленности, обеспеченного GCI,разработал стратегию кибербезопасности[: https://news.itu.int/benin-launches-a-new-national-cybersecurity-strategy/](file:///D:\ITU-JOBS\445\492114\:%20https:\news.itu.int\benin-launches-a-new-national-cybersecurity-strategy\)  **Республика Конго** приняла Закон о кибербезопасности, направленный на борьбу с киберпреступностью: <https://postetelecom.gouv.cg/le-senat-adopte-a-lunanimite-la-creation-de-lagence-nationale-de-securite-des-systemes-dinformation/>  В 2018 году, согласно оценкам GCI, был отмечен прогресс в выполнении обязательств в области кибербезопасности в следующих странах:   * Бенин, Эстония, Польша, Зимбабве, Замбия, Египет, Южно-Африканская Республика и Эсватини – в части принятия законов о киберпреступности; * Уганда – в части разработки законодательства о защите данных/ конфиденциальности; * Австралия, Ботсвана, Канада, Чешская Республика, Дания, Япония, Иордания, Нидерланды, Испания, Самоа, Сингапур и Люксембург – в части обновления национальных стратегий кибербезопасности (NCSS); а также * Камерун, Малави, Танзания и Зимбабве – в части разработки NCSS.   Освещение GCI в СМИ: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | * Материалы, поступающие в GCI, проходят независимую проверку нашей группой. * Независимая группа экспертов предоставляет данные о весовых коэффициентах показателей в модели, и ни один эксперт не может существенно изменить весовые коэффициенты в одиночку. |

# 

# Система оценки потенциала стран (NCAF)

## Агентство Европейского союза по кибербезопасности (ENISA)

Основная цель разработки *Системы оценки потенциала стран* (NCAF) заключалась в том, чтобы создать инструмент самооценки для оказания помощи государствам – членам ЕС в измерении уровня зрелости их потенциала кибербезопасности. Для достижения этой цели ENISA использовало в качестве отправной точки стратегические цели национальных стратегий кибербезопасности (NCSS) государств – членов ЕС. Поскольку потенциал кибербезопасности служит странам основным средством для достижения их целей в области NCSS, NCAF содержит вопросы по пяти уровням зрелости с учетом 17 стратегических целей, включенных в большинство европейских NCSS. Система дает простое и репрезентативное представление о зрелости потенциала государства-члена в области кибербезопасности на трех уровнях – на уровне целей, групповом и глобальном.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | 2 декабря 2020 года |
| Как называется инструмент оценки? | Система оценки потенциала стран (NCAF) |
| Как называется организация, обслуживающая инструмент? | Агентство Европейского союза по кибербезопасности (ENISA) |
| Кто осуществляет оценку? | Государства – члены ЕС |
| Ссылки на инструмент и любая дополнительная информация | <https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework>  В 2021 году NCAF будет преобразована в онлайновый инструмент. |
| К кому следует обращаться для обсуждения организации оценки? | Агентство Европейского союза по кибербезопасности (ENISA) |
| Географический охват | Европейский союз/глобальный |
| Кто может пользоваться инструментом? | Целевая аудитория NCAF – это лица, определяющие политику, эксперты и государственные чиновники, ответственные за разработку, внедрение и оценку NCSS и, в более широком плане, потенциала кибербезопасности или участвующие в этих процессах. Кроме того, результаты, формализованные в опубликованном документе, могут быть полезны специалистам и ученым в области политики кибербезопасности, работающим на национальном или европейском уровне. |
| Какие темы охвачены? | Концептуальная модель системы самооценки охватывает 17 стратегических целей, взятых из NCSS государств – членов ЕС, и построена на основе четырех основных групп целей. Каждая из этих групп охватывает ключевую тематическую область целей развития потенциала кибербезопасности и состоит из отдельных целей. Затем каждая цель оценивается с помощью вопросов для разных уровней зрелости. Группы целей охватывают следующие темы.  **I. Управление кибербезопасностью и стандарты кибербезопасности**   * 1. Разработка национального плана действий в чрезвычайных ситуациях в киберпространстве   2. Определение основных мер безопасности   3. Защита цифровой идентичности и укрепление доверия к государственным цифровым услугам   Для этой группы целей рассматриваются аспекты планирования для подготовки государства-члена к отражению кибератак, а также стандарты для защиты государств-членов и цифровой идентичности. |
|  | **II. Наращивание потенциала и осведомленность**   * 1. Организация учений по кибербезопасности   2. Обеспечение возможности реагирования на инциденты   3. Повышение осведомленности пользователей   4. Совершенствование учебно-образовательных программ   5. Поощрение научных исследований и разработок   6. Стимулирование инвестиций частного сектора в меры безопасности   7. Повышение кибербезопасности цепочки поставок   Для этой группы целей оценивается способность государств-членов к повышению осведомленности о рисках и угрозах кибербезопасности и о средствах борьбы с ними. Кроме того, этот параметр измеряет способность страны постоянно наращивать потенциал кибербезопасности и повышать уровень знаний и навыков в этой области.  **III. Нормативно-правовые вопросы**   1. Защита критической информационной инфраструктуры, операторов важнейших услуг (OES) и поставщиков цифровых услуг (DSP) 2. Борьба с киберпреступностью 3. Создание механизмов сообщения об инцидентах 4. Усиление конфиденциальности и защиты данных   Для этой группы целей измеряется способность государств-членов внедрять необходимые нормативно-правовые инструменты для борьбы с киберпреступностью, а также выполнять юридические требования, такие как сообщение об инцидентах, обеспечение конфиденциальности и защита критической информационной инфраструктуры (CIIP).  **IV. Сотрудничество**   * 1. Создание государственно-частного партнерства   2. Институционализация сотрудничества между государственными органами   3. Участие в международном сотрудничестве   В этой группе целей оценивается сотрудничество и обмен информацией между различными группами заинтересованных сторон на национальном и международном уровнях. |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки  ☒ CBM и соответствующие нормы  ☒ Кибердипломатия   * Международное право в киберпространстве  Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью  ☒ Регистрация и анализ инцидентов  ☒ Учения по кибербезопасности  ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве  ☒ Подготовка по вопросам киберпреступности  ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты |
| Тип показателей | Система включает качественные показатели, построенные на двух уровнях – стратегическом и оперативном.  Для каждой цели, включенной в систему самооценки, имеется ряд показателей, распределенных по пяти уровням зрелости. Каждый показатель основан на дихотомическом вопросе (предусматривающем ответ "да" или "нет"). Показатель может быть обязательным или необязательным. |
| Сколько показателей используется и как они применяются? | Модель дает оценку, основанную на значении двух параметров – ***уровня зрелости*** и ***коэффициента охвата***. Каждый из этих параметров можно рассчитать на разных уровнях: i) на уровне отдельной цели; ii) на уровне группы целей; или iii) на общем уровне.  Кроме того, для адаптации к специфике стран – членов ЕС при обеспечении согласованного анализа оценка рассчитывается на основе двух разных выборок на уровне группы целей и на общем уровне:   * **общая оценка** – одна полная выборка, охватывающая все цели, включенные в группу целей или в общую структуру (от 1 до 17); * **специальные оценки** –одна специальная выборка, охватывающая только цели, выбранные государством-членом (обычно соответствующие целям, представленным в NCS конкретной страны) в рамках группы целей или общей структуры.   Для каждой группы целей в таблице представлен исчерпывающий набор показателей в форме вопросов, соответствующих данному уровню зрелости. Вопросник является основным инструментом самооценки. Для каждой цели необходимо отметить два набора показателей:   * набор вопросов, относящихся к зрелости стратегии (9 общих вопросов), помеченных латинскими буквами от "а" до "с" для каждого уровня зрелости и повторяющихся для каждой цели; и * набор вопросов, относящихся к потенциалу кибербезопасности (319 вопросов по потенциалу кибербезопасности), пронумерованных от 1 до 10 для каждого уровня зрелости в зависимости от области, охватываемой целью. |
| Методика – тип используемой оценки | **Уровни зрелости** – пятиуровневая шкала зрелости  **Атрибуты** – на основе четырех измерений/групп целей, охватывающих области развития потенциала кибербезопасности  **Метод оценки** – самооценка  **Отображение результатов** – представление результатов с разными уровнями детализации |
| Метод сбора первичных данных | * Ожидание действий по координации сбора данных и консолидации данных. * Определение центрального органа, ответственного за проведение самооценки на национальном уровне. * Использование мероприятий по оценке как способа обмена информацией и обсуждения вопросов кибербезопасности. * Использование NCSS как способа выбора целей, подлежащих оценке.   По мере расширения области применения NCSS необходимо гарантировать сохранение соответствия интерпретации оценок развитию NCSS. Жизненный цикл NCSS – это многолетний процесс. |
| Проводится ли сбор вторичных данных? | Заполняя вопросник для самооценки, необходимо помнить о том, что основной целью является оказание поддержки государствам-членам в развитии потенциала кибербезопасности. |
| Какие механизмы применяются для обеспечения точности собранных данных? | Чтобы извлечь выгоду из результатов применения системы, государства – члены ЕС/страны, проводящие оценку, должны обеспечить точность данных. |
| Каковы основные результаты оценки? | Результаты оценки предоставляются на трех разных уровнях: на уровне цели, на уровне групп целей и на общем уровне.  Страна оценивается и получает окончательную общую оценку, учитывающую все цели в каждой группе, и окончательную специальную оценку, учитывающую только цели, выбранные страной.  Кроме того, NCAF указывает коэффициент охвата. Он рассчитывается как **отношение** **количества вопросов,** **на которые дан положительный ответ,** к **общему количеству вопросов,** относящихся к данной цели. Коэффициент охвата выражается в процентах. |
| Формат представления результатов оценки | Отчет  Визуализация онлайнового инструмента (работа ENISA на будущее) |
| Можно ли публиковать результаты оценки? | Результаты оценки публикуются только в том случае, если государство-член решит сделать это по собственной инициативе. |
| Как получить доступ к предыдущим отчетам? | Государство-член может отслеживать достигнутый им с течением времени прогресс на основе повторных оценок. |
| Каковы имеющиеся доказательства оказанного влияния? | В общей сложности в разработке этой системы участвовали около 20 государств-членов, и почти все государства-члены приняли участие в семинаре по утверждению системы, на котором она была представлена и подробно обсуждалась.  В частности, система должна расширить возможности государств-членов в:   * проведении оценки их национального потенциала кибербезопасности; * повышении осведомленности об уровне зрелости страны; * определении областей для улучшения; и * наращивании потенциала кибербезопасности. |
| Какие преимущества дает проведение оценки? | NCAF является инструментом, который помогает странам:   * получить полезную информацию для разработки долгосрочной стратегии (например, примеры передового опыта, руководящие указания); * выявить недостающие элементы в NCSS; * наращивать потенциал кибербезопасности; * обеспечить подотчетность за политические действия; * завоевать доверие широкой общественности и международных партнеров; * вести информационно-пропагандистскую деятельность и укреплять имидж прозрачной организации; * предвидеть будущие проблемы; * учитывать извлеченные уроки и передовой опыт; * создать базовую модель потенциала кибербезопасности в ЕС для облегчения дискуссий; и * оценивать возможности страны в отношении обеспечения кибербезопасности. |
| Имеется ли процесс расчета весовых коэффициентов? | Государство – член ЕС может публиковать результаты оценки, представляя уровень зрелости в отношении потенциала кибербезопасности страны, группы целей или даже отдельной цели.  Все подвергаемые оценки цели в системе одинаково актуальны; следовательно, они имеют одинаковую значимость. То же относится и к показателям, используемым в системе. |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | NCAF предназначена для измерения потенциала кибербезопасности государств-членов в отношении 17 целей. Однако государство-член может выбрать отдельные цели, по которым оно хочет получить оценку, и рассматривать только часть из этих 17 целей. |

# Индекс национальной кибербезопасности (NCSI)

## Академия электронного государственного управления (eGA)

*Индекс национальной кибербезопасности* (NCSI) – это глобальный индекс, измеряющий готовность стран к предотвращению киберугроз и управлению инцидентами кибербезопасности. NCSI также представляет собой базу данных, содержащую общедоступные доказательные материалы, и инструмент наращивания потенциала кибербезопасности стран.

NCSI фокусируется на поддающихся измерению аспектах кибербезопасности, реализованных центральным правительством.

1. **Действующее законодательство** –правовые акты, постановления, приказы и т. д.
2. **Учрежденные подразделения** –существующие организации, департаменты и т. д.
3. **Форматы сотрудничества** –комитеты, рабочие группы и т. д.
4. **Результаты** –правила, учения, технологии, веб-сайты, программы и т. д.

С 2016 года с помощью NCSI было оценено 160 стран. Сбор, анализ и публикация данных в NCSI – непрерывный процесс. NCSI не публикует ежегодных отчетов. Когда представляются новые доказательства, они оцениваются, и в случае их обоснованности в рейтинг немедленно вносятся необходимые изменения. Методика NCSI была разработана в 2016 году и обновлена в 2018 году. В настоящее время она пересматривается, и не позднее 2022 года будет опубликована новая версия.

### Обзор

|  |  |
| --- | --- |
| Дата последнего обновления инструмента | Записи о странах в NCSI постоянно обновляются, а это означает, что и сам NCSI постоянно обновляется. |
| Как называется инструмент оценки? | [Индекс национальной кибербезопасности (NCSI)](https://ncsi.ega.ee/) |
| Как называется организация, обслуживающая инструмент? | [Академия электронного государственного управления](https://ega.ee/) |
| Кто осуществляет оценку? | * [Академия электронного государственного управления](https://ega.ee/) * Организации и учреждения оцениваемых стран, связанные с обеспечением кибербезопасности |
| Ссылки на инструмент и любая дополнительная информация | Портал Cybil: <https://cybilportal.org/projects/national-cybersecurity-index/> |
| К кому следует обращаться для обсуждения организации оценки? | Г‑жа Эпп Маатен: [epp.maaten@ega.ee](mailto:epp.maaten@ega.ee)  Г‑н Раду Серрано: [radu.serrano@ega.ee](mailto:radu.serrano@ega.ee)  Г‑жа Мерль Мегр: [merle.maigre@ega.ee](mailto:merle.maigre@ega.ee)  Группа NCSI: ncsi@ega.ee |
| Географический охват | Глобальный |
| Кто может пользоваться инструментом? | * Министерства/учреждения стран * Агентства кибербезопасности/директивные органы * Академические организации * Специалисты по кибербезопасности * Любые заинтересованные лица   По вопросам сотрудничества в области сбора данных по стране для NCSI следует обращаться в группу NCSI. |
| Какие темы охвачены? | 1. **Разработка политики в области кибербезопасности**    1. Подразделение политики в области кибербезопасности    2. Формат координации политики в области кибербезопасности    3. Стратегия кибербезопасности    4. План реализации стратегии кибербезопасности 2. **Анализ киберугроз и информация о них**    1. Подразделение анализа киберугроз    2. Открытые отчеты о киберугрозах, публикуемые ежегодно    3. Веб-сайт по кибербезопасности 3. **Образование и повышение квалификации**    1. Навыки кибербезопасности в системе начального или среднего образования    2. Программа кибербезопасности на уровне бакалавра    3. Программа кибербезопасности на уровне магистра    4. Программа кибербезопасности на уровне доктора философии    5. Профессиональная ассоциация специалистов по кибербезопасности 4. **Вклад в глобальную кибербезопасность**    1. Конвенция о киберпреступности    2. Представительство в форматах международного сотрудничества    3. Международная организация по кибербезопасности, размещенная в стране    4. Создание потенциала кибербезопасности для других стран 5. **Защита цифровых услуг**    1. Ответственность за кибербезопасность для поставщиков цифровых услуг    2. Стандарт кибербезопасности для государственного сектора    3. Компетентный надзорный орган 6. **Защита важнейших услуг**    1. Определение операторов важнейших услуг    2. Требования к кибербезопасности для операторов важнейших услуг    3. Компетентный надзорный орган    4. Регулярный контроль за соблюдением мер безопасности 7. **Электронная идентификация и доверительные услуги**    1. Уникальный постоянный идентификатор    2. Требования к криптосистемам    3. Электронная идентификация    4. Электронная подпись    5. Отметка времени    6. Служба доставки с электронной регистрацией    7. Компетентный надзорный орган 8. **Защита персональных данных**    1. Законодательство о защите персональных данных    2. Орган по защите персональных данных 9. **Реагирование на инциденты кибербезопасности**    1. Подразделение реагирования на инциденты кибербезопасности    2. Ответственность за отчетность    3. Единый контактный центр для международной координации 10. **Управление в условиях киберкризиса**     1. План управления в условиях киберкризиса     2. Учения по управлению в условиях киберкризиса на национальном уровне     3. Участие в международных учениях по управлению в условиях киберкризиса     4. Оперативная поддержка волонтеров в условиях киберкризиса 11. **Борьба с киберпреступностью**     1. Криминализация киберпреступлений     2. Подразделение по борьбе с киберпреступностью     3. Подразделение цифровой криминалистики     4. Круглосуточный контактный центр по вопросам международной киберпреступности 12. **Военные кибероперации**     1. Подразделение киберопераций     2. Учения по кибероперациям     3. Участие в международных учениях по кибероперациям |
| Какие темы GFCE охвачены? | Политика и стратегия ☒ Стратегии  ☒ Оценки   * CBM и соответствующие нормы   ☒ Кибердипломатия   * Международное право в киберпространстве  Управление инцидентами и CIIP ☒ Реагирование на инциденты, связанные с национальной компьютерной безопасностью  ☒ Регистрация и анализ инцидентов  ☒ Учения по кибербезопасности  ☒ Защита критической информационной инфраструктуры Киберпреступность ☒ Правовая база/законодательство по киберпреступности  ☒ Правоохранительные органы в киберпространстве   * Подготовка по вопросам киберпреступности   ☒ Предупреждение киберпреступности Культура и навыки ☒ Осведомленность по вопросам кибербезопасности  ☒ Образование и обучение  ☒ Развитие трудовых ресурсов Стандарты ☒ Международные и/или национальные стандарты |
| Тип показателей | Осуществляется сбор качественных данных для NCSI с использованием системы оценок за наличие конкретного правового акта, специализированного подразделения, официального формата сотрудничества и/или результата. |
| Сколько показателей используется и как они применяются? | Используется в общей сложности 46 показателей (представленных в форме вышеупомянутых тем). Сами показатели распределены по 12 качествам. Каждый показатель имеет значение, показывающее относительную важность показателя в индексе, и соответствующий критерий, объясняющий, какие данные могут быть представлены в качестве доказательств.  Чтобы получить положительное значение по любому критерию, необходимо предоставить доказательный материал в виде данных. Если предоставленные данные соответствуют всем аспектам критерия, они принимаются в качестве достаточного доказательного материала. |
| Методика – тип используемой оценки | Информация по каждой стране вводится в NCSI и обновляется в индивидуальном порядке. После ввода/обновления информации по стране NCSI отображает место страны в общем сравнительном рейтинге. |
| Метод сбора первичных данных | * Информация из открытых источников * Документы и записи * Законодательство и другие официальные документы * Официальные веб-сайты |
| Проводится ли сбор вторичных данных? | Да. NCSI не является статическим индексом, поэтому сбор данных осуществляется непрерывно в течение года.   * Информация из открытых источников * Документы и записи * Законодательство и другие официальные документы * Официальные веб-сайты |
| Какие механизмы применяются для обеспечения точности собранных данных? | Все доказательные материалы должны быть общедоступными. В качестве доказательных материалов могут рассматриваться только официальные данные. Принимаются следующие доказательства/ссылки: правовые акты, официальные документы и официальные веб-сайты.  По завершении сбора данных предоставленная информация просматривается как минимум двумя экспертами NCSI. После проверки набор данных публикуется на веб-сайте NCSI. |
| Каковы основные результаты оценки? | * Обновленная информация на странице страны (для стран, включенных в NCSI) * Страницы стран (для стран, которые еще не включены в NCSI) * Рейтинг NCSI (обновляется каждый раз при обновлении страницы страны) |
| Формат представления результатов оценки | * Веб-сайт * Инструмент визуализации (с возможностью сравнения прошлых или настоящих наборов данных для одной страны или между странами) * Возможность скачать страницу страны в формате PDF |
| Можно ли публиковать результаты оценки? | Да, всегда. |
| Как получить доступ к предыдущим отчетам? | Для страницы той или иной страны NCSI показывает, когда была обновлена информация о стране. Обычно на странице страны представлена самая последняя доступная информация. Посетитель может просмотреть информацию о предыдущем обновлении, выбрав конкретную дату обновления из раскрывающегося меню "Выбрать версию". |
| Каковы имеющиеся доказательства оказанного влияния? | * Участие в NCSI все большего числа стран свидетельствует о постоянно растущем интересе к индексу. Отдельные страны запросили отдельные подробные индивидуальные оценки на основе NCSI, чтобы установить текущее положение дел в стране в области кибербезопасности и улучшить его. * Научные работники пользовались этим инструментом для работы над одним или несколькими тематическими исследованиями. |
| Какие преимущества дает проведение оценки? | Страны могут определить свой уровень готовности к предотвращению киберугроз. Обеспечивая сопоставимость между странами и разбивая оценки по показателям, NCSI поддерживает совместный, транснациональный подход к обеспечению кибербезопасности, при котором передовой опыт используется многими странами. |
| Имеется ли процесс расчета весовых коэффициентов? | Нет |
| Применяется ли для оценки механизм выставления баллов и/или ранжирования? | Да – для показателей, рейтинга NCSI (страны), уровня цифрового развития (DDL) и расхождения (между рейтингом NCSI и DDL).   * Каждый показатель имеет значение, показывающее относительную важность показателя в индексе. Значения присваиваются экспертной группой по следующим правилам:   1 балл – за правовой акт, регулирующий конкретную сферу;  2–3 балла – за специализированное подразделение;  2 балла – за официальный формат сотрудничества;  1–3 балла – за результат/продукт.   * Оценка NCSI отражает процент от максимального значения показателей, полученный страной. Максимальная оценка NCSI всегда равна 100 (100%), независимо от добавления или исключения показателей. * В дополнение к оценке NCSI индексная таблица также показывает уровень цифрового развития (DDL). DDL рассчитывается по индексу развития ИКТ (IDI) и индексу сетевой готовности (NRI). DDL – это усредненный процент от максимального значения обоих индексов, полученный страной.   Расхождение показывает соотношение между оценками NCSI и DDL. Положительный результат указывает на то, что развитие кибербезопасности в стране соответствует ее цифровому развитию или опережает его. Отрицательный результат указывает на то, что цифровое общество страны развито в большей степени, чем ее национальный потенциал кибербезопасности. |

### Подробное описание

|  |  |
| --- | --- |
| На какие основные вопросы помогает ответить инструмент? | * Насколько моя страна готова к отражению кибератак/угроз? * Чего недостает моей стране для защиты от киберугроз? * Какие учреждения подходят для решения этой задачи? * Как еще больше повысить готовность к меняющимся киберугрозам? * Какой передовой мировой опыт мы можем адаптировать и/или внедрить? |
| На каких этапах жизненного цикла стратегии проводится оценка? | Оценка (анализ страны) может проводиться на любом этапе жизненного цикла стратегии, чтобы по возможности поддерживать NCSI в актуальном состоянии. Однако для отдельных стран оценку рекомендуется выполнять на начальном этапе, этапе обзора и анализа или на этапе мониторинга и оценки. |
| Как оценка помогает согласовать другие виды деятельности? | NCSI помогает выявить области относительной силы и слабости в уровне готовности страны к предотвращению киберугроз, тем самым указывая, где ей может потребоваться дополнительная помощь в развитии потенциала, а где она может оказать помощь другим. Страницы стран в индексе NCSI также содержат описание их национального передового опыта, который может быть адаптирован/внедрен другими странами с помощью спонсоров, международных организаций и т. д. или без посторонней помощи. |
| Какую роль играет оценка в процессе поиска партнеров для GFCE? | Поскольку NCSI предоставляет общедоступную информацию, спонсоры и исполнители могут видеть области относительной силы и слабости страны. Следовательно, они могут обратиться к соответствующим странам, предлагая помощь в развитии потенциала кибербезопасности или аналогичные мероприятия и усовершенствования там, где они необходимы. |
| Какие имеются тематические исследования или свидетельства преимуществ инструмента? | [Обзор ситуации: безопасность и защита киберпространства и электронной демократии в странах Восточного партнерства](https://ega.ee/publication/situation-review-safety-and-security-of-cyberspace-and-e-democracy-in-the-eastern-partnership-countries/) (2017 год), Академия электронного государственного управления |
| Каковы механизмы обеспечения независимости, беспристрастности и нейтральности результатов? | Материалы, поданные в NCSI странами-участниками, проходят независимую проверку нашей группой. |
| Дополнительная информация | Справочник   * [Национальная кибербезопасность на практике](https://ega.ee/publication/national-cyber-security-handbook/) (2020 год), Академия электронного государственного управления   Подкаст/статья   * [Что делать правительствам для защиты своего национального киберпространства?](https://ega.ee/blog_post/podcast-what-should-governments-do-to-secure-their-national-cyber-space/) (2020 год), Академия электронного государственного управления * [NCSI – насколько ваша страна готова к отражению кибератак?](https://ega.ee/blog_post/ncsi-how-prepared-country-cyber-attack/?fbclid=IwAR1xJDYVtMQg3P0W1hbTyjgnjETlSEAGEhpiM7Z_z2zkvHIO27VuxfXdfss) (2020 год), Академия электронного государственного управления * [Что такое кибергигиена?](https://ega.ee/blog_post/podcast-what-is-cyber-hygiene/)(2020 год), Академия электронного государственного управления   Статья   * [160 стран в NCSI: препятствия, извлеченные уроки и интересные факты](https://ega.ee/blog_post/160-countries-in-the-ncsi-barriers-lessons-learnt-and-interesting-facts/) (2020 год), Академии электронного государственного управления |

# Обзор инструментов

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Инструмент для наращивания потенциала по борьбе с киберпреступностью | Киберзрелость стран Азиатско-Тихоокеанского региона | CRI | CMM | CSDI | GCI | NCAF | NCSI |
| Политика и стратегия |  |  |  |  |  |  |  |  |
| Стратегии |  |  |  |  |  |  |  |  |
| Оценки |  |  |  |  |  |  |  |  |
| CBM и соответствующие нормы |  |  |  |  |  |  |  |  |
| Кибердипломатия |  |  |  |  |  |  |  |  |
| Международное право в киберпространстве |  |  |  |  |  |  |  |  |
| Управление инцидентами и CIIP |  |  |  |  |  |  |  |  |
| Реагирование на инциденты, связанные с национальной компьютерной безопасностью |  |  |  |  |  |  |  |  |
| Регистрация и анализ инцидентов |  |  |  |  |  |  |  |  |
| Учения по кибербезопасности |  |  |  |  |  |  |  |  |
| Защита критической информационной инфраструктуры |  |  |  |  |  |  |  |  |
| Киберпреступность |  |  |  |  |  |  |  |  |
| Правовая база/ законодательство по киберпреступности |  |  |  |  |  |  |  |  |
| Правоохранительные органы в киберпространстве |  |  |  |  |  |  |  |  |
| Подготовка по вопросам киберпреступности |  |  |  |  |  |  |  |  |
| Предупреждение киберпреступности |  |  |  |  |  |  |  |  |
| Культура и навыки |  |  |  |  |  |  |  |  |
| Осведомленность по вопросам кибербезопасности |  |  |  |  |  |  |  |  |
| Образование и обучение |  |  |  |  |  |  |  |  |
| Развитие трудовых ресурсов |  |  |  |  |  |  |  |  |
| Стандарты |  |  |  |  |  |  |  |  |
| Международные или национальные стандарты |  |  |  |  |  |  |  |  |