Руководство для заполнения анкеты по Глобальному индексу кибербезопасности (ГИК) за 2015-2016 годы

Данный документ предназначен исключительно для ознакомительных целей. ГИК оценивает степень выполнения странами обязательств по обеспечению кибербезопасности на основе пяти столпов Глобальной программы кибербезопасности: правовые меры, технические меры, организационные меры, развитие потенциала и сотрудничество.

Данная анкета объединяет в себе вопросы, разработанные для определения итоговой оценки по ГИК за 2015/2016 годы, а также вопросы, предусмотренные в рамках Вопроса 3 2-й Исследовательской комиссии МСЭ-D. Анкета состоит из трех отдельных разделов: в то время как в первых двух разделах приведены вопросы типа "да/нет", последний раздел содержит открытые вопросы. Заполнение анкеты осуществляется в онлайновом режиме. Каждый респондент получит (по официальному адресу электронной почты, предоставленному МСЭ) индивидуальный URL, который необходимо будет сохранить в безопасном месте. Онлайновая анкета позволяет респондентам закачивать соответствующие документы (и URL) по каждому вопросу в качестве справочной информации.

Предполагается, что информация, предоставленная респондентами в рамках данной анкеты, не будет носить конфиденциальный характер.

РАЗДЕЛ 1

1. Существует ли какое-либо законодательство, связанное с киберпространством?

1.1. Существует ли какое-либо законодательство в сфере киберпреступлений?

Поясн.: *В законодательстве касательно киберпреступлений прописаны законы о несанкционированном доступе, вмешательстве в данные или их перехвате, вмешательстве в работу систем или их взломе, а также неправомерном использовании компьютерных систем. Среди них – процессуальное законодательство, действующие статьи об ускоренном сохранении данных, хранимых на компьютере, порядке предоставления информации, сборе компьютерных данных в реальном времени, экстрадиции, взаимопомощи, конфиденциальности и ограничении использования, а также прецедентное право в сфере киберпреступлений и неправомерного использования компьютерной техники; кроме того, сюда относятся преступления, связанные с контентом. Соответствующие положения могут быть включены в национальное уголовное законодательство, Закон о защите данных, Закон о свободе информации, законодательство в сфере авторских прав / интеллектуальной собственности.*

1.1.1. Существует ли какое-либо материальное право в сфере киберпреступлений?

Поясн.: *Под материальным правом подразумевается публичное и частное право всех видов, включая договорное право, право в сфере недвижимости, деликтное право, завещательное право и уголовное право, которое создает, определяет и регулирует права по сути.*

1.1.1.1. Существуют ли какие-либо статьи по несанкционированному доступу к компьютерам, системам и данным?

Поясн.: *Под несанкционированным доступом подразумевается получение доступа к компьютеру, системе и данным с помощью учетной записи другого лица или нечестным путем, включая угадывание/взламывание пароля или кражу идентичности.*

1.1.1.2. Существуют ли какие-либо статьи по несанкционированному вмешательству в данные, работу компьютеров и систем или модификации данных, компьютеров и систем?

Поясн.: *Под несанкционированным вмешательством/модификацией подразумевается незаконное вмешательство в данные, работу системы или компьютера, при котором в первоначальное состояние компьютера, системы или данных вносятся изменения, в том числе, возможно, ввод, повреждение, удаление или общее изменение компьютерных данных.*

1.1.1.3. Существуют ли какие-либо статьи по несанкционированному взлому компьютеров и систем и перехвату данных?

Поясн.: *Под несанкционированным взломом или перехватом подразумевается незаконный сбор компьютерных данных при их передаче по внутренним каналам.*

1.1.2. Существует ли какое-либо процессуальное право в сфере киберпреступлений?

Поясн.: *Правила, согласно которым суд рассматривает и определяет действия в рамках гражданских исков, уголовных и административных производств. Данные правила направлены на обеспечение применения справедливого и последовательного надлежащего судопроизводства или основных принципов отправления правосудия в отношении всех дел, направляемых в суд.*

1.1.2.1. Существуют ли какие-либо статьи по ускоренному сохранению данных, хранимых на компьютере?

Поясн.: Сохранение данных – обязательство, налагаемое государственным органом на отдельное лицо или организацию, требующее обеспечить защиту определенных данных от утери или модификации в течение определенного периода времени.

1.1.2.2. Существуют ли какие-либо статьи о порядке предоставлении данных?

Поясн.: *Порядок предоставления данных – обязательство, налагаемое государственным органом на отдельное лицо или организацию, требующее предоставить правоохранительным органам доступные и определенные компьютерные данные в течение определенного периода времени.*

1.1.2.3. Существуют ли какие-либо статьи по поиску и изъятию данных, хранимых на компьютере?

Поясн.: *Под поиском и изъятием компьютерных данных подразумеваются меры, в том числе законодательные, предоставляющие органам власти полномочия, необходимые для поиска компьютерной системы и компьютерных данных, хранимых на их территории, а также получения доступа к таким данным и компьютерной системе.*

1.1.2.4. Существуют ли какие-либо статьи по сбору данных в реальном времени?

Поясн.: *Под сбором данных в реальном времени подразумеваются меры, в том числе законодательные, предоставляющие органам власти полномочия, необходимые для сбора и регистрации на их территории в реальном времени трафика данных, передача которых осуществляется с помощью компьютерной системы.*

1.1.2.5. Существуют ли какие-либо статьи по экстрадиции киберпреступников?

Поясн.: *Экстрадиция – это процедура, в соответствии с которой государство или страна, после получения официального запроса от другого государства или страны, передает стороне другой юрисдикции лицо, обвиненное или признанное виновным в совершении киберпреступления на территории такой юрисдикции.*

1.1.2.6. Существуют ли какие-либо статьи, относящиеся к взаимопомощи?

Поясн.: *Соглашение между двумя или более странами, направленное на сбор и обмен информацией с целью исполнения общего и уголовного законодательства.*

1.1.2.7. Существуют ли какие-либо статьи, относящиеся к конфиденциальности и ограничению использования?

Поясн.: *Сторона имеет право использовать данные при условии соблюдения определенных положений о конфиденциальности или использования таких данных исключительно в конкретных целях, предусмотренных таким соглашением.*

1.1.3. Существует какое-либо прецедентное право по киберпреступности или неправомерному использованию компьютерной техники?

Поясн.: *Правонарушения, подпадающие под определение неправомерного использования компьютерной техники, могут включать хакерство, несанкционированный доступ к компьютерным системам, а также умышленное распространение вредоносного программного обеспечения. Несанкционированный доступ с целью модификации компьютерной техники может включать изменение программного обеспечения, данных, пароля и настроек для предотвращения получения другими лицами доступа к системе, а также вмешательство в нормальную работу системы для причинения ей вреда.*

1.2. Существуют ли какие-либо законодательные или регламентарные положения в сфере кибербезопасности?

Поясн.: *Регламент – это правило, основанное на и предназначенное для исполнения определенной части законодательства. Исполнение регламентарных положений, как правило, осуществляется регуляторным органом, созданным или уполномоченным реализовывать цели или положения законодательства. Таким образом, регламентарные положения в сфере кибербезопасности определяют принципы, которым должны следовать различные заинтересованные стороны и которые проистекают из и являются частью исполнения законов в сфере защиты данных, уведомления о нарушениях, требований к сертификации/стандартизации в области кибербезопасности, требований в области кибербезопасности для взрослых, защиты конфиденциальности частной информации, защиты ребенка в онлайновой среде,*

цифровых подписей и электронных транзакций, а также ответственности поставщиков услуг интернета.

1.2.1. Существуют ли какие-либо законодательные или регламентарные положения в сфере защиты данных?

Поясн.: *Регламентарные положения, относящиеся к защите личных, коммерческих и государственных данных от несанкционированного доступа, изменения, уничтожения или использования.*

1.2.2. Существуют ли какие-либо законодательные или регламентарные положения в сфере защиты систем и сетей?

Поясн.: *Правовые меры, направленные на защиту систем и сетей от вредоносного вмешательства.*

1.2.3. Существуют ли какие-либо законодательные или регламентарные положения в сфере уведомления о нарушениях?

Поясн.: *Законодательные и регламентарные положения в сфере уведомления о нарушениях – это законодательные и регламентарные положения, обязывающие лицо, ставшее объектом нарушения, уведомлять о таком нарушении органы власти, своих клиентов и другие стороны, а также предпринимать другие меры, направленные на устранение причиненного таким нарушением ущерба. Принятие таких законов, как правило, происходит в ответ на растущее число случаев взламывания баз данных пользователей, содержащих информацию, позволяющую установить личность.*

1.2.3.1. В отношении данных?

Поясн.: *Законы в сфере уведомления о нарушениях, касающиеся утечки данных.*

1.2.3.2. В отношении систем и сетей?

Поясн.: *Законы в сфере уведомления о нарушениях, касающиеся взламывания систем и сетей. Такие законы могут предусматривать, среди прочего, введение стандарта в отношении обеспечения кибербезопасности или других основных требований с целью защитить данные пользователей, например путем кодирования.*

1.2.4. Существуют ли какие-либо законодательные или регламентарные положения по сертификации/стандартизации в сфере кибербезопасности?

Поясн.: *Регламентарные положения в контексте сертификации/стандартизации обязывают лиц, работающих в рамках территории той или иной страны, проходить определенную процедуру сертификации/стандартизации в отношении соответствия минимальным стандартам. Данное требование может отличаться в зависимости от отрасли экономики. Эти стандарты, среди прочего, включают стандарты, разработанные следующими органами: ISO, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS и т. п.*

1.2.4.1. Для государственного сектора?

Поясн.: *Регламентарное положение, касающееся обязательной сертификации/стандартизации в сфере кибербезопасности в государственном секторе.*

1.2.4.2. Для частного сектора?

Поясн.: *Регламентарное положение, касающееся обязательной сертификации/стандартизации в сфере кибербезопасности в частном секторе.*

1.2.5. Предусматривают ли законодательные или регламентарные положения обязательное проведение мер по обеспечению кибербезопасности?

Поясн.: *Меры по обеспечению кибербезопасности могут, среди прочего, включать технические и организационные меры, такие как брандмауэр, список управления доступом, определение функций и сфер ответственности по обеспечению безопасности, а также страхование (собственное) от киберпреступлений.*

1.2.5.1. Со стороны государственного сектора?

1.2.5.2. Со стороны операторов важнейшей инфраструктуры?

Поясн.: *Важнейшая инфраструктура – это основные системы, имеющие решающее значение для обеспечения защиты, безопасности, в том числе экономической, а также общественного здравоохранения, страны. Такие системы, среди прочего, включают следующее: системы обороны, банковская деятельность и финансы, электросвязь, транспорт, здравоохранение, энергетика и т. д.*

1.2.5.3. Со стороны частного сектора?

1.2.6. Предусматривают ли законодательные или регламентарные положения обязательное проведение проверки кибербезопасности?

Поясн.: *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.*

1.2.6.1. Со стороны государственного сектора?

1.2.6.2. Со стороны операторов важнейшей инфраструктуры?

1.2.6.3. Со стороны частного сектора?

1.2.7. Существуют ли законодательные или регламентарные положения, подробно описывающие защиту конфиденциальности частной информации?

Поясн.: *Конфиденциальность частной информации в интернете – это степень конфиденциальности и безопасности личных данных, обнародованных в интернете. Это широкий термин, обозначающий множество факторов. подходов и технологий, применяемых для защиты конфиденциальных данных, частной информации, коммуникаций и предпочтений. Примером таких законодательных положений может служить Закон о защите данных.*

1.2.8. Существуют ли какие-либо законодательные или регламентарные положения, относящиеся к цифровым подписям и электронным транзакциям?

Поясн.: *Цифровая подпись – это математический подход, 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, осуществленные через*

компьютеризированные сети; примерами таких 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 создание контролера органов сертификации.

1.2.9. Существуют ли какие-либо законодательные или регламентарные положения, относящиеся к ответственности поставщиков услуг интернета?

Поясн.: *Поставщики услуг интернета несут ответственность за нарушение авторских прав вследствие действий своих клиентов. Поставщики обязаны сообщать полиции, CERT или другим компетентным органам/национальным органам о незаконных действиях в киберпространстве, возникающих в рамках их инфраструктуры, т. е. выполнять требование относительно активного мониторинга сети.*

1.2.10 Существуют ли какие-либо законодательные или регламентарные положения, относящиеся к ограничению или сдерживанию спама?

1.3. Проводятся ли какие-либо учебные курсы по кибербезопасности для сотрудников правоохранительных и судебных органов, а также других субъектов права?

Поясн.: *Формальный процесс обучения субъектов права вопросам компьютерной безопасности.*

1.3.1. Для сотрудников правоохранительных органов (сотрудников полиции и агентов по принудительному обеспечению исполнения обязательств)?

1.3.2. Для сотрудников судебных органов и других субъектов права (судьи, юрисконсульты, адвокаты, прокуроры, юристы, средний юридический персонал и т. д.)?

1.3.3. Проводится ли обучение на постоянной основе?

Поясн.: *Обучение, проводимое периодически или систематически.*

2. Предпринимаются ли у вас какие-либо технические меры?

2.1. Существуют ли группы CIRT, CSIRT или CERT с общенациональной сферой ответственности?

Поясн.: *CIRT расшифровывается как группа реагирования на компьютерные инциденты. CSIRT – это группа реагирования на нарушения компьютерной безопасности, а CERT – группа реагирования на нарушения компьютерной защиты. Данные термины используются взаимозаменяемо для обозначения организации, получающей, анализирующей и реагирующей на сообщения о нарушении защиты. Национальная CSIRT/CIRT/CERT – это организация , уполномоченная в рамках общенациональной сферы ответственности осуществлять мониторинг и обработку информации об инцидентах кибербезопасности, а также реагирование на них, посредством действующих на местном уровне структур, включая академические организации, правоохранительные органы, гражданское общество, частный сектор (в рамках групп по экономическим вопросам или вопросам большой важности, важнейшей информационной инфраструктуры (энергетика, здравоохранение, транспорт, финансы и т. д.)) и правительственные органы. Кроме того, такая группа взаимодействует с национальными группами CIRT других стран, а также субъектами регионального и международного значения, для обеспечения надлежащей и эффективной координации действий в случае атак.*

2.1.1. Есть ли у такой группы предоставленный правительством мандат?

Поясн.: Подтвержденный решением правительства или являющийся частью мандата правительственных органов.

2.1.2. Проводят ли CIRT, CSIRT или CERT практические занятия по кибербезопасности на постоянной основе?

Поясн.: *Запланированное мероприятие, в ходе которого организация симулирует связанный с использованием киберпространства сбой для развития или проверки таких способностей, как предотвращение, выявление и реагирование на такой сбой, смягчение его последствий, а также восстановление после такого сбоя. Проводятся ли такие занятия периодически или систематически?*

2.1.3. Являются ли CIRT, CSIRT или CERT членами FIRST?

Поясн.: *Полноправный или ответственный за взаимодействие член Форума групп реагирования на инциденты и обеспечения безопасности.*

2.1.4. Являются ли CIRT, CSIRT или CERT членами каких-либо других сообществ CERT? (региональных CERT)

Поясн.: *Наличие какой-либо формальной или неформальной связи с какой-либо CERT внутри или за пределами страны; функционирование в рамках деятельности какой-либо региональной CERT.*

2.2. Существует ли правительственная CERT?

Поясн.: *Правительственная CERT|CIRT|CSIRT – организация, реагирующая на связанные с компьютерной безопасностью или кибербезопасностью инциденты, которые затрагивают исключительно правительственные учреждения. Кроме услуг реагирования, такая группа может предоставлять и превентивные услуги, такие как анализ уязвимости и проверка безопасности. В отличие от национальной CERT,*

предоставляющей услуги как частному, так и государственному сектору, правительственная CERT предоставляет услуги своим клиентам исключительно в государственном секторе.

2.3. Существуют ли какие-либо отраслевые CERT?

Поясн.: *Отраслевая CERT|CIRT|CSIRT – это организация, реагирующая на связанные с компьютерной безопасностью или кибербезопасностью инциденты, которые затрагивают ту или иную отрасль. Отраслевые CERT, как правило, создаются для работы в важнейших отраслях, таких как здравоохранение, коммунальные услуги, экстренные службы, а также финансовый сектор. В отличие от правительственной CERT, предоставляющей услуги государственному сектору, отраслевая CERT предоставляет услуги своим клиентам исключительно в одной отрасли.*

2.4. Существует ли какая-либо программа для применения стандартов кибербезопасности?

Поясн.: *Существование одобренной (или утвержденной) государством программы (или программ) для применения признанных на международном уровне стандартов кибербезопасности в государственном секторе (правительственные органы) и в управлении важнейшей инфраструктурой (даже если оно ведется частным сектором). Эти стандарты, среди прочего, включают стандарты, разработанные следующими органами: ISO, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS и т. п.*

2.4.1. В государственном секторе?

2.4.2. В частном секторе?

2.5. Существует ли какая-либо программа для сертификации и аккредитации специалистов по кибербезопасности?

Поясн.: *Существование одобренной (или утвержденной) государством программы (или программ) для сертификации и аккредитации специалистов в соответствии с признанными на международном уровне стандартами кибербезопасности. Среди прочего, такие программы сертификации и аккредитации и стандарты включают следующие: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Совет ЕС), OSSTMM (ISECOM), PCIP/CCISP (Институт важнейшей инфраструктуры), Q/ISP, Техническая сертификация защиты программного обеспечения (Университет безопасности), CPP, PSP, PCI (ASIS), LPQ, LPC (Институт предотвращения ущерба), CFE (Ассоциация сертифицированных специалистов по расследованию мошенничества), сертифицированные CERT специалисты по устранению компьютерных инцидентов (SEI), CITRMS (Институт финансового образования потребителей), CSFA (Институт кибербезопасности), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Институт внутренних аудиторов), (Международная ассоциация специалистов по управлению рисками), PMP (Институт управления проектами) и т. п.*

2.5.1. В государственном секторе?

2.5.2. В частном секторе?

2.6. Внедрены ли какие-либо механизмы и возможности для решения проблемы спама?

2.7. Доступны ли лицам с ограниченными возможностями какие-либо инструменты обеспечения кибербезопасности, такие как антивирусное или антиспамовое программное обеспечение?

3. Предпринимаются ли у вас какие-либо организационные меры?

3.1. Внедрена ли национальная стратегия кибербезопасности?

Поясн.: *Политика национальных стратегий по кибербезопасности и национальных планов по защите информационной инфраструктуры – это такая политика, которая официально устанавливается и утверждается каждым государством, а также которая может включать следующие обязательства: четкое определение функций и сфер ответственности в области кибербезопасности на всех уровнях управления (местном, региональном и федеральном или национальном), с четким распределением функций и сфер ответственности; установление четких обязательств по обеспечению кибербезопасности – общественных и прозрачных; содействие участию частного сектора и создания партнерств при реализации правительственных инициатив по развитию кибербезопасности; дорожная карта по управлению с определением основных заинтересованных лиц.*

3.1.1. Является ли ваша национальная стратегия обособленной?

Поясн.: *Национальная стратегия кибербезопасности может быть документально изложена отдельно от национальной стратегии в области информации, технологии и безопасности.*

3.1.1.1. Учитывает ли она интересы частного сектора?

Поясн.: *В стратегии определяются связанные с кибербезопасностью функции и сферы ответственности задействованных лиц в рамках частного сектора.*

3.1.1.2. Учитывает ли она интересы государственного сектора?

Поясн.: *В стратегии определяются связанные с кибербезопасностью функции и сферы ответственности задействованных лиц в рамках государственного сектора.*

3.1.1.3. Есть ли раздел, посвященный защите важнейшей информационной инфраструктуры?

Поясн.: *В стратегии содержатся планы по защите важнейшей информационной инфраструктуры.*

3.1.1.4. Есть ли дорожная карта по управлению?

Поясн.: *Стратегия содержит дорожную карту, в которой определены этапы достижения целей и реализации стратегии.*

3.1.1.5. Осуществляется ли пересмотр стратегии на постоянной основе?

Поясн.: *Обновление стратегии осуществляется с учетом национальных особенностей, а также обстоятельств технологического, социального, экономического и политического развития, которые могут повлиять на нее.*

3.1.1.6. Открыта ли стратегия для публичного обсуждения?

Поясн.: *Стратегия открыта для обсуждения с участием всех соответствующих заинтересованных сторон, включая операторов инфраструктуры, ПУИ, академических организаций и т. д.*

3.1.1.7. Содержит ли стратегия национальный план восстановления?

Поясн.: *Национальный план восстановления предусматривает оперативное и эффективное восстановление страны после бедствия (как стихийного, так и антропогенного), в том числе путем сохранения и восстановления ее жизненно важных сооружений и функций.*

3.1.2. Является ли ваша национальная стратегия кибербезопасности частью другой, более широкой национальной стратегии?

3.1.2.1. Есть ли раздел, посвященный защите важнейшей информационной инфраструктуры?

Поясн.: *Важнейшая инфраструктура – это основные системы, имеющие решающее значение для обеспечения защиты, безопасности, в том числе экономической, а также общественного здравоохранения, страны. Такие системы, среди прочего, включают следующее: системы обороны, банковская деятельность и финансы, электросвязь, транспорт, здравоохранение, энергетика и т. д.*

3.1.2.2. Есть ли дорожная карта по управлению сферой обеспечения кибербезопасности?

3.1.3.Определяет ли она приоритеты государственного сектора?

3.1.4.Если стратегия кибербезопасности еще не внедрена, находится ли она в стадии разработки?

3.1.5.Предусматривает ли существующая или разрабатываемая стратегия какие-либо действия в отношении лиц с ограниченными возможностями?

3.2. Существует ли какой-либо национальный орган, ответственный за обеспечение кибербезопасности?

Поясн.: *К ответственным за реализацию национальной стратегии/политики кибербезопасности органам 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 внедрять политику и стандарты.*

3.2.1.Существует ли какой-либо орган, ответственный за защиту важнейшей информационной инфраструктуры?

3.2.2.Существует ли какой-либо национальный орган, выполняющий роль координатора по вопросам спама?

3.3. Существуют ли какие-либо показатели, на основании которых можно было бы измерить развитие кибербезопасности на национальном уровне?

Поясн.: *Существование каких-либо 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 с целью ее улучшения в будущем. Например на основе стандарта ISO/IEC 27004,* предназначенного для измерения управления информационной безопасностью.

3.3.1. Осуществляется ли оценка риска кибербезопасности на периодической основе?

Поясн.: Систематический процесс, включающий в себя определение, анализ и оценку риска.

3.3.1.1. Существуют ли контрольные показатели кибербезопасности для оценки риска?

3.3.1.2. Осуществляется ли измерение и оценка результатов для их улучшения в будущем?

3.3.2. Осуществляются ли проверки кибербезопасности на постоянной основе?

Поясн.: *Проверка безопасности – систематическая оценка безопасности информационной системы, заключающаяся в измерение степени соответствия комплексу установленных критериев. Всесторонняя проверка, как правило, предусматривает оценку безопасности физической конфигурации и среды системы, программного обеспечения, процессов обработки информации, а также методов работы пользователей.*

3.3.2.1. Являются ли они обязательными?

Поясн.: *Вводятся на основании внутренних, отраслевых регламентарных положений или в соответствии с сертификационными стандартами ISO270001.*

4. Проводятся ли мероприятия по созданию потенциала?

4.1. Есть ли в стране орган стандартизации?

Поясн.: *Стандартизация – это отличный показатель уровня зрелости технологий, и появление новых стандартов в важнейших сферах подчеркивает значимость введения стандартов. Хотя кибербезопасность всегда являлась вопросом государственной безопасности, и в разных странах ее обеспечение играет разную роль, существуют общепризнанные стандарты, способствующие применению единых подходов. Эти стандарты, среди прочего, включают стандарты, разработанные следующими органами: ISO, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS и т. п. Данный показатель оценивает существование национального органа стандартизации в области кибербезопасности, а также мероприятия, направленные на разработку и внедрение стандартов кибербезопасности.*

4.1.1. Разрабатывает ли он свои собственные стандарты кибербезопасности?

Поясн.: *Стандарты кибербезопасности – это, как правило, описываемые в публикуемых материалах подходы, которые направлены на защиту киберсреды пользователя или организации. К указанной выше среде принадлежат сами пользователи, сети, устройства, все программное обеспечение, процессы, передаваемая или хранимая информация, приложения, услуги, а также системы, которые можно напрямую или опосредованно присоединить к сетям. Основная задача – снизить риски, в том числе предупредить угрозы кибербезопасности или смягчить их последствия; в некоторых странах вводят международные стандарты, адаптируют их к местной среде, а затем представляют их в качестве национального стандарта.* В других же странах (достигнувших большего прогресса в вопросе научно-исследовательской деятельности) создаются собственные стандарты, зависящие от степени внедрения, которые затем получают международное признание и внедряются в качестве новых международных стандартов.

4.1.2. Внедряет ли он существующие международные стандарты кибербезопасности?

Поясн.: *Стандарты кибербезопасности – это, как правило, описываемые в публикуемых материалах подходы, которые направлены на защиту киберсреды пользователя или организации. К указанной выше среде принадлежат сами пользователи, сети, устройства, все программное обеспечение, процессы, передаваемая или хранимая информация, приложения, услуги, а также системы, которые можно напрямую или опосредованно присоединить к сетям. Основная задача – снизить риски, в том числе предупредить угрозы кибербезопасности или смягчить их последствия; в некоторых странах вводят международные стандарты, адаптируют их к местной среде, а затем представляют их в качестве национального стандарта.* В других же странах (достигнувших большего прогресса в вопросе научно-исследовательской деятельности) создаются собственные стандарты, зависящие от степени внедрения, которые затем получают международное признание и внедряются в качестве новых международных стандартов.

4.2. Осуществляется ли сбор информации с примерами передового опыта или разработка руководящих принципов в области кибербезопасности на национальном или отраслевом уровнях?

Поясн.: *Передовой опыт – методы и процедуры, зарекомендовавшие себя как успешные. Внедрение передового опыта не только снизит вероятность неудачи, но и повысит эффективность.*

4.3. Осуществляются ли инвестиции в программы научно-исследовательской деятельности в области кибербезопасности?

Поясн.: *Научно-исследовательские программы в области кибербезопасности, среди прочего, включают анализ вредоносного программного обеспечения, исследования в области криптографии, уязвимости систем, а также моделей и концепций безопасности. Программы развития кибербезопасности – это программы разработки аппаратного и программного обеспечения, включая, среди прочего, брандмауэры, системы предотвращения вторжения, "медоносы", а также модули обеспечения безопасности аппаратного обеспечения. Существование общего национального органа повысит координацию деятельности разных учреждений и совместное использование ресурсов.*

4.3.1. В государственном секторе?

4.3.2. В высших учебных заведениях?

4.3.3. Существует ли какой-либо признанный на национальном уровне орган, ответственный за надзор за научно-исследовательской деятельностью в области кибербезопасности?

4.4. Осуществляется ли разработка и проведение кампаний по повышению осведомленности общественности в области кибербезопасности?

Поясн.: *Повышение осведомленности общественности предусматривает, среди прочего, содействие проведению масштабных информационных кампаний, охватывающих максимально возможное количество человек, а также использование НПО, учреждений, организаций, ПУИ, библиотек, местных учреждений торговли, общественных центров, компьютерных магазинов, местных образовательных учреждений и программ обучения взрослых, школ и организованных родительских комитетов, для распространения информации о безопасном поведении в кибер- и онлайн-пространстве. Это включает такие меры, как создание порталов и веб-сайтов, способствующих повышению осведомленности, распространению справочных материалов и дальнейшему укоренению культуры кибербезопасности.*

4.4.1. Для организаций?

Поясн.: *Кампании по повышению осведомленности общественности, ориентированные на организации.*

4.4.2. Для гражданского общества?

Поясн.: *Кампании по повышению осведомленности, ориентированные на общественность в целом.*

4.4.2.1. Для взрослого населения (>18 лет)?

4.4.2.2. Для молодежи (12-17 лет)?

4.4.2.3. Для детей (<12 лет)?

4.4.3. Информируется ли общественность о преимуществах использования программного и аппаратного обеспечения и решений на основе услуг в области кибербезопасности в рамках кампаний по повышению осведомленности общественности?

4.4.4. Доступны ли общественности такие решения на основе услуг и программное и аппаратное обеспечение в области кибербезопасности?

Поясн.: *Доступны общественности на бесплатной основе, например в рамках кампании по повышению осведомленности или по сниженному тарифу.*

4.5. Занимается ли ваша организация/правительство разработкой или содействием разработке каких-либо курсов профессиональной подготовки в области кибербезопасности?

Поясн.: *Существование национальных или отраслевых образовательных программ или программ профессиональной подготовки, способствующих проведению посвященных вопросам кибербезопасности курсов для трудовых ресурсов (в технической сфере, сфере социальных наук и т. д.), а также сертификации специалистов в государственном или частном секторе.*

4.5.1. Для организаций?

4.5.2. Для государственного сектора?

4.5.3. Для гражданского общества?

4.6. Занимается ли ваша организация/правительство разработкой или содействием разработке каких-либо образовательных программ или учебных планов в области кибербезопасности?

Поясн.: *Существование и продвижение национальных образовательных курсов и программ, направленных на обучение младших поколений навыкам и профессиям в области кибербезопасности, в школах, колледжах, университетах и других учебных заведениях. Навыки в области кибербезопасности включают, среди прочего, установку эффективного пароля и нераскрытие личной информации в онлайновом режиме. Профессии в области кибербезопасности включают, среди прочего, профессии специалиста по криптоанализу, специалиста по цифровому экспертно-техническому анализу, специалиста по реагированию на инциденты, специалиста по архитектуре безопасности, а также специалиста по тестированию на проникновение.*

4.6.1. В начальной школе?

4.6.2. В средней школе?

4.6.3. В высших учебных заведениях?

4.7. Существуют ли какие-либо правительственные стимулирующие механизмы, которые способствовали бы созданию потенциала в области кибербезопасности?

Поясн.: *Какие-либо стимулирующие меры со стороны правительства, которые способствовали бы созданию потенциала в области кибербезопасности, будь то путем предоставления налоговых льгот, грантов, финансирования или займов, отчуждения сооружений или за счет других экономических или финансовых средств мотивации, включая признанный на национальном уровне специализированный орган, ответственный за надзор за деятельностью по созданию потенциала в области кибербезопасности. Стимулы повышают спрос на связанные с кибербезопасностью услуги и продукты, что повышает уровень защиты от кибератак.*

4.7.1. Существует ли какой-либо признанный на национальном уровне орган, ответственный за надзор за созданием потенциала в области кибербезопасности?

4.8. Существует ли собственная отрасль кибербезопасности?

Поясн.: *Благоприятная экономическая, политическая и социальная среда, способствующая обеспечению кибербезопасности, будет стимулировать развитие частного сектора, ориентированного на обеспечение кибербезопасности. Проведение кампаний по повышению осведомленности общественности, развитие трудовых ресурсов, создание потенциала и внедрение правительственных стимулов станут движущей силой рынка продуктов и услуг в области кибербезопасности. Существование собственной отрасли кибербезопасности подтверждает наличие благоприятной среды и будет стимулировать рост новых компаний в области кибербезопасности, а также смежных рынков киберстрахования.*

4.8.1. Существует ли рынок киберстрахования?

Поясн.: *Киберстрахование – это страховой продукт, предназначенный для защиты предприятий и отдельных лиц от связанных с использованием интернета рисков, а в более широком смысле – от рисков, связанных с инфраструктурой информационных технологий и соответствующей деятельностью.*

4.8.1.1 Предоставляют ли у вас субсидии предприятиям и другим лицам, которые не могут приобрести страховку от киберрисков на открытом рынке?

4.8.2. Предоставляются ли какие-либо стимулы для развития отрасли кибербезопасности?

Поясн.: *Какие-либо стимулирующие меры со стороны правительства, которые способствовали бы созданию потенциала в области обеспечения кибербезопасности, будь то путем предоставления налоговых льгот, грантов, финансирования или займов, отчуждения сооружений или за счет других экономических или финансовых средств мотивации, включая признанный на национальном уровне специализированный орган, ответственный за надзор за деятельностью по созданию потенциала в области кибербезопасности. Стимулы увеличивают спрос на связанные с кибербезопасностью услуги и продукты, что повышает уровень защиты от кибератак.*

4.8.2.1. Оказывается ли какая-либо поддержка новым компаниям в области кибербезопасности?

Поясн.: *Механизмы, внедренные для содействия развитию новых компаний в области кибербезопасности (налоговые стимулы, технологические парки, зоны свободной торговли и т. д.), а также МСП (малые и средние предприятия).*

5. Предпринимаются ли у вас какие-либо меры в области сотрудничества?

5.1. Существуют ли какие-либо двусторонние соглашения, направленные на сотрудничество в области кибербезопасности?

Поясн.: *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 (т. е. сотрудничество или обмен информацией квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами).*

5.1.1. С государствами?

5.1.1.1. Имеет ли такое соглашение обязательную юридическую силу?

Поясн.: *Стандартная юридическая фраза, указывающая на то, что соглашение заключено сознательно и теперь те или иные действия разрешены или запрещены в соответствии с законодательством.*

5.1.1.1.1. В целях совместного использования информации?

Поясн.: *Под совместным использованием информации подразумевается совместное использование данных об угрозах.*

5.1.1.1.2. В целях совместного использования ресурсов?

Поясн.: *Совместное использование ресурсов – это совместное использование профессиональных кадров (откомандирование, назначение или другие временные поручения в отношении сотрудников), сооружений, оборудования и других инструментов и услуг.*

5.1.1.2. Является ли соглашение таким, которое не имеет обязательной юридической силы, носит неофициальный характер или ожидает ратификации?

5.1.1.2.1. В целях совместного использования информации?

5.1.1.2.2. В целях совместного использования ресурсов?

Поясн.: *Ресурсы могут включать людские ресурсы, сооружения, оборудование и т. д.*

5.1.2. С международными организациями?

5.1.2.1. Имеет ли такое соглашение обязательную юридическую силу?

5.1.2.1.1. В целях совместного использования информации?

5.1.2.1.2. В целях совместного использования ресурсов?

Поясн.: Ресурсы могут включать людские ресурсы, сооружения, оборудование и т. д.

5.1.2.2. Является ли соглашение таким, которое не имеет обязательной юридической силы, носит неофициальный характер или ожидает ратификации?

5.1.2.2.1. В целях совместного использования информации?

5.1.2.2.2. В целях совместного использования ресурсов?

Поясн.: Ресурсы могут включать людские ресурсы, сооружения, оборудование и т. д.

5.2. Существуют ли какие-либо многосторонние или международные соглашения, направленные на сотрудничество в области кибербезопасности?

Поясн.: *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 (т. е. сотрудничество или обмен информацией квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами). Такие соглашения могут также предусматривать ратификацию международных соглашений в области кибербезопасности, таких как Конвенция Африканского союза по киберпреступности и защите личных данных, Будапештская конвенция по киберпреступности и т. д.*

5.2.1. Имеет ли такое соглашение обязательную юридическую силу?

5.2.1.1. В целях совместного использования информации?

5.2.1.2. В целях совместного использования ресурсов?

Поясн.: Ресурсы могут включать людские ресурсы, сооружения, оборудование и т. д.

5.2.2. Является ли соглашение таким, которое не имеет обязательной юридической силы, носит неофициальный характер или ожидает ратификации?

5.2.2.1. В целях совместного использования информации?

5.2.2.2. В целях совместного использования ресурсов?

Поясн.: Ресурсы могут включать людские ресурсы, сооружения, оборудование и т. д.

5.3. Принимает ли ваша организация/правительство участие в работе международных форумов/ассоциаций в области кибербезопасности?

5.4. Существуют ли какие-либо действующие государственно-частные партнерства?

Поясн.: *Государственно-частные партнерства (ГЧП) – это совместные предприятия представителей государственного и частного секторов. Оценка данного показателя эффективности может выполняться исходя из числа официально признанных общенациональных и действующих в отдельных секторах ГЧП для совместного использования информации (данных об угрозах) и ресурсов (трудовых ресурсов, процедур, инструментов) в сфере кибербезопасности между государственным и частным секторами (т. е. официальные партнерства по сотрудничеству и обмену информацией, опытом, технологиями и/или ресурсами) как на национальном, так и на международном уровнях.*

5.4.1. С местными компаниями?

5.4.1.1. В целях совместного использования информации?

5.4.1.2. В целях совместного использования ресурсов?

5.4.2. С иностранными компаниями?

5.4.2.1. В целях совместного использования информации?

5.4.2.2. В целях совместного использования ресурсов?

Поясн.: *Ресурсы могут включать людские ресурсы, сооружения, оборудование.*

5.5. Существуют ли какие-либо действующие межведомственные партнерства?

Поясн.: *Данный показатель эффективности касается официальных партнерств между различными правительственными органами (не касается международных партнерств). Сюда могут относиться партнерства между министерствами, департаментами, программами и другими учреждениями государственного сектора, направленные на совместное использование информации или ресурсов.*

5.5.1. В целях совместного использования информации?

5.5.2. В целях совместного использования ресурсов?

Поясн.: *Ресурсы могут включать людские ресурсы, сооружения, оборудование.*

РАЗДЕЛ 2

1. Предпринимаются ли у вас меры по защите ребенка в онлайновой среде?

1.1. Существует ли законодательство по защите ребенка в онлайновой среде?

Поясн.: *Как правило, потребуется введение блока законов, которые разъясняют, что все без исключения преступления, которые могут быть совершены против ребенка в реальном мире, могут, с учетом соответствующих поправок, также быть совершены в интернете или любой другой электронной сети. Кроме того, может потребоваться разработать новые или пересмотреть существующие законы, чтобы установить незаконность определенных видов поведения, которые могут существовать только в интернете, например дистанционное заманивание детей для выполнения или просмотра сексуальных действий или "соблазнение" детей для встречи в реальном мире с сексуальными целями (Руководящие указания для директивных органов по защите ребенка в онлайновой среде, разработанные МСЭ).*

1.2. Существует ли какой-либо орган/лицо, ответственный/ответственное за защиту ребенка в онлайновой среде?

Поясн.: *Существование национального органа, специализирующегося на защите ребенка в онлайновой среде.*

1.2.1. Существует ли какой-либо государственный механизм предоставления информации по вопросам защиты ребенка в онлайновой среде?

Поясн.: *Номер телефона, адрес электронной почты или веб-сайт, с помощью которого заинтересованные стороны могут сообщить о фактах, связанных с защитой ребенка в онлайновой среде, или о соответствующих основаниях для беспокойства.*

1.2.2. Внедрены ли какие-либо механизмы и возможности для содействия защите ребенка в онлайновой среде?

1.2.3. Предпринимали ли правительственные или неправительственные органы какие-либо действия, направленные на предоставление заинтересованным сторонам информации и поддержки относительно методов защиты ребенка в онлайновой среде?

1.2.4. Существуют ли какие-либо образовательные программы по защите ребенка в онлайновой среде?

1.2.4.1. Для учителей?

1.2.4.2. Для родителей?

1.2.4.3. Для детей?

1.3. Внедрена ли национальная стратегия защиты ребенка в онлайновой среде?

1.4. Существуют ли какие-либо кампании по повышению осведомленности общественности относительно защиты ребенка в онлайновой среде?

1.4.1.1. Для взрослого населения (>18 лет)?

1.4.1.2. Для молодежи (12-17 лет)?

1.4.1.3. Для детей (<12 лет)?

РАЗДЕЛ 3

Дополнительный документ: исследование мнения

1. По вашему мнению, насколько важным является повышение осведомленности в вопросах кибербезопасности как основной шаг в достижении такой безопасности?
    a. Не важным
    b. В какой-то степени важным
    c. Важным
    d. Очень важным
2. На какие группы ориентированы кампании по повышению осведомленности в области кибербезопасности в вашей стране?
    a. Дети
    b. Молодежь
    c. Учащиеся
    d. Пожилые люди
    e. Лица с ограниченными возможностями
    f. Частные учреждения
    g. Правительственные учреждения
    h. Прочие
3. На какую из перечисленных ниже групп эта кампания ориентирована больше? Расположите в порядке от 1 до 6 степень ориентированности кампании: от высокой до низкой.
    a. Дети
    b. Молодежь
    c. Учащиеся
    d. Пожилые люди
    e. Лица с ограниченными возможностями
    f. Частные учреждения
    g. Правительственные учреждения
    h. Прочие
4. Какие проблемы кибербезопасности затрагиваются в ходе кампании по повышению осведомленности? (Возможны несколько вариантов ответа)
    a. Безопасность интернета
    b. Конфиденциальность
    c. Мошенничество
    d. "Фишинг"
    e. Вредоносное программное обеспечение
    f. Защита детей в онлайновой среде
    g. Прочие
5. Какова степень важности каждой из этих проблем? Расположите их в порядке от наибольшей до наименьшей степени важности и обоснуйте этот порядок.
    a. Безопасность интернета
    b. Конфиденциальность
    c. Мошенничество
    d. "Фишинг"
    e. Вредоносное программное обеспечение
    f. Защита детей в онлайновой среде
    g. Прочие

6. Получаете ли вы какую-либо помощь от МСЭ или сотрудничаете ли вы с МСЭ в области кибербезопасности?
    a. Если да, приведите подробную информацию и скажите, что вы думаете об эффективности такой помощи/сотрудничества, а также каким образом должны рассматриваться вопросы, связанные с какими-либо конкретными аспектами кибербезопасности.
    b. Если нет, предоставьте обоснование и скажите, как мы можем помочь.