ГЛОБАЛЬНЫЙ ИНДЕКС КИБЕРБЕЗОПАСНОСТИ, ВЕРСИЯ 4, 2019/2020 годы

Вопросы, содержащиеся в настоящей анкете, разработаны и рассмотрены на собрании групп Докладчиков исследовательских комиссий МСЭ-D по Вопросу 3/2 "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности". На этом собрании было получено одобрение Членами запуска процесса GCIv4 – 2019/2020. Вопросник состоит из пяти разделов; в каждом разделе ответы на вопросы следует давать в форме "да/нет", поставив отметку в клетке перед соответствующим вариантом. Заполнять вопросник необходимо в онлайновом режиме. Каждый респондент получит от МСЭ по электронной почте официальное сообщение, содержащее индивидуальный URL, который необходимо сохранить в безопасном месте. Если координатор решит заполнять вопросник в группе, он может использовать для ответов общий логин.

Онлайновый вопросник позволяет респондентам загружать соответствующие документы (и URL) по каждому вопросу в качестве справочной информации. Предполагается, что информация, предоставленная респондентами данного вопросника, не будет носить конфиденциальный характер.

ПРАВОВЫЕ МЕРЫ

1. Нормы материального права в области киберпреступности

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

1.1 Имеются ли у вас нормы материального права о противозаконном поведении в сети?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.1 Имеются ли у вас нормы материального права о противозаконном доступе к устройствам, компьютерным системам и данным?

Пояснение. Доступ *– способность и средства осуществлять связь или иное взаимодействие с системой, использовать ресурсы системы для обработки информации, получать сведения об информации, содержащейся в системе, или управлять компонентами и функциями системы (NICCS).*

Компьютерная система *или* ***система*** *– любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, выполняет автоматизированную обработку данных (COE – Конвенция о киберпреступности).*

Компьютерные данные *– любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию (COE – Конвенция о киберпреступности).*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.2 Имеются ли у вас нормы материального права о противозаконном вмешательстве (посредством ввода, изменения или уничтожения данных) в устройства, данные и компьютерные системы?

Пояснение. Вмешательство в компьютерную систему *– умышленное несанкционированное создание серьезных помех функционированию компьютерной системы. Сюда могут относиться ввод, передача, повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.*

Вмешательство в данные *– умышленное несанкционированное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.1.3 Имеются ли у вас нормы материального права о противозаконном перехвате данных в устройствах и компьютерных системах?

Пояснение. Противозаконный перехват *– осуществляемый с использованием технических средств умышленный несанкционированный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы и/или другие электронные системы.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.1.4 Имеются ли у вас нормы материального права о краже идентичности и хищении данных в онлайновой среде?

Пояснение. Кража идентичности в онлайновой среде *– хищение персональных данных, таких как имена, адреса, дата рождения, контактная информация или банковские реквизиты. Это может происходить в результате фишинга, несанкционированного доступа к учетным записям в интернете, извлечения информации из социальных сетей или противозаконного доступа к базам данных.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.2 Имеются ли у вас положения о подлоге с использованием компьютерных технологий (пиратство/нарушение авторского права)?

Пояснение. *Несанкционированный ввод, изменение или стирание компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, в целях совершения обмана или злого умысла.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.3 Имеются ли у вас нормы материального права о безопасности в онлайновой среде?

Пояснение. Безопасность в онлайновой среде *– достижение максимальной защищенности в интернете от различных рисков для безопасности личной или персональной информации или информации, связанной с имуществом, а также усиление самозащиты пользователей от киберпреступлений.*

1.3.1 Имеются ли у вас положения/правовые меры в отношении преступлений, связанных с материалами расистского и ксенофобского характера в онлайновой среде?

Пояснение. *Меры по предотвращению различных форм онлайновых агрессивных высказываний и других форм нетерпимости в отношении расы, цвета кожи, религии, происхождения или национальной или этнической принадлежности, сексуальной ориентации или гендерной идентичности, ограниченных физических возможностей, социального статуса или других характеристик.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.3.2 Имеются ли у вас положения/правовые меры, направленные против преследования и нарушения уважения к достоинству/неприкосновенности личности в онлайновой среде?

Пояснение. Киберпреследование или запугивание *– сообщения по электронной почте, прямые сообщения или оскорбительные веб-сайты, имеющие целью запугивание или иное преследование отдельного лица или группы лиц посредством персонализированных нападок.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

1.3.3 Имеются ли у вас положения/правовые меры, направленные на защиту ребенка в онлайновой среде?

Пояснение. *Законодательство, в котором четко прописано, что все без исключения преступления, какие могут совершаться против ребенка в реальном мире, могут совершаться и в интернете или любой другой электронной сети. Необходимо разработать новые или пересмотреть существующие законы, с тем чтобы установить противозаконность определенных видов поведения, характерных только для интернета, таких как дистанционное склонение детей к совершению или просмотру сексуальных действий или их заманивание для встречи в реальном мире с сексуальными целями (Руководящие указания для директивных органов по защите ребенка в онлайновой среде, разработанные МСЭ).*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

2 Имеются ли какие-либо регламентарные положения в области кибербезопасности, относящиеся к следующим вопросам?

Пояснение. *Регламентарное положение – это правило, основанное на определенной части законодательства и предназначенное для ее исполнения. Исполнение регламентарных положений обычно осуществляется регуляторным органом, созданным для реализации целей или положений законодательства или уполномоченным на это.*

Регламентарные положения в сфере кибербезопасности определяют принципы, которым должны следовать различные заинтересованные стороны и которые проистекают из законов, относящихся к защите данных, уведомлению о нарушениях, требованиям сертификации/стандартизации в области кибербезопасности, требованиям в области кибербезопасности для взрослых, защите конфиденциальности частной информации, защите ребенка в онлайновой среде, цифровым подписям и электронным транзакциям, а также к ответственности поставщиков услуг интернета, и являются частью исполнения этих законов.

2.1 Защита персональных данных/конфиденциальности частной информации.

Пояснение. *Нормативно-правовые положения о защите персональных данных от несанкционированного доступа, изменения, разрушения или использования. Конфиденциальность частной информации в интернете – это степень конфиденциальности и безопасности личных данных, обнародованных в интернете. Это широкий термин, обозначающий множество факторов, способов и технологий, применяемых для защиты*

конфиденциальных данных, частной информации, коммуникаций и предпочтений; примером таких законодательных положений может служить Закон о защите данных.

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Уведомления о случаях утечки данных

Пояснение. *Законодательные и регламентарные положения, касающиеся уведомления о случаях утечки данных, обязывают пострадавшую организацию уведомить о такой утечке соответствующие инстанции, своих клиентов и другие стороны, а также принять меры к устранению причиненного ущерба. Такие законы, как правило, принимаются в ответ на растущее число случаев взлома баз данных, содержащих информацию, позволяющую установить личность пользователей.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3 Требования проверки кибербезопасности

Пояснение. *Проверка безопасности – это систематически и периодически проводимая оценка безопасности информационной системы. Стандартная проверка может включать оценку безопасности физической конфигурации и среды системы, программного обеспечения, процессов обработки информации, а также методов работы пользователей.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.4 Применение стандартов

Пояснение. *Существование одобренной (или утвержденной) государством системы (или систем) для применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственных учреждениях) и в рамках критически важной инфраструктуры (даже если она эксплуатируется частным сектором). Эти стандарты, среди прочего, включают стандарты, разработанные следующими организациями: ИСО, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETCИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.5 Использование цифровых подписей в государственных службах и приложениях (электронное правительство)

Пояснение. *Цифровая подпись – это математический метод, используемый для подтверждения подлинности и целостности сообщения, программного обеспечения или цифрового документа. Электронная транзакция – это продажа или покупка товаров или услуг между предприятиями, домашними хозяйствами, отдельными лицами, правительственными организациями, а также другими государственными или частными организациями, осуществляемые через компьютеризированные сети; примерами соответствующих законодательных документов, среди прочего, являются Закон об электронных сделках, Закон об электронных подписях, Закон об электронных транзакциях и т. д., которые могут содержать положения, предусматривающие учреждение контролера органов сертификации.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.6 Сдерживание спама

Пояснение. *Приведите сведения о любых законах или нормативных актах, ограничивающих деятельность по рассылке СПАМА.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.7 Выявление и защита критически важных государственных информационных инфраструктур

Пояснение. *Критически важная инфраструктура – это основные системы, имеющие решающее значение для обеспечения защищенности, безопасности, в том числе экономической, а также охраны здоровья населения страны. К таким системам, среди прочего, относятся системы обороны, банковские и финансовые системы, системы электросвязи, энергетические системы и т. д. Приведите любые ссылки или документы, которые определяют критически важные инфраструктуры, или документы/новостные материалы, подтверждающие эти определения.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в области правовых норм, относящихся к кибербезопасности, которые связаны с вашей страной.
(Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы)

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

ТЕХНИЧЕСКИЕ МЕРЫ

1 Национальные/правительственные CIRT/CSIRT/CERT

Пояснение. *CIRT-CSIRT-CERT – группы реагирования на компьютерные инциденты, укомплектованные штатами специальные организационные структуры, отвечающие за координацию и поддержку мер реагирования на события или инциденты, связанные с компьютерной безопасностью, на национальном или государственном уровне.*

ПРИМЕЧАНИЕ. *Иногда делается различие между правительственными и национальными CIRT как отдельными/разными структурами – правительственные CIRT обслуживают правительственные учреждения, а национальные CIRT – национальные субъекты, включая частные предприятия и граждан. Иногда их считают одной и той же структурой.*

1.1 Имеется ли национальная/государственная CIRT/CSIRT/CERT?

Пояснение. *Учрежденная решением правительства или являющаяся частью правительственных или национальных структур.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Занимается ли ваша национальная или правительственная CIRT/CSIRT/CERT следующими видами деятельности?

1.2.1 Разработка и реализация мероприятий по повышению осведомленности в вопросах кибербезопасности

Пояснение. *Работа по организации широких информационно-пропагандистских кампаний в целях распространения в масштабах страны информации о безопасном киберповедении в кибер- и онлайн-пространстве.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.2 Проведение регулярных учений по кибербезопасности, таких как CyberDrills

Пояснение. *Запланированное мероприятие, в ходе которого организация имитирует нарушение киберпространства для развития или проверки таких навыков и умений, как предотвращение, выявление подобных нарушений, реагирование на них, смягчение их последствий, а также восстановление после таких нарушений. Проводятся ли такие учения периодически или систематически?*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.3 Распространение общедоступных информационных бюллетеней

Пояснение. *Информационные бюллетени CIRT – донесение до сведения широкой общественности информации о возникающих киберугрозах и рекомендуемых действиях.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2.4 Содействие обеспечению защиты ребенка в онлайновой среде

Пояснение. *CIRT/CSIRT/CERT обеспечивает поддержку инициативам по защите ребенка в онлайновой среде путем проведения кампаний по повышению осведомленности, информирования о происшествиях, связанных с детьми, предоставления учебных материалов по этим вопросам и др.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) Форумом групп реагирования на инциденты и обеспечения безопасности (FIRST)?

Пояснение. *Полноправный или ответственный за взаимодействие член Форума групп реагирования на инциденты и обеспечения безопасности (www.first.org).*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.4 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) с региональной группой CERT?

Пояснение. *Формальная или неформальная связь с какой-либо группой CERT внутри или за пределами страны в рамках региональной группы CERT. Примеры региональных групп CERT: APCERT, AFRICACERT, EGC, OIC и OAS.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.5 Был ли уровень развития вышеупомянутых групп CIRT, CSIRT или CERT сертифицирован по схеме сертификации TI в соответствии с TF-CSIRT – SIM3?

Пояснение. *SIM3 – основа сертификации CIRT.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Отраслевые группы CIRT/CSIRT/CERT

Пояснение. *Отраслевая группа CIRT|CSIRT|CERT – это организация, которая реагирует на связанные с компьютерной безопасностью или кибербезопасностью инциденты, затрагивающие ту или иную отрасль. Отраслевые CERT, как правило, создаются в важнейших отраслях, таких как здравоохранение, коммунальные услуги, научные и образовательные учреждения, экстренные службы и финансовый сектор. Отраслевая CERT обслуживает клиентов только из определенной отрасли.*

2.1 Существуют ли отраслевые группы CIRT/CSIRT/CERT в вашей стране?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2. Занимаются ли ваши отраслевые организации CIRT/CSIRT/CERT следующими видами деятельности?

2.2.1 Подготовка и проведение мероприятий по повышению осведомленности по кибербезопасности в отрасли

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2.2 Активное участие в национальных учениях CyberDrill

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2.3 Распространение информации о случившихся в отрасли инцидентах среди отраслевых предприятий

Пояснение. *Распространение информации о возникающих киберугрозах и рекомендуемых действиях.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Национальная система для применения стандартов кибербезопасности

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

3.1 Имеется ли система для применения/принятия стандартов кибербезопасности?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.2 Распространяется ли эта система на международные или другие соответствующие стандарты?

Пояснение. *МСЭ-Т, ИСО/МЭК, NIST, ANSI/ISA и др.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

4 Защита ребенка в онлайновой среде

Пояснение. *Это показатель наличия в стране национального агентства, занимающегося вопросами защиты ребенка в онлайновой среде; телефонного номера для сообщений о проблемах, связанных с пребыванием детей в онлайновой среде; любых технических механизмов и возможностей, используемых для защиты детей в онлайновой среде; и любой деятельности государственных и негосударственных учреждений по распространению знаний и оказанию поддержки с предоставлением телефонного номера, адреса электронной почты, веб-форм и т. п. для защиты детей в онлайновой среде, по которым заинтересованные стороны могут сообщать об инцидентах или проблемах, связанных с инициативой по защите ребенка в онлайновой среде.*

4. Имеются ли какие-либо механизмы и средства подачи сообщений, которые помогают защитить детей в онлайновой среде?

Пояснение. *Горячие линии, телефоны доверия и т. п.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в технических областях, относящихся к кибербезопасности, которые связаны с вашей страной.
(Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы)

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

ОРГАНИЗАЦИОННЫЕ МЕРЫ

1 Национальная стратегия кибербезопасности

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

1.1 Имеется ли в вашей стране национальная стратегия/политика в области кибербезопасности?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.1 Предусматривает ли она защиту критически важных национальных информационных инфраструктур, в том числе в секторе электросвязи?

Пояснение. *Любые физические или виртуальные информационные системы, которые контролируют, обрабатывают, передают, получают или хранят электронную информацию любого вида, включая данные, голос или видео, имеющие жизненно важное значение для функционирования критически важных инфраструктур, настолько важное, что неработоспособность или разрушение таких систем приведет к катастрофическим последствиям для национальной безопасности, национальной экономической безопасности или здоровья и безопасности населения.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.2 Включает ли она упоминание об устойчивости национальной системы кибербезопасности?

Пояснение. *Национальный план обеспечения устойчивости кибербезопасности гарантирует наличие у страны возможности своевременно и эффективно противостоять последствиям любой угрозы (стихийной или антропогенной), переносить их, приспосабливаться к ним и восстанавливаться своевременно и эффективно, в том числе путем сохранения и восстановления своих собственных основных служб и функций с помощью внешних служб.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.3 Производится ли пересмотр и обновление национальной стратегии кибербезопасности на постоянной основе?

Пояснение. *Установлено управление жизненным циклом стратегии, стратегия обновляется в соответствии с изменениями в национальной, технологической, социальной, экономической и политической сферах, которые могут повлиять на ситуацию с кибербезопасностью в стране.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.1.4 Открыта ли стратегия кибербезопасности для консультаций с национальными экспертами в области кибербезопасности в той или иной форме?

Пояснение. *Стратегия открыта для консультаций со всеми заинтересованными сторонами, включая операторов критически важных инфраструктур, поставщиков услуг интернета, научные учреждения и др.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.2 Имеется ли установленный план действий/дорожная карта по осуществлению управления в области кибербезопасности?

Пояснение. *Стратегический план, определяющий общие результаты в области национальной кибербезопасности, включая необходимые для его реализации шаги и этапы.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

1.3 Имеется ли национальная стратегия защиты ребенка в онлайновой среде?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2 Ответственный орган

Пояснение. *К органам, ответственным за реализацию национальной стратегии/политики кибербезопасности, могут относиться постоянные комитеты, официальные рабочие группы, консультативные советы или междисциплинарные центры. Такие органы также могут быть непосредственно ответственными за работу национальных CIRT. Ответственные органы могут функционировать в рамках правительства и иметь полномочия принуждать другие учреждения и национальные органы к осуществлению политики и внедрению стандартов.*

2.1 Имеется ли орган, ответственный за координацию в области кибербезопасности на национальном уровне?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.1.1 Осуществляет ли этот орган контроль в области защиты важнейшей государственной информационной инфраструктуры?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.2 Имеется ли национальный орган, контролирующий развитие национального потенциала в области кибербезопасности?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

2.3 Имеется ли орган, осуществляющий надзор за реализацией инициатив по защите ребенка в онлайновой среде на национальном уровне?

Пояснение. *Наличие национального органа, предназначенного для надзора за обеспечением защиты ребенка в онлайновой среде и содействия ей.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3 Показатели кибербезопасности

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

3.1 Проводятся ли какие-либо проверки кибербезопасности на национальном уровне?

Пояснение. *Проверка безопасности – систематическая оценка безопасности информационной системы, заключающаяся в измерении степени ее соответствия набору установленных критериев. Всесторонняя проверка, как правило, предусматривает оценку безопасности физической конфигурации и среды системы, программного обеспечения, процессов обработки информации, а также методов работы пользователей. Регуляторные органы могут требовать в отношении критически важных инфраструктур, находящихся в частной собственности, проведения периодической оценки состояния их безопасности и представления отчетов о результатах.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.2 Существуют ли показатели для оценки рисков, связанных с киберпространством, на национальном уровне?

Пояснение. *Это процесс, включающий выявление, анализ и оценку рисков.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

3.3 Имеются ли показатели для оценки уровня развития кибербезопасности на национальном уровне?

Пояснение. *Это подход к измерению уровня развития кибербезопасности в государстве.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок в области организационных мер, относящихся к кибербезопасности, которые связаны с вашей страной. (Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы)

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

РАЗВИТИЕ ПОТЕНЦИАЛА

1 Кампании по повышению осведомленности населения в области кибербезопасности

Пояснение. *Повышение осведомленности населения предусматривает содействие проведению кампаний, охватывающих максимально возможное количество человек, а также использование НПО, учреждений, организаций, поставщиков услуг интернета, библиотек, местных торговых организаций, общественных центров, местных колледжей и программ обучения взрослых, школ и организованных родительских комитетов для распространения информации о безопасном поведении в кибер- и онлайн-пространстве. Сюда относятся такие действия, как создание порталов и веб-сайтов для повышения осведомленности, распространение вспомогательных материалов и другие соответствующие мероприятия.*

1.1 Проводятся ли кампании по повышению осведомленности населения, ориентированные на определенный сектор, такой как МСП, компании частного сектора и госучреждения?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.2 Проводятся ли кампании по повышению осведомленности населения, ориентированные на гражданское общество?

Пояснение. *НПО, общественные организации.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.3 Проводятся ли кампании по повышению осведомленности населения, ориентированные на граждан?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.4 Проводятся ли кампании по повышению осведомленности населения, ориентированные на пожилых людей?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.5 Проводятся ли кампании по повышению осведомленности населения, ориентированные на лиц с особыми потребностями?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.6 Проводятся ли кампании по повышению осведомленности населения с участием родителей, педагогов и детей (связанные с инициативой "Защита ребенка в онлайновой среде" (COP))?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2 Подготовка специалистов по кибербезопасности

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

Сюда также относится подготовка по вопросам кибербезопасности для сотрудников правоохранительных, судебных и других юридических органов. Это специализированная профессионально-техническая подготовка, которая может периодически проводиться для сотрудников полиции, правоохранительных органов, судей, адвокатов, поверенных, юристов, помощников юристов и других лиц, работающих в сфере права и правоприменения. Этот показатель также учитывает наличие утвержденной (или одобренной) правительством структуры (или структур) для сертификации и аккредитации специалистов по признанным на международном уровне стандартам кибербезопасности. В число этих сертификаций, аккредитаций и стандартов входят, помимо прочего, следующие: Cloud Security Knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²) и др.

2.1 Осуществляет ли ваше правительство разработку или проведение курсов профессиональной подготовки по кибербезопасности?

Пояснение. *Содействие проведению курсов по кибербезопасности среди работников (технических, социальных и т. п.) и сертификации специалистов предприятий государственного или частного сектора.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2.2 Имеется ли в вашей стране программа аккредитации специалистов по кибербезопасности?

Пояснение. *Учреждения, проводящие аккредитацию специалистов по кибербезопасности, или любые другие соответствующие механизмы.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для специалистов по кибербезопасности?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2.3.1 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников правоохранительных органов?

Пояснение. *Официальный процесс просвещения специалистов в области правоприменения (сотрудников полиции и правоохранительных органов) по вопросам компьютерной безопасности.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2.3.2 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для сотрудников судебных и других юридических органов?

Пояснение. *Профессиональная или техническая подготовка по кибербезопасности, которая может периодически проводиться для сотрудников полиции, правоохранительных органов, судей, адвокатов, поверенных, юристов, помощников юристов и других лиц, работающих в сфере права и правоприменения.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

2.3.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников МСП/частных компаний?

Пояснение. *Учебные занятия по освоению передового опыта/развитию потенциала в области кибербезопасности для защиты своего бизнеса и т. п. путем правильного использования онлайновых услуг.*

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

2.3.4 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для других должностных лиц из государственного сектора и правительственных учреждений?

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

3 Осуществляет ли ваше правительство/ваша организация разработку или поддержку каких-либо образовательных программ или учебных планов в области кибербезопасности...

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

3.1 В начальной школе?

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

3.2 В средней школе?

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

3.3 В высшей школе?

☐ ***ДА***

☐ ***Нет***

Приведите гиперссылки/URL

Предоставьте документы

4 Научно-исследовательские программы в области кибербезопасности

Пояснение. *Этот показатель используется для оценки инвестиций в национальные научно-исследовательские программы в области кибербезопасности, осуществляемые учреждениями, которые могут быть частными, государственными, академическими, неправительственными или международными. Он также служит для определения наличия признанного на общенациональном уровне учреждения, осуществляющего надзор за выполнением программы. Научно-исследовательские программы исследований в области кибербезопасности включают, помимо прочего, анализ вредоносного программного обеспечения, исследования в области криптографии, уязвимости систем, а также моделей и концепций безопасности. Программы развития кибербезопасности – это программы разработки аппаратного или программного обеспечения, которые включают, в частности, брандмауэры, системы предотвращения вторжения, сети-приманки, а также модули обеспечения безопасности аппаратного обеспечения. Для улучшения координации деятельности различных учреждений и совместного использования ресурсов необходим общий национальный орган.*

4.1 Проводится ли научно-исследовательская деятельность в области кибербезопасности на общенациональном уровне?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

4.1.1 Имеются ли программы НИОКР по кибербезопасности в частном секторе?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

4.1.2 Имеются ли программы НИОКР по кибербезопасности в государственном секторе?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

4.1.3 Вовлечены ли в научно-исследовательскую деятельность высшие учебные заведения, такие как академии и университеты?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

5 Национальная отрасль кибербезопасности

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

5.1 Имеется ли национальная отрасль кибербезопасности?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

6 Имеются ли какие-либо правительственные механизмы стимулирования...

Пояснение. *Этот показатель учитывает любые усилия правительства по стимулированию создания потенциала в области кибербезопасности, будь то путем предоставления налоговых льгот, грантов, финансирования, займов, реализации объектов или за счет других экономических и финансовых средств мотивации, включая признанный на национальном уровне специализированный орган, осуществляющий надзор за деятельностью по созданию потенциала в области кибербезопасности. Стимулы повышают спрос на связанные с кибербезопасностью услуги и продукты, что способствует улучшению защиты от киберугроз.*

6.1 Для содействия созданию потенциала в области кибербезопасности?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

6.2 Для развития отрасли кибербезопасности?

Пояснение. *Поддержка новых компаний в сфере услуг по обеспечению кибербезопасности в научной и других областях.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передового опыта/достижений/текущих разработок, связанных с мерами по созданию потенциала в области кибербезопасности, которые связаны с вашей страной. (Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы)

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.

МЕРЫ В ОБЛАСТИ СОТРУДНИЧЕСТВА

1 Двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами

Пояснение. *Двусторонние соглашения (соглашения, заключаемые одной стороной с другой стороной) – это официально признанные национальные или отраслевые партнерства между правительством одной страны и правительством другой страны или региональной или международной организацией, направленные на трансграничное совместное использование информации или ресурсов в области кибербезопасности (то есть сотрудничество или обмен информацией, квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами). Этот показатель служит также для определения того, осуществляется ли обмен информацией о выявленных угрозах. Создание потенциала – это обмен профессиональными инструментами, расширение круга экспертов и др.*

1.1 Имеются ли у вас двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.1.1 Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?

Пояснение. *Под обменом информацией понимается практика обмена неконфиденциальной информацией.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.1.2 Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?

Пояснение. *Возможность поощрять проведение в рамках сотрудничества учебных занятий для укрепления навыков, компетенций и способностей национальных специалистов по кибербезопасности в целях обеспечения согласованности совместных действий против киберугроз.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

1.1.3 Предусматривает(ют) ли это (эти) соглашение(я) взаимную правовую помощь?

Пояснение. *Оказание двумя или более странами взаимной помощи по сбору и обмену информацией в целях обеспечения применения норм публичного или уголовного права.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

2 Участие правительства в международных механизмах, связанных с деятельностью в сфере кибербезопасности

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

2.1 Участвует ли ваше правительство/ваша организация в международных механизмах, связанных с деятельностью в сфере кибербезопасности?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

3 Многосторонние соглашения по кибербезопасности

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

3.1 Имеются ли у вашего государства многосторонние соглашения о сотрудничестве в области кибербезопасности?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

3.1.1 Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?

Пояснение. *Под обменом информацией понимается практика обмена неконфиденциальной информацией.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

3.1.2 Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?

Пояснение. *Возможность поощрять проведение в рамках сотрудничества учебных занятий для укрепления навыков, компетенций и способностей национальных специалистов по кибербезопасности в целях обеспечения согласованности совместных действий против киберугроз.*

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

4 Партнерские отношения с частным сектором (ГЧП)

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

4.1 Участвует ли ваше правительство в ГЧП с местными компаниями?

☐ *ДА*
☐ *Нет*
Приведите гиперссылки/URL
Предоставьте документы

4.2 Участвует ли ваше правительство в ГЧП с иностранными компаниями в вашей стране?

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

5. Межведомственные партнерства

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

5.1 Имеются ли межведомственные партнерства/соглашения между различными правительственными органами, касающиеся кибербезопасности?

Пояснение. *Сотрудничество между министерствами или специализированными учреждениями.*

☐ *ДА*

☐ *Нет*

Приведите гиперссылки/URL

Предоставьте документы

Просьба привести какие-либо примеры передовой практики/достижений/текущих разработок, относящихся к мерам в области сотрудничества в рамках деятельности в области кибербезопасности, которые связаны с вашей страной. (Подробно опишите пример(ы) в поле для комментариев и включите ссылки на подтверждающие документы)

Или приведите документ(ы), содержащий(е) ссылки на подтверждающие документы.