Программа МСЭ-D в области кибербезопасности

Глобальный индекс кибербезопасности – GCIv5

Пересмотренный и окончательный вариант вопросника

Содержание

Стр.

Программа МСЭ-D в области кибербезопасности **1**

Показатели Глобального индекса кибербезопасности в разбивке по составляющим **4**

Правовые меры **4**

1 Законодательство в области киберпреступности 4

2 Регламентация в области кибербезопасности 7

Технические меры **9**

1 Национальные CERT/CIRT/CSIRT или SOC 10

2 Отраслевые CERT/CIRT/CSIRT или SOC 12

3 Национальная система для применения стандартов кибербезопасности 14

Организационные меры **15**

1 Национальная стратегия кибербезопасности 15

2 Ответственный орган 17

3 Показатели кибербезопасности 18

4 Стратегии и инициативы по защите ребенка в онлайновой среде 19

Меры по развитию потенциала **20**

1 Кампании по повышению осведомленности населения в области кибербезопасности 20

2 Подготовка специалистов по кибербезопасности 23

3 Образовательные программы по кибербезопасности в рамках национальных образовательных стандартов 26

4 Программы исследований и разработок (НИОКР) в области кибербезопасности 27

5 Национальная отрасль кибербезопасности 28

6 Государственные механизмы стимулирования 28

Меры в области сотрудничества **29**

1 Двусторонние соглашения по кибербезопасности 29

2 Многосторонние соглашения по кибербезопасности с другими странами 31

3 Договоры о взаимной правовой помощи (ДВПП, связанные с кибербезопасностью 32

4 Государственно-частное партнерство (ГЧП) 32

5 Межведомственные партнерства 33

Определения **34**

Глобальный индекс кибербезопасности GCIv5 – Журнал изменений и определения

Пересмотренная версия вопросника GCIv5, включающая соответствующие меры из предыдущих изданий Глобального индекса кибербезопасности, определения ключевых терминов и обоснования/методики формирования показателей

Условные обозначения

Код-[НОМЕР ИЗДАНИЯ] – код вопроса/раздела в издании, имеющем соответствующий номер

Обоснование-[НОМЕР ИЗДАНИЯ] – логическое обоснование или мотивировка вопроса в соответствующем издании

Показатели Глобального индекса кибербезопасности в разбивке по составляющим

Правовые меры

Обоснование-GCIv5: Законодательство имеет решающее значение для формирования согласованной системы, чтобы различные структуры выстраивали свою деятельность в соответствии с общими правовыми и регуляторными основами, будь то в отношении запретов определенного преступного поведения или минимальных регуляторных требований. Нормативно-правовая база определяет роли, обязанности и ответственность различных заинтересованных сторон. Законодательство в области кибербезопасности можно определить как ответ на пять основных вопросов: "1) безопасность чего мы обеспечиваем?; 2) где и чью безопасность мы обеспечиваем?; 3) как мы обеспечиваем безопасность?; 4) когда мы обеспечиваем безопасность?; и 5) почему мы обеспечиваем безопасность?"[1]. Безопасность данных является важным, но не единственным компонентом кибербезопасности, поскольку кибербезопасность охватывает "системы, в которых хранятся данные, и сети, по которым передаются данные"[2].

Правовые меры также позволяют стране создать основные механизмы реагирования на нарушения – путем проведения расследований, уголовного преследования и наложения санкций за несоблюдение либо нарушение законодательства. Законы защищают безопасность в целом и гарантируют права граждан в ситуации злоупотребления другими лицами, а также обеспечивают защиту в ситуации неправомерного использования новейших технологий. Законодательная база устанавливает минимальный набор стандартов поведения во всех областях, которые применимы ко всем лицам и могут служить основой для дальнейшего формирования потенциала в сфере кибербезопасности. Конечная цель заключается в наличии адекватного странового законодательства, которое позволило бы добиться согласованности практик на наднациональном уровне, обеспечило бы условия для принятия функционально совместимых мер, упростив ведение международной борьбы с киберпреступностью.

Правовая среда может быть измерена с точки зрения наличия правовых институтов и систем по проблематике кибербезопасности и киберпреступности, а также количества этих институтов и систем. Данная подгруппа включает следующие показатели эффективности:

1 Законодательство в области киберпреступности

Код-GCIv5: Legal1

Обоснование-GCIv5: Законодательством в области киберпреступности определяются несанкционированный (без права) доступ к компьютерам, системам и данным, вмешательство в них и их перехват. Это законодательство может относиться к материальному и/или процессуальному, публичному и/или частному, общему, прецедентному, статутному, административному праву или другой применимой форме права.

1.1 Законодательство в отношении несанкционированного онлайнового поведения

Код-GCIv5: Legal1.1

Обоснование-GCIv5: Разные виды онлайнового поведения могут негативно сказаться на безопасности действий в онлайновой среде и уверенности при их совершении. Некоторые из этих видов поведения нашли отражение в международных соглашениях, таких как Конвенция Совета Европы о киберпреступности (Будапештская конвенция) 2011 года. Действующее законодательство в отношении такого поведения может содержать четкие руководящие принципы для

---

1 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022.

2 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022.

правоохранительных органов, вносить ясность в судебную практику и обеспечивать помощь тем, на кого повлияло такое поведение.

1.1.1 Действует ли в вашей стране законодательство о незаконном доступе к устройствам, компьютерным системам и данным?

Код-GCIv5: Legal1.1.1

Обоснование-GCIv5: Разные виды онлайнового поведения могут негативно сказаться на безопасности действий в онлайновой среде и уверенности при их совершении. Одним из способов борьбы с таким поведением является законодательство. Цель данного вопроса состоит в том, чтобы определить, действовало ли в стране на момент заполнения вопросника GCI специальное законодательство о незаконном доступе к устройствам, компьютерным системам и данным, который может привести к нарушению границ частной жизни, нанесению вреда имуществу или достоинству личности, помимо нанесения других видов вреда или ущерба. Планируемое к разработке, существующее в виде проекта и в настоящее время не действующее законодательство не приносит здесь полный балл.

1.1.2 Действует ли в вашей стране законодательство о незаконном вмешательстве (посредством ввода, изменения и/или уничтожения данных) в устройства, данные и компьютерные системы?

Код-GCIv5: Legal1.1.2

Обоснование-GCIv5: Разные виды онлайнового поведения могут негативно сказаться на безопасности действий в онлайновой среде и уверенности при их совершении. Одним из способов борьбы с таким поведением является законодательство. Цель данного вопроса состоит в том, чтобы определить, действовало ли в стране на момент заполнения вопросника GCI специальное законодательство о противодействии незаконному вмешательству (посредством ввода, изменения и/или уничтожения данных) в устройства, данные и компьютерные системы. Планируемое к разработке, существующее в виде проекта и в настоящее время не действующее законодательство не приносит здесь полный балл.

1.1.3 Действует ли в вашей стране законодательство о незаконном перехвате устройств, данных и компьютерных систем?

Код-GCIv5: Legal1.1.3

Обоснование-GCIv5: Разные виды онлайнового поведения могут негативно сказаться на безопасности действий в онлайновой среде и уверенности при их совершении. Одним из способов борьбы с таким поведением является законодательство. Цель данного вопроса состоит в том, чтобы определить, действовало ли в стране на момент заполнения вопросника GCI специальное законодательство о незаконном перехвате устройств, данных и компьютерных систем. Планируемое к разработке, существующее в виде проекта и в настоящее время не действующее законодательство не приносит здесь полный балл.

1.1.4 Есть ли в вашей стране нормы материального права в отношении онлайновой идентичности?

Код-GCIv5: Legal1.1.4

Обоснование-GCIv5: В связи с растущим объемом онлайновой активности людям необходимо иметь возможность идентифицировать себя в онлайновой среде надежными и заслуживающими доверия способами. Нормы, вне зависимости от того, являются ли они частью законов, посвященных непосредственно онлайновой деятельности, являются ли частью законов, связанных с идентичностью, или иных законов, помогают обеспечить правовую основу для использования онлайновой идентичности, управления онлайновой идентичностью и онлайнового поведения.

1.2 Действует ли в вашей стране законодательство о подлоге, связанном с использованием вычислительной техники (пиратство/нарушение авторских прав)?

Код-GCIv5: Legal1.2

Обоснование-GCIv5: Основой цифровой экосистемы является доверие. Компьютерный подлог снижает уровень этого доверия. Компьютерный подлог включает в себя "умышленное совершение и без права на это ввода, изменения, удаления или утаивания компьютерных данных, приводящее к появлению неаутентичных данных, с намерением, чтобы они рассматривались или обрабатывались для законных целей, как если бы они были аутентичными, вне зависимости от того, могут ли они читаться и/или пониматься напрямую"[3]. "Примером может служить случай, когда злоумышленник изменяет аутентичное электронное письмо от финансового учреждения и отправляет измененную версию нескольким получателям (также известно как *фишинг*). Согласно подходам, используемым в ряде стран, документация, предназначенная для возложения имеющих обязательную силу правовых обязательств, должна содержать оригинальные компьютерные данные. В других странах достаточно намерения злоумышленника сделать так, чтобы получившаяся измененная версия считалась юридически обязывающей или чтобы действия совершались соответственно"[4].

1.3 Законодательство в области безопасности в онлайновой среде

Код-GCIv5: Legal1.3

Обоснование-GCIv5: Ниже оценивается нормативно-правовое регулирование определенных видов поведения с учетом дестимулирующего характера антиобщественного поведения в онлайновой среде, приводящего к тому, что пользователи и сообщества чувствуют себя в меньшей безопасности. Нормативно-правовое регулирование такого поведения часто должно обеспечивать тонкий баланс прав человека и, в частности, других ценностей, установленных Конвенцией ООН по правам человека. Следует обратить внимание на то, что нет необходимости, чтобы в законах прямо говорилось, что они применимы к цифровым/онлайновым обстоятельствам, однако судебные органы внутри страны должны признавать, что законы к ним применимы.

1.3.1 Действует ли в вашей стране законодательство, применимое к расистским и ксенофобским онлайновым материалам?

Код-GCIv5: Legal1.3.1

Обоснование-GCIv5: Расистские и ксенофобские онлайновые материалы оказывают значительное негативное воздействие на онлайновые сообщества, в том числе уменьшают разнообразие, разжигают разногласия и могут причинить вред отдельным лицам. Действующее законодательство в отношении расизма и ксенофобии должно быть четким, чтобы людям было легко понять и соблюдать его. Законодательство, не посвященное непосредственно сфере технологий, приемлемо; нет необходимости, чтобы в законодательстве было указано, что оно применимо к расистским и ксенофобским онлайновым материалам, если существуют соответствующие юридические заявления, материалы amicae curiae, прецедентного права, прошлых судебных разбирательств или другие соответствующие материалы, которые доказывали бы применимость к онлайновым обстоятельствам.

---

[3] https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html.

[4] http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls.

1.3.2 Действует ли в вашей стране законодательство, применимое к домогательствам и злоупотреблениям в отношении достоинства/неприкосновенности личности в онлайновой среде?

Код-GCIv5: Legal1.3.2

Обоснование-GCIv5: Домогательства и злоупотребления в отношении достоинства/неприкосновенности личности, особенно в онлайновой среде, могут иметь серьезные негативные последствия для человека. Действующее законодательство определяет, какие случаи берутся правоохранительными органами в работу и каким образом судебные органы рассматривают дела, а также дает возможность помочь пострадавшим, что в конечном итоге способствует доверию и безопасности в онлайновой среде. Законодательство, не посвященное непосредственно сфере технологий, приемлемо; нет необходимости, чтобы в законодательстве было указано, что оно применимо к домогательствам и злоупотреблениям в онлайновой среде или к ксенофобским онлайновым материалам, если существуют соответствующие юридические заявления, материалы amicae curiae, прецедентного права, прошлых судебных разбирательств или другие соответствующие материалы, которые доказывали бы применимость к онлайновым обстоятельствам.

2 Нормативные положения в области кибербезопасности

Код-GCIv5: Legal2

Обоснование-GCIv2: Нормативные положения в области кибербезопасности определяют правила, касающиеся защиты данных, уведомления о нарушениях, требований сертификации/стандартизации в области кибербезопасности, реализации мер по обеспечению кибербезопасности, требований проверки кибербезопасности, защиты конфиденциальности, защиты ребенка в онлайновой среде (COP), цифровых подписей и электронных транзакций, а также ответственности поставщиков услуг интернета. Зачастую нормативные положения служат основой соблюдения закона, определяя, как именно закон должен выполняться. Страны могут повысить эффективность своей работы в области кибербезопасности за счет четких, последовательных, применимых и актуальных нормативных положений.

2.1 Есть ли в вашей стране нормативные положения в отношении защиты персональных данных?

Код-GCIv5: Legal2.1

Обоснование-GCIv5: Нормативные положения в сфере персональных данных укрепляют управление данными, определяя ответственность держателей данных и права отдельных лиц. В них могут содержаться указания об ответственности держателей данных за то, как они используют персональные данные, и они могут обеспечивать, чтобы организации не злоупотребляли собранными данными.

2.2 Есть ли в вашей стране нормативные положения в отношении защиты конфиденциальности?

Код-GCIv5: Legal2.2

Обоснование-GCIv5: Нормативные положения в сфере защиты конфиденциальности гарантируют защиту персональных данных, прозрачность использования данных организациями и наличие у лиц права на доступ к своим персональным данным и их исправление. Нормативные положения могут запрещать организациям продавать персональные данные или обмениваться ими без согласия лица. В рамках защиты конфиденциальности может быть гарантировано право лица осуществлять контроль за своими персональными данными. Неправомерное использование персональных данных может способствовать киберпреступности и подрыву доверия в сфере цифровых технологий.

2.3 Есть ли в вашей стране нормативные положения в отношении уведомления об утечке данных/инцидентах, применимые к субъектам частного сектора?

Код-GCIv5: Legal2.3

Обоснование-GCIv5: Утечка данных может негативно повлиять на отдельных лиц, компании и государственные органы в результате финансовых хищений, кражи персональных данных, негативных последствий для репутации и карательных мер в отношении держателей данных. Эффективное нормативно-правовое регулирование может предусматривать уведомление об утечке данных, т. е. требовать от субъектов своевременно уведомлять лиц, компании и государственные органы об утечке данных. Это позволит лицам, компаниям и государственным органам принимать меры для защиты от вреда, который может быть нанесен в результате утечки данных. В нормативных положениях об утечке данных может распространяться передовой опыт в области управления данными, а также могут содержаться требования о своевременном уведомлении и предоставлении средств правовой защиты пострадавшим.

2.4 Есть ли в вашей стране нормативные положения в отношении требований проверки кибербезопасности, применимые к национальным государственным учреждениям, ведомствам или их подрядчикам?

Код-GCIv5: Legal2.4

Обоснование-GCIv5: Нормативные положения в отношении требований проверки кибербезопасности могут способствовать выявлению рисков кибербезопасности и продвижению более эффективного опыта обеспечения кибербезопасности путем поощрения учреждений, ведомств и их подрядчиков к выявлению и устранению уязвимостей в своих системах. Кроме того, нормативные положения могут побуждать учреждения, ведомства и их подрядчиков следовать передовому опыту обеспечения кибербезопасности и соблюдать международные стандарты.

2.5 Есть ли в вашей стране нормативные положения в отношении стандартов кибербезопасности, применимые к национальным субъектам государственного сектора?

Код-GCIv5: Legal2.5

Обоснование-GCIv5: Субъекты государственного сектора часто становятся целью кибератак. В связи с этим важно, чтобы эти субъекты имели надежную киберзащиту и могли защитить себя и своих граждан. Наличие нормативных положений, касающихся стандартов кибербезопасности, применимых к национальным субъектам государственного сектора, способно помочь обеспечить более эффективную защиту этих субъектов от кибератак, а также гарантировать, что они используют передовой опыт в области кибербезопасности.

В число этих стандартов входят, помимо прочего, 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 EC), OSSTMM (ISECOM), PCIP/CCISP (Институт критической 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), а также связанные с требованиями стандартов ИСО 27001 "Системы менеджмента информационной безопасности", ИСО 28000 "Системы менеджмента безопасности цепочки поставок", МЭК 62443 "Безопасность систем промышленной автоматизации и управления" и другие.

2.6 Есть ли в вашей стране нормативные положения в отношении использования цифровых подписей и электронных операций в сфере государственных услуг и приложений (электронное правительство)?

Код-GCIv5: Legal2.6

Обоснование-GCIv5: Органы государственного управления все чаще используют цифровые подписи и электронные операции при оказании услуг и в своих приложениях. Этот переход к электронным системам имеет ряд преимуществ, включая повышение эффективности и безопасности. Однако в отсутствие надлежащего нормативно-правового регулирования существует риск того, что эти системы могут использоваться неэффективно и небезопасно.

Нормативные положения помогают гарантировать, что граждане могут быть уверены в том, что их данные защищены, а государственные системы эффективны и надежны.

2.7 Есть ли в вашей стране нормативные положения в отношении незапрашиваемых сообщений, также известных как спам?

Код-GCIv5: Legal2.7

Обоснование-GCIv5: Благодаря нормативно-правовому регулированию незапрашиваемых сообщений страны могут создавать более безопасный и приятный опыт в онлайновой среде для всех. Соответствующие нормативные положения помогают защитить граждан от негативного воздействия спама и предотвратить использование людей спамерами.

2.8 Есть ли в вашей стране нормативные положения в отношении определения и защиты объектов национальной критической инфраструктуры?

Код-GCIv5: Legal2.8

Обоснование-GCIv5: Определяя и защищая объекты национальной критической инфраструктуры, страна может управлять рисками, связанными с кибербезопасностью. Нормативно-правовое регулирование защиты национальной критической инфраструктуры помогает странам планировать меры реагирования в случае серьезного бедствия или агрессии, гарантируя, что страна способна быстро и эффективно среагировать на серьезное бедствие или нападение. У страны также должен быть план восстановления после серьезного бедствия или нападения.

2.9 Есть ли в вашей стране нормативные положения в отношении защиты ребенка в онлайновой среде?

Код-GCIv5: Legal2.9

Обоснование-GCIv5: Решение проблемы защиты ребенка в онлайновой среде с помощью соответствующих нормативных положений позволяет соответствующим учреждениям и субъектам принимать меры и выполнять конкретные требования и правила для реагирования на преступления в онлайновой среде/киберпреступления против детей и молодежи, а также для борьбы с этими преступлениями. Принципиально важно, чтобы широкий круг заинтересованных сторон применял подобные правила во всех секторах и слоях общества – от отраслевых операторов до правоохранительных органов и заинтересованных сторон гражданского общества, – которые должны действовать сообща, чтобы способствовать созданию безопасной и защищенной цифровой среды для детей и молодежи.

Технические меры

Обоснование-GCIv5: Технологии составляют первую линию защиты от киберугроз и вредоносных агентов, действующих в онлайновом режиме. В отсутствие адекватных технических мер и возможностей для обнаружения кибератак и реагирования на них страны и их соответствующие организации остаются уязвимыми для киберугроз. Появление и успех ИКТ по-настоящему возможны только в атмосфере доверия и безопасности. Вследствие этого странам следует иметь возможность

разрабатывать стратегии по внедрению общепринятых критериев минимальной безопасности и схем аккредитации для приложений и систем программного обеспечения. Одновременно с этим должно быть создано национальное учреждение, занимающееся киберинцидентами на национальном уровне, или по крайней мере специализированное государственное учреждение и соответствующий национальный механизм для наблюдения за инцидентами, предупреждения о них и реагирования на них.

Технические меры могут быть оценены на основании наличия специализированных учреждений и систем в сфере кибербезопасности, одобренных или созданных страной, а также их количества. Данная подгруппа включает следующие показатели эффективности:

1 Национальные CERT/CIRT/CSIRT или SOC

Код-GCIv5: Tech1

Обоснование-GCIv5: Для обнаружения, предупреждения киберугроз и инцидентов, реагирования на них и смягчения их последствий необходимы эффективные механизмы и институциональные структуры национального уровня. Группы реагирования на компьютерные инциденты (CIRT), группы реагирования на инциденты в области компьютерной безопасности (CSIRTS), группы реагирования на нарушения компьютерной защиты (CERT) и центры обеспечения безопасности (SOC)[5] отвечают за защиту от инцидентов кибербезопасности, их обнаружение и реагирование на них и могут повысить способность страны управлять инцидентами в сфере кибербезопасности. CIRT или SOC могут заниматься созданием базы знаний, которая способствовала бы реализации страной национальной стратегии кибербезопасности, и выработкой подхода к защите критической информационной инфраструктуры; поддержкой формирования национальной культуры и экосистемы кибербезопасности и созданием соответствующих инициатив по повышению осведомленности; поддержкой разработки соответствующих национальных платформ кибербезопасности, таких как национальные системы услуг электронного правительства, управления идентичностью и доступом; и дальнейшим предоставлением стране возможности развивать и укреплять свой потенциал реагирования на инциденты и координации действий.

1.1 Есть ли в вашей стране полностью функционирующие национальные/правительственные CIRT/CSIRT/CERT или SOC?

Код-GCIv5: Tech1.1

Обоснование-GCIv5: Группы реагирования на компьютерные инциденты (CIRT), группы реагирования на инциденты в области компьютерной безопасности (CSIRTS), группы реагирования на нарушения компьютерной защиты (CERT) и центры обеспечения безопасности (SOC) отвечают за защиту от инцидентов кибербезопасности, их обнаружение и реагирование на них. CIRT/CSIRT/CERT и SOC считаются полностью функционирующими при соблюдении следующих условий:

- имеется определенная и утвержденная организационная структура;
- обеспечено укомплектование обученным и квалифицированным персоналом;
- обеспечена безопасность помещений (применяются соответствующие меры для защиты помещений от физических и экологических угроз);
- разработаны и внедрены подробные процессы и процедуры их деятельности;
- приняты и развернуты необходимые технологии для их деятельности;
- внедрены процессы взаимодействия с ключевыми заинтересованными сторонами и партнерами;
- оказание услуг участникам производится эффективно и действенно.

---

[5] https://ieeexplore.ieee.org/document/9296846.

Первоначальные процессы развертывания CIRT могут включать оценку (измерение готовности к созданию CIRT, а также подготовку соответствующих заинтересованных сторон к необходимому участию), проектирование (подготовку подробной проектной документации для CIRT) и процесс создания (развертывание инфраструктуры, установление отношений с заинтересованными сторонами, клиентами, введение процессов и услуг в соответствии с мандатом, начало работы и подачу заявки на членство в международной ассоциации).

1.2 Деятельность национальных CIRT/CSIRT/CERT или SOC

Код-GCIv5: Tech1.2

Обоснование-GCIv5: Национальные группы реагирования на компьютерные инциденты (CIRT), группы реагирования на инциденты в области компьютерной безопасности (CSIRTS), группы реагирования на нарушения компьютерной защиты (CERT) и центры обеспечения безопасности (SOC) отвечают за защиту от инцидентов кибербезопасности, их обнаружение и реагирование на них. Они являются центральной точкой для подготовки отчетности об инцидентах в области кибербезопасности. Они также предоставляют информацию и техническую помощь организациям по предотвращению киберинцидентов, смягчению их последствий и реагированию на них. Кроме того, национальные CIRT или SOC проводят исследования по вопросам кибербезопасности, собирают примеры передового опыта и готовят рекомендации по реагированию на киберинциденты.

1.2.1 Разрабатывают ли ваши национальные/правительственные CIRT/CSIRT/CERT или SOC мероприятия по повышению осведомленности в области кибербезопасности и проводят ли их?

Код-GCIv5: Tech1.2.1

Обоснование-GCIv5: Национальные CIRT или SOC могут играть важную роль в проведении кампаний по повышению осведомленности в области кибербезопасности; будучи центральными координационными органами, они могут получить более широкое представление об имеющихся и возникающих киберугрозах, вызовах в области кибербезопасности, уязвимостях, понимании основных тенденций кибербезопасности, технологических достижениях в области кибербезопасности и передовом опыте обнаружения киберугроз и реагирования на них. Для развития культуры кибербезопасности и распространения знаний о мерах, передовом опыте и поведении в области кибербезопасности CIRT/CSIRT/CERT или SOC должны разрабатывать, проводить и/или координировать инициативы и мероприятия по повышению осведомленности в области кибербезопасности, ориентированные на различные заинтересованные стороны и основанные на сборе информации о меняющейся среде угроз, основных тенденциях кибербезопасности и передовом опыте.

1.2.2 Проводят ли ваши национальные/правительственные CIRT/CSIRT/CERT или SOC регулярные практические (тренировочные) занятия по кибербезопасности?

Код-GCIv5: Tech1.2.2

Обоснование-GCIv5: Практическое занятие – это запланированное мероприятие, в ходе которого организация симулирует связанный с использованием киберпространства сбой для развития или проверки таких способностей, как предотвращение и выявление сбоя, реагирование на него и смягчение его последствий, а также восстановление после такого сбоя. Практические занятия по кибербезопасности, проводимые на регулярной основе совместно с соответствующими заинтересованными сторонами, являются упреждающей мерой, направленной на повышение готовности и устойчивости в области кибербезопасности. CIRT/CSIRT/CERT или SOC следует периодически готовить и проводить занятия по управлению в условиях киберинцидентов/кризисов, в том числе с участием любых соответствующих государственных либо частных организаций по всей стране, для проверки их возможностей реагирования на инциденты.

1.2.3 Занимаются ли ваши национальные/правительственные CIRT/CSIRT/CERT или SOC распространением общедоступных информационных бюллетеней по кибербезопасности?

Код-GCIv5: Tech1.2.3

Обоснование-GCIv5: Общедоступные информационные бюллетени по кибербезопасности являются гарантией того, что учреждения и ведомства осведомлены о возможных угрозах кибербезопасности и могут принять меры предосторожности. Кроме того, наличие информационных бюллетеней может способствовать скоординированному ответу на угрозы кибербезопасности.

1.3 Являются ли ваши национальные/правительственные CIRT/CSIRT/CERT или SOC участниками Форума групп реагирования на инциденты и обеспечения безопасности (FIRST) и/или входят ли они в список TF-CSIRT?

Код-GCIv5: Tech1.3

Обоснование-GCIv5: Национальные CIRT или SOC, являющиеся участниками FIRST, пользуются преимуществами членства в глобальной сети CIRT, возможностями обучения, ресурсами и опытом работников FIRST, а также возможностями сотрудничества и обмена передовым опытом. Критериями соответствия требованиям к участникам FIRST предусматривается активная деятельность стран. При ответе на этот вопрос принимается во внимание статус в списке TF-CSIRT.

1.4 Являются ли вышеуказанные национальные/правительственные CIRT/CSIRT/CERT или SOC участниками региональных CIRT (например, APCERT, PACSON, AFRICA CERT, ENSIA, OIC, OAS)?

Код-GCIv5: Tech1.4

Обоснование-GCIv5: Участие в региональных CIRT предполагает любые формальные или регулярные отношения с любой другой региональной CIRT. Участие в региональных CIRT или CERT имеет множество преимуществ, среди которых возможность обмена знаниями и опытом: региональные CIRT и CERT часто могут делиться соответствующими знаниями и опытом, близкими к условиям страны.

2 Отраслевые CERT/CIRT/CSIRT или SOC

Код-GCIv5: Tech2

Обоснование-GCIv5: Отраслевые CERT/CIRT/CSIRT или SOC служат своим участникам, работающим в определенной отрасли, например в финансовом секторе, академических кругах, сфере энергетики, здравоохранения, электросвязи, коммунальных услуг, критической инфраструктуры и т. д. Отраслевые CIRT или SOC служат своим участникам посредством адаптированного под конкретные потребности специализированного анализа угроз и оказания соответствующих услуг. Страны могут иметь совместные отраслевые CIRT или SOC с другими странами, поскольку отраслевые CIRT или SOC служат участникам из определенной отрасли в нескольких странах. Для целей данного показателя военные CIRT не принимаются во внимание.

2.1 Есть ли в вашей стране отраслевые CIRT/CSIRT/CERT или SOC?

Код-GCIv5: Tech2.1

Обоснование-GCIv5: Отраслевые CERT/CIRT/CSIRT или SOC служат своим участникам, работающим в определенной отрасли, например в финансовом секторе, академических организациях, сфере энергетики, здравоохранения, электросвязи, коммунальных услуг, критической инфраструктуры и т. д. Отраслевые CIRT или SOC служат своим участникам посредством адаптированного под конкретные потребности специализированного анализа угроз и оказания соответствующих услуг. Страны могут иметь совместные отраслевые CIRT или SOC с другими странами, поскольку отраслевые CIRT или SOC служат участникам из определенной отрасли в нескольких странах. Для целей данного

показателя военные CIRT не принимаются во внимание. Отраслевые CIRT/CSIRT/CERT или SOC считаются полностью функционирующими при соблюдении следующих условий:

- имеется определенная и утвержденная организационная структура;
- обеспечено укомплектование обученным и квалифицированным персоналом;
- обеспечена безопасность помещений (применяются соответствующие меры для защиты помещений от физических и экологических угроз);
- разработаны и внедрены подробные процессы и процедуры их деятельности;
- приняты и развернуты необходимые технологии для их деятельности;
- внедрены процессы взаимодействия с ключевыми заинтересованными сторонами и партнерами;
- оказание услуг участникам производится эффективно и действенно.

Частично развернутые отраслевые CIRT могут включать оценку (измерение готовности к созданию отраслевых CIRT, а также подготовку соответствующих заинтересованных сторон к необходимому участию), проектирование (подготовку подробной проектной документации для CIRT) и процесс создания (развертывание инфраструктуры, установление отношений с заинтересованными сторонами, клиентами, введение процессов и услуг в соответствии с мандатом, начало работы и подачу заявки на членство в международной ассоциации).

2.2 Деятельность отраслевых CIRT/CSIRT/CERT или SOC

Код-GCIv5: Tech2.2

Обоснование-GCIv5: Отраслевые группы реагирования на компьютерные инциденты (CIRT), отраслевые группы реагирования на инциденты в области компьютерной безопасности (CSIRTS), отраслевые группы реагирования на нарушения компьютерной защиты (CERT) или отраслевые центры обеспечения безопасности (SOC) отвечают за защиту от инцидентов кибербезопасности, их обнаружение и реагирование на них.

Отраслевые CIRT или SOC являются центральной точкой для подготовки отчетности об отраслевых инцидентах кибербезопасности. Они также предоставляют информацию и оказывают техническую помощь отраслевым организациям по предотвращению киберинцидентов, смягчению их последствий и реагированию на них. Кроме того, отраслевые CIRT или SOC проводят исследования по вопросам кибербезопасности, собирают примеры передового опыта и готовят рекомендации по реагированию на киберинциденты.

2.2.1 Разрабатывают ли отраслевые CIRT, CSIRT, CERT или SOC мероприятия по повышению осведомленности в области кибербезопасности для отрасли и проводят ли их?

Код-GCIv5: Tech2.2.1

Обоснование-GCIv5: Отраслевые CIRT или SOC могут играть важную роль в проведении кампаний по повышению осведомленности в области кибербезопасности в конкретной отрасли. Будучи центральными координационными органами отрасли, они обладают пониманием тенденций в области кибербезопасности, актуальных для их заинтересованных сторон. Основываясь на отраслевом и общем анализе угроз, отраслевые CIRT могут помочь в разработке и проведении мероприятий по повышению осведомленности различных групп заинтересованных сторон, связанных с отраслью, в целях улучшения моделей кибербезопасного поведения.

2.2.2 Принимают ли отраслевые CIRT, CSIRT, CERT или SOC регулярное участие в национальных практических (тренировочных) занятиях по кибербезопасности?

Код-GCIv5: Tech2.2.2

Обоснование-GCIv5: Практическое занятие – это запланированное мероприятие, в ходе которого организация симулирует связанный с использованием киберпространства сбой для развития или

проверки таких способностей, как предотвращение и выявление сбоя, реагирование на него и смягчение его последствий, а также восстановление после такого сбоя. Участие отраслевых CIRT в национальных практических занятиях по кибербезопасности является упреждающей мерой, направленной на повышение общего потенциала в области кибербезопасности.

2.2.3 Распространяют ли отраслевые CIRT, CSIRT, CERT или SOC сведения об инцидентах, связанных с отраслью, среди своих участников?

Код-GCIv5: Tech2.2.3

Обоснование-GCIv5: Обмен сведениями об отраслевых угрозах может позволить заинтересованным сторонам отрасли узнать больше о соответствующих угрозах и уязвимостях и повысить время и эффективность реагирования на инциденты. Кроме того, это может помочь обеспечить более скоординированную реакцию государственных структур, частного сектора и широкой общественности на инциденты кибербезопасности.

3 Национальная система для применения стандартов кибербезопасности

Код-GCIv5: Tech3

Обоснование-GCIv5: Национальные системы для применения стандартов кибербезопасности включают существование утвержденной (или одобренной) правительством системы (или систем) сертификации и аккредитации специалистов в соответствии с международно признанными стандартами 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), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Совет ЕС), OSSTMM (ISECOM), PCIP/CCISP (Институт критической 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), а также связанные с требованиями стандартов ИСО 27001 "Системы менеджмента информационной безопасности", ИСО 28000 "Системы менеджмента безопасности цепочки поставок", МЭК 62443 "Безопасность систем промышленной автоматизации и управления" и другие.

3.1 Есть ли у вашего правительства система для применения/принятия национальных или международно признанных стандартов кибербезопасности?

Код-GCIv5: Tech3.1

Обоснование-GCIv5: Национальные системы для применения стандартов кибербезопасности включают существование утвержденной (либо одобренной) правительством системы (либо систем) для применения/принятия национальных или международно признанных стандартов кибербезопасности. Системой может определяться план или дорожная карта применения/принятия стандартов, будут вовлекаться заинтересованные стороны, для последующих обновлений будут использоваться специальные процедуры, а применение будет вестись в соответствии с конкретными методами.

В число этих стандартов входят, помимо прочего, 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 критической 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), а также связанные с требованиями стандартов ИСО 27001 "Системы менеджмента информационной безопасности", ИСО 28000 "Системы менеджмента безопасности цепочки поставок", МЭК 62443 "Безопасность систем промышленной автоматизации и управления" и другие.

3.2 Учитывается ли в системе для применения/принятия признанных на национальном или международном уровне стандартов кибербезопасности критическая инфраструктура?

Код-GCIv5: Tech3.2

Обоснование-GCIv5: Учет критической инфраструктуры в рамках любой системы для применения/принятия признанных на национальном или международном уровне стандартов кибербезопасности имеет первостепенное значение для повышения уровня защиты и устойчивости критической инфраструктуры и способствует сокращению числа уязвимостей и эффективному управлению рисками кибербезопасности.

Организационные меры

Обоснование-GCIv5: Организационные меры необходимы для надлежащей реализации национального подхода к кибербезопасности. Правительством должны быть установлены стратегические цели, а также план реализации, получения результатов и их анализа. Необходимо создать структуры управления, обладающие полномочиями по реализации подхода к кибербезопасности, мониторинга процесса реализации и оценки результатов. Без четко определенной организационной сети работающих вместе партнеров в промышленности, гражданском обществе и академических организациях усилия в различных секторах и отраслях становятся разрозненными и несвязанными, что мешает гармонизации усилий по развитию потенциала в области кибербезопасности на национальном уровне.

Организационные структуры могут быть оценены на основании наличия и количества институтов и стратегий, структурирующих разработку мер в области кибербезопасности на национальном уровне. Создание эффективной организационной структуры необходимо для содействия развитию кибербезопасности, борьбы с киберпреступностью и поддержки роли наблюдения, предупреждения об инцидентах и реагирования на них для обеспечения внутриучрежденческой, межсекторальной и трансграничной координации между новыми и существующими инициативами.

1 Национальная стратегия кибербезопасности

Код-GCIv5: Org1

Обоснование-GCIv5: Национальная стратегия кибербезопасности обеспечивает основу для распределения ресурсов[6], направленных на определение национальных задач кибербезопасности и установление приоритетов в использовании ресурсов при выполнении этих задач с целью повышения уровня безопасности и устойчивости страны[7]. Наличие стратегии также дает возможность правительству сотрудничать со всеми соответствующими заинтересованными сторонами на национальном уровне. Помимо этого, национальная стратегия кибербезопасности может содействовать продвижению инноваций и защите конфиденциальности и гражданских свобод.

---

6 https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained.

7 https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

Стратегия должна четко определять национальные задачи в сфере кибербезопасности, а также структуру управления, обеспечивающую их выполнение[8].

1.1 Есть ли в вашей стране национальная стратегия кибербезопасности (NCS) или национальная политика кибербезопасности в форме самостоятельного документа или как часть другого документа?

Код-GCIv5: Org1.1

Обоснование-GCIv5: Кибербезопасность несомненно является критически важным вопросом для всех стран. Национальная стратегия кибербезопасности обеспечивает основу для распределения ресурсов для защиты критической инфраструктуры страны. Она также дает возможность правительствам работать с частным сектором для выявления и смягчения киберугроз. Помимо этого, национальная стратегия кибербезопасности может содействовать продвижению инноваций и защите конфиденциальности и гражданских свобод.

1.2 Приоритеты национальной стратегии кибербезопасности

Код-GCIv5: Org1.2

Обоснование-GCIv5: Наличие приоритетов в национальной стратегии обеспечивает скоординированное реагирование на киберриски. Поскольку каждая страна сталкивается с разными проблемами кибербезопасности, внимание к конкретным областям кибербезопасности помогает странам устанавливать приоритеты в использовании ресурсов и координировать ответ на киберугрозы. Большинство практических руководств по разработке национальной стратегии кибербезопасности может быть посвящено разным приоритетам, например такому, как "Разработка национальной стратегии кибербезопасности"[9]. В некоторых стратегиях приоритетные области могут также носить название "основные направления"[10]. Вопросы 1.2.1–1.2.4 охватывают приоритетные области, которые могут быть проработаны в рамках национальной стратегии кибербезопасности страны. Однако страны могут иметь и другие приоритетные области.

1.2.1 Предусматривает ли NCS вашей страны защиту национальной критической инфраструктуры?

Код-GCIv5: Org1.2.1

Обоснование-GCIv5: Национальная критическая инфраструктура включает в себя все, от энергосетей и систем водоснабжения до транспортных сетей и финансовых учреждений. Если хотя бы один из этих элементов выходит из строя, страна погружается в хаос. Вот почему так важно, чтобы национальная стратегия кибербезопасности включала план, обеспечивающий их надежную защиту, поскольку критическая инфраструктура необходима для обеспечения общественного порядка и защищенности, важна для экономики страны и имеет решающее значение для национальной безопасности.

1.2.2 Соблюдены ли в NCS вашей страны принципы управления жизненным циклом, в частности предусмотрены ли мониторинг, оценка и внесение обновлений на регулярной основе?

Код-GCIv5: Org1.2.3

Обоснование-GCIv5: В национальной стратегии кибербезопасности (NCS) страны должны соблюдаться принципы управления жизненным циклом[11], в частности в ней должны быть предусмотрены мониторинг, оценка и внесение обновлений на регулярной основе, чтобы гарантировать, что стратегия остается эффективной и актуальной. Это помогает обнаруживать и

---

8 https://ncsguide.org/the-guide/.

9 http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

10 https://ncsguide.org/the-guide/.

11 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

устранять риски конкретной стратегии, а также обеспечивать необходимую адаптацию стратегии к меняющимся условиям. Продуманный подход к управлению жизненным циклом также помогает обеспечить участие всех заинтересованных сторон в разработке и реализации стратегии и четкое понимание каждым своей роли и обязанностей. Благодаря этому стратегия может выполняться эффективно, когда все работают ради достижения одной цели. Наконец, с использованием принципов управления жизненным циклом можно осуществлять мониторинг реализации стратегии и оценивать ее результаты. Это позволяет при необходимости оперативно корректировать курс и гарантировать, что стратегия остается актуальной и эффективной с течением времени.

1.2.3 Включает ли NCS вашей страны механизм, обеспечивающий проведение регулярных консультаций с экспертами по кибербезопасности и заинтересованными сторонами?

Код-GCIv5: Org1.2.4

Обоснование-GCIv5: Обстановка в сфере кибербезопасности постоянно меняется, и важно иметь механизм регулярного обновления NCS. Источником ценной информации о новейших угрозах и способах противодействия им могут быть эксперты по кибербезопасности. Чтобы повысить эффективность осуществления политики, в ходе реализации NCS также необходимо консультироваться с заинтересованными сторонами, такими как предприятия и граждане. Они могут дать отзыв о работе стратегии и предложить улучшения. Посредством консультаций с экспертами и заинтересованными сторонами NCS может быть адаптирована к нуждам страны.

1.2.4 Есть ли в вашей стране конкретный план действий/дорожная карта по выполнению стратегии кибербезопасности?

Код-GCIv5: Org1.2.5

Обоснование-GCIv5: Конкретный план действий или дорожная карта по выполнению стратегии кибербезопасности является важнейшей частью защиты цифровой инфраструктуры страны и граждан. Без плана трудно распределить ресурсы и измерить прогресс, что может привести к неэффективности и пробелам в охвате. Четко определенный план действий/дорожная карта может помочь гарантировать, что все заинтересованные стороны осознают свои роли и обязанности в выполнении стратегии, а план достижим и реалистичен. Он также может помочь отслеживать и оценивать влияние стратегии в динамике по времени, что позволило бы вносить любые необходимые корректировки.

2 Ответственный орган

Код-GCIv5: Org2

Обоснование-GCIv5: Ответственным органом является компетентный орган, отвечающий за управление кибербезопасностью. Этот орган (единоличный или коллегиальный) должен обладать статусом высшего, иметь прочные позиции на самом высоком правительственном уровне и быть способным обеспечить руководство, координацию действий и контроль за реализацией мер и программ в сфере кибербезопасности. Национальный компетентный орган также должен выступать в качестве органа управления для определения и уточнения ролей, обязанностей, процессов, прав принятия решений и задач, необходимых для обеспечения эффективного подхода к кибербезопасности.

2.1 Есть ли в вашей стране учреждение или министерство, отвечающее за кибербезопасность на национальном уровне?

Код-GCIv5: Org2.1

Обоснование-GCIv5: Национальное учреждение или министерство, отвечающее за кибербезопасность на национальном уровне, может поддерживать согласованное управление киберугрозами и активные действия в области кибербезопасности. Такое учреждение или министерство должно работать с другими государственными ведомствами, частным сектором,

гражданским обществом и иными соответствующими субъектами в целях разработки и реализации национальной стратегии кибербезопасности.

2.2 Есть ли в вашей стране учреждение или министерство, отвечающее за вопросы кибербезопасности, связанные с защитой национальной критической инфраструктуры?

Код-GCIv5: Org2.2

Обоснование-GCIv5: Учреждение или министерство, отвечающее за критическую инфраструктуру на национальном уровне, обеспечивает устойчивость и непрерывность ее работы. К критической инфраструктуре могут относиться важнейшие службы, такие как службы водоснабжения, энергоснабжения и связи, необходимые для функционирования общества. Национальное учреждение или министерство, отвечающее за критическую инфраструктуру, может помочь предотвратить или смягчить подобные сбои, ведя работу с соответствующими заинтересованными сторонами.

2.3 Есть ли в вашей стране учреждение, министерство, целевая группа или другой орган, отвечающий за надзор за развитием национального потенциала в области кибербезопасности?

Код-GCIv5: Org2.3

Обоснование-GCIv5: Скоординированный комплексный подход к развитию необходимых навыков и потенциала в области кибербезопасности может снизить вероятность инцидентов в области кибербезопасности и повысить устойчивость. Кибербезопасность – это многоплановая проблема, требующая координации и сотрудничества многочисленных государственных учреждений и субъектов частной деятельности.

2.4 Входит ли координация инициатив и мероприятий по защите ребенка в онлайновой среде в сферу ответственности какого-либо учреждения, министерства, целевой группы или другого органа в вашей стране?

Код-GCIv5: Org2.5

Обоснование-GCIv5: Координация между заинтересованными сторонами и целевыми группами, а также обеспечение надзора за деятельностью важны для гарантии взаимодополняющих мер по защите ребенка в онлайновой среде (СОР). Обязанности по координацию инициатив и деятельности в области СОР на национальном уровне могут быть возложены на отдельное учреждение, министерство, целевую группу или другой орган или же могут быть частью более широкого круга обязанностей какого-либо органа.

3 Показатели кибербезопасности

Код-GCIv5: Org3

Обоснование-GCIv5: К показателям кибербезопасности относятся любые официально признанные национальные или отраслевые контрольные или референтные показатели 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, стандарт 27004 ИСО/МЭК предназначен для измерений, связанных с управлением информационной безопасностью.

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

Код-GCIv5: Org3.1

Обоснование-GCIv5: Проверки кибербезопасности на национальном уровне могут проводиться ввиду соображений безопасности, во исполнение нормативных или иных документов руководящего характера. Нормативные положения по проведению проверок кибербезопасности необходимы, как

необходимы сами эффективные национальные проверки кибербезопасности. Результаты этих проверки могут облекаться в форму отчетов, кратких обзоров, презентаций, служебных записок или других подобных документов о проверках.

Проверка кибербезопасности – это выявление потенциальных уязвимостей. По мере их выявления возможно проводить оценку и приоритизацию уязвимостей, чтобы определить уровень риска, который они представляют для организации. Существует множество инструментов, которые можно использовать для оценки этих уязвимостей, в том числе сканеры уязвимостей, тестирование на проникновение и практические занятия с участием "красной команды". Каждый из этих инструментов имеет свои сильные и слабые стороны, и для работы важно выбрать правильный инструмент. После выявления уязвимостей важно определить уровень риска, который они представляют для организации.

3.2 Существуют ли показатели/инструменты для оценки рисков кибербезопасности на национальном уровне?

Код-GCIv5: Org3.2

Обоснование-GCIv5: Показатели, используемые для оценки рисков кибербезопасности на национальном уровне, будут различаться в разных странах и должны отражать конкретные угрозы, возможности и проблемы страны. Можно использовать такие показатели, как факторы воздействия, факторы вероятности и ценность соответствующих ресурсов. С их помощью можно определить уровень и серьезность риска для каждой уязвимости и принять соответствующие корректирующие меры[13]. В стандарте 27004[14] ИСО/МЭК предлагаются техники обеспечения безопасности, которые могут использоваться для мониторинга, измерения, анализа и оценки рисков, связанных с кибербезопасностью.

3.3 Существуют ли способы оценки уровня развития кибербезопасности на национальном уровне с использованием таких инструментов, как модель зрелости потенциала кибербезопасности, киберготовность или любые другие подходящие инструменты оценки?

Код-GCIv5: Org3.3

Обоснование-GCIv5: Оценка уровня развития кибербезопасности может позволить странам понять зрелость и надежность их инфраструктуры кибербезопасности, при этом конкретные способы оценки могут различаться от страны к стране. К некоторым часто используемым инструментам оценки уровня развития кибербезопасности на национальном уровне относятся модель зрелости потенциала кибербезопасности[15], киберготовность[16] или любой другой способ, используемый страной. В рамках данного вопроса участие страны в Глобальном индексе кибербезопасности МСЭ не относится к инструментам оценки.

4 Стратегии и инициативы по защите ребенка в онлайновой среде

Код-GCIv5: Org4

Обоснование-GCIv5: Защита ребенка в онлайновой среде (COP) – это собирательный термин, относящийся к стратегиям и инициативам, направленным на защиту детей от нанесения вреда или от эксплуатации при выходе в интернет. Сюда может относиться обеспечение того, что детьми используются компьютерные программы и инструменты фильтрации, соответствующее возрасту, а также обучение родителей и детей способам оставаться в безопасности в онлайновой среде.

---

13 https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

14 https://www.iso.org/standard/64120.html.

15 https://gcscc.ox.ac.uk/cmm-2021-edition.

16 https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Существует множество различных стратегий и инициатив по СОР, обычно предназначенных для удовлетворения конкретных потребностей детей в целевой стране.

4.1 Есть ли в вашей стране национальная стратегия по защите ребенка в онлайновой среде, с которой связаны действующие инициативы по защите ребенка в онлайновой среде?

Код-GCIv5: Org4.1

Обоснование-GCIv5: Согласно руководящим принципам СОР, рекомендуется, чтобы стратегия по СОР была самостоятельным документом целостного характера, поскольку она должна охватывать такие области, связанные с детством, как здравоохранение, благополучие и развитие навыков. В случаях, когда стратегия по СОР представляет собой часть какого-либо иного документа, она зачастую не является целостной, а внимание в ней нередко уделяется только сексуальным злоупотреблениям или детской порнографии.

4.2 Есть ли в вашей стране какие-либо механизмы и возможности национального уровня для доведения сведений до государственных органов, развернутые в целях содействия защите ребенка в онлайновой среде?

Код-GCIv5: Org4.2

Обоснование-GCIv5: Доступные широкой общественности механизмы доведения сведений в целях выявления, отслеживания и решения проблем, связанных с детьми в онлайновой среде, позволяют людям выявлять проблемы, влияющие на ребенка в онлайновой среде, и сообщать о них. Эти механизмы могут также носить технический характер, например предупреждать о специфическом контенте. Такие механизмы доведения сведений могут быть предложены CIRT и правоохранительными органами. В идеале должны работать различные системы, например национальные телефоны доверия либо онлайновые порталы, на которых доступны системы направления к специалистам и системы поддержки.

Меры по развитию потенциала

Обоснование-GCIv5: Развитие потенциала является неотъемлемой частью юридических, технических и организационных мер в рамках Глобального индекса кибербезопасности и движущей силой цифрового развития. Программы развития потенциала направлены на создание навыков, знаний и доверия на местном уровне, что в свою очередь устраняет дефицит квалификаций и создает более открытую для всех экосистему технологий. Кроме того, способность оказывать открытые для всех цифровые услуги все более зависит от квалифицированной рабочей силы. Основа создания потенциала для содействия кибербезопасности может включать повышение осведомленности и оцениваться на основе существования и числа программ НИОКР, образовательных программ и программ профессиональной подготовки, дипломированных специалистов и учреждений государственного сектора.

1 Кампании по повышению осведомленности населения в области кибербезопасности

Код-GCIv5: CapDev1

Обоснование-GCIv5: Кампании по повышению осведомленности населения в области кибербезопасности в первую очередь направлены на обучение безопасному поведению в онлайновой среде. Чтобы добиться значимого изменения поведения, в рамках кампаний по повышению осведомленности населения необходимо убедить людей в важности этой информации, помочь им разобраться в способах реагирования и заставить их реагировать в свете других

приоритетов[17]. При реализации кампаний по повышению осведомленности возникают многочисленные проблемы, связанные прежде всего с тем, что для их проведения требуются значительные усилия и навыки, а также с тем, что "попытка вызвать страх редко приводит к изменению поведения"[18]. В рамках адресных кампаний по повышению осведомленности меры могут корректироваться в целях более эффективного решения подобных проблем.

1.1 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на ММСП?

Код-GCIv5: CapDev1.1

Обоснование-GCIv5: Микро-, малые и средние предприятия (ММСП) являются важнейшей частью экономики страны и должны быть осведомлены об угрозах кибербезопасности, которые могут повлиять на их бизнес. Они сталкиваются с такими специфическими проблемами в плане повышения кибербезопасности, как нехватка ресурсов и технических знаний. С помощью адресных мер возможно решить эти специфические проблемы и добиться для ММСП максимального эффекта. В рамках кампаний по повышению осведомленности в области кибербезопасности, особенно для малых и средних предприятий, среди ММСП может распространяться информация о том, как защитить себя от кибератак и как реагировать в случае такой атаки.

1.2 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на частный сектор в целом?

Код-GCIv5: CapDev1.2

Обоснование-GCIv5: Любой субъект частного сектора сталкивается с проблемами кибербезопасности. Помимо конкретных потребностей ММСП, кампании по повышению осведомленности населения о киберрисках частного сектора могут помочь улучшить модели поведения.

1.3 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на учреждения государственного сектора на местном, муниципальном и национальном уровнях, а также на работников государственного сектора?

Код-GCIv5: CapDev1.3

Обоснование-GCIv5: Кампании по повышению осведомленности в области кибербезопасности могут быть полезны учреждениям государственного сектора. Такие кампании специально разработаны для работников государственного сектора и являются источником важной информации о том, как защитить конфиденциальные данные и критическую инфраструктуру.

1.4 Проводит ли ваше правительство кампании по и повышению осведомленности населения, ориентированные на гражданское общество?

Код-GCIv5: CapDev1.4

Обоснование-GCIv5: Организации гражданского общества могут становиться целью кибератак. Эти атаки могут включать домогательства в онлайновой среде, кражу данных или финансовой информации. Организации гражданского общества должны сознавать риски и защищать себя. Это предполагает обучение персонала, использование безопасных паролей и обновление антивирусного программного обеспечения. Страны могут содействовать защищенности этих важных организаций от

---

[17] Rogers, R.W. Attitude change and information integration in fear appeals. Psychological Reports, 56, (1985) 183−188. Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2), (1993) 147−155. https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8.

[18] https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8.

вреда путем обеспечения осведомленности, что поможет им надежно защищать себя, сети и данные граждан.

1.5 Проводит ли ваше правительство кампании по информированию населения, ориентированные на население в целом?

Код-GCIv5: CapDev1.5

Обоснование-GCIv5: Кибербезопасность не является чем-то, что нужно только предприятиям и правительствам. Граждане наиболее уязвимы для киберпреступности, однако им часто не хватает знаний и инструментов для собственной защиты. Киберпреступники постоянно ищут новые способы кражи данных, денег или идентичности. Это может быть сделано путем взлома компьютерных систем, кражи паролей или создания поддельных веб-сайтов. На национальном уровне правительства могут повышать осведомленность с целью защиты граждан и учить их защищать себя с помощью надежных паролей, учить их быть осторожными при открытии электронных писем и ни в коем случае не разглашать персональную информацию в онлайновой среде. Граждане также должны знать о предупреждающих признаках мошенничества или фишинговой атаки. Правительства должны заниматься информированием всех граждан о кибербезопасности и призывать всех принимать необходимые меры самозащиты в онлайновой среде.

1.6 Проводит ли ваше правительство кампании по информированию населения, ориентированные на престарелых людей (лиц пожилого возраста)?

Код-GCIv5: CapDev1.6

Обоснование-GCIv5: По мере того, как наше население продолжает стареть, все больше и больше пожилых людей будет использовать интернет и электронные устройства. К сожалению, это делает их основной мишенью для киберпреступников. Пожилые люди более уязвимы для киберугроз по ряду причин: они могут быть не так осведомлены об опасностях, связанных с использованием интернета, им не хватает технических навыков для самозащиты, они с большей вероятностью попадутся на удочку и с меньшей вероятностью сообщат о киберпреступлениях.

По этой причине правительства работают над повышением осведомленности лиц пожилого возраста о кибербезопасности, чтобы они оставались в безопасности в онлайновой среде и защищали информацию персонального характера.

1.7 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на лиц с особыми потребностями, в том числе лиц с ограниченными возможностями?

Код-GCIv5: CapDev1.7

Обоснование-GCIv5: По мере перехода от медицинской модели инвалидности к модели инвалидности, основанной на понимании прав человека, устранение социальных барьеров, с которыми сталкиваются лица с особыми потребностями, таких как "архитектурные и коммуникативные барьеры, отношение и структуры общества"[19], может расширить возможности и повысить уровень безопасности таких лиц. Аналогичным образом усиливается потребность повышать осведомленность непосредственно лиц с ограниченными возможностями и проводить их обучение в области кибербезопасности. Лица с ограниченными возможностями более уязвимы для кибератак по ряду причин, включая незнание технологий, зависимость от посторонней помощи и нежелание просить помочь. Поэтому образование и осведомленность крайне важны, и правительства должны обеспечить, чтобы все члены сообщества были охвачены усилиями по обеспечению кибербезопасности. Удовлетворение потребностей этой группы населения в рамках

---

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#.

кампаний по повышению осведомленности имеет значение для открытого для всех и эффективного развития потенциала в области кибербезопасности.

1.8 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на родителей, преподавателей и детей, в рамках деятельности по защите ребенка в онлайновой среде (COP)?

Код-GCIv5: CapDev1.8

Обоснование-GCIv5: Правительству следует содействовать разработке кампаний по повышению осведомленности населения, ориентированных на родителей и преподавателей, чтобы дать им возможность получать больше информации о рисках, которым подвергаются дети и молодые люди, и о вреде, который им наносится, и расширить возможности для решения проблем, связанных с COP.

1.9 Проводит ли ваше правительство кампании по повышению осведомленности населения, ориентированные на детей, в рамках деятельности по защите ребенка в онлайновой среде (COP)?

Код-GCIv5: CapDev1.9

Обоснование-GCIv5: Чем больше времени дети проводят в онлайновой среде, тем они уязвимее. Дети особенно уязвимы для киберугроз, поскольку они могут быть менее осведомлены об опасностях, чем взрослые, и могут не иметь того же уровня знаний и опыта в области кибербезопасности, что и взрослые. Правительствам следует содействовать разработке кампаний по повышению осведомленности населения, ориентированных на детей, чтобы помочь им приобрести знания о разных рисках в онлайновой среде, с которыми они могут столкнуться, расширить их возможности по выявлению и смягчению этих рисков и добиться ответственного поведения в онлайновой среде.

2 Подготовка специалистов по кибербезопасности

Код-GCIv5: CapDev2

Обоснование-GCIv5: Развитие навыков может содействовать формированию квалифицированных кадров в области кибербезопасности с современными знаниями. Подготовка кадров в области кибербезопасности требует постоянных усилий для учета изменений и разработок в этой области.

2.1 Разрабатывает ли ваше правительство или поддерживает учебные курсы по кибербезопасности для специалистов по кибербезопасности?

Код-GCIv5: CapDev2.1

Обоснование-GCIv5: Поскольку все больше предприятий переносят свою деятельность в онлайновую среду, потребность в специалистах по кибербезопасности как никогда высока. Однако слишком часто эти специалисты не имеют необходимой подготовки, чтобы защитить своих работодателей от кибератак. Подготовка по вопросам кибербезопасности важна по нескольким причинам, включая помощь специалистам по кибербезопасности в создании прочной основы для кибербезопасности, умение применять свои знания на практике, быть в курсе последних тенденций и событий в области кибербезопасности, а также помощь специалистам в развитии необходимых навыков для обеспечения безопасности сетей и данных своих организаций.

2.2 Существуют ли в вашей стране признанные на национальном или международном уровне программы аккредитации специалистов по кибербезопасности?

Код-GCIv5: CapDev2.2

Обоснование-GCIv5: Программы аккредитации в области кибербезопасности помогают гарантировать соответствие квалификации специалистов, работающих в этой сфере, высоким

стандартам. Это может способствовать повышению общего качества специалистов по кибербезопасности и поможет защитить людей и организации от потенциального вреда. Кроме того, страны могут укрепить доверие между специалистами по кибербезопасности и их клиентами. Наличие общепризнанной программы аккредитации может гарантировать, что все заинтересованные стороны могут доверять квалификации специалистов, с которыми они работают.

2.3 Национальные отраслевые образовательные программы/программы подготовки по кибербезопасности для специалистов

Код-GCIv5: CapDev2.3

Обоснование-GCIv5: Внутри страны специалисты, работающие в различных отраслях, могут извлечь пользу из образовательных программ/программ подготовки по кибербезопасности, которые направлены на решение конкретных проблем и ситуаций, с которыми сталкиваются эти специалисты, и на оснащение их необходимыми навыками.

2.3.1 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для правоохранительных органов на национальном уровне?

Код-GCIv5: CapDev2.3.1

Обоснование-GCIv5: Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для правоохранительных органов на национальном уровне?

2.3.2 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для работников судебной системы на национальном уровне?

Код-GCIv5: CapDev2.3.2

Обоснование-GCIv5: Работники национальной судебной системы играют важнейшую роль в обеспечении безопасности своих стран, и им необходимо обладать знаниями и инструментами для борьбы с угрозами кибербезопасности**.** При планировании национальных программ подготовки по кибербезопасности необходимо учитывать подготовку по кибербезопасности для работников судебной системы и других субъектов правовой отрасли, профессиональную или техническую подготовку по кибербезопасности, которая может периодически проводиться для судей, адвокатов, поверенных, юристов, помощников юристов и других лиц, работающих в сфере права и правоприменения.

2.3.3 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для ММСП? [НЕ СЧИТАТЬ]

Код-GCIv5: CapDev2.3.3

Обоснование-GCIv5: ММСП необходимы программы подготовки по кибербезопасности, поскольку они хранят большое количество конфиденциальных данных, которые могут быть украдены или скомпрометированы в случае кибератаки. Кроме того, ММСП часто не знают о рисках, связанных с использованием технологий, и могут не иметь необходимых инструментов или ресурсов для защиты своих данных. Обучение по кибербезопасности может помочь ММСП понять риски, связанные с использованием технологий, и способы защиты своих данных. Кроме того, обучение может помочь ММСП выявлять подозрительную активность и реагировать на кибератаки. Предоставляя ММСП инструменты и знания, необходимые им для защиты своих данных, страны, в свою очередь, помогают защитить свое экономическое развитие.

2.3.4 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для частного сектора в целом?

Код-GCIv5: CapDev2.3.4

Обоснование-GCIv5: Частный сектор все чаще сталкивается с растущими масштабами, размахом и сложностью киберрисков, которые влияют на финансы, репутацию и имущество корпораций. Технологии являются лишь одним из компонентов кибербезопасности, поэтому реализация политики и программ для изменения поведения людей в частном секторе может повысить устойчивость и снизить киберриски.

2.3.5 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для сотрудников государственного сектора/правительства в целом?

Код-GCIv5: CapDev2.3.5

Обоснование-GCIv5: Государственный сектор предоставляет важнейшие услуги гражданам и предприятиям. Для безопасного предоставления услуг субъектам государственного сектора необходимо глубокое понимание кибербезопасности и того, как защитить себя и своих избирателей от цифровых угроз. Сотрудники государственного сектора/правительства, работающие вне судебной системы и правоохранительных органов, могут извлечь пользу из образовательных программ и программ подготовки по кибербезопасности.

2.3.6 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для субъектов сектора финансов, здравоохранения, электросвязи, транспорта и/или энергетики?

Код-GCIv5: CapDev2.3.6

Обоснование-GCIv5: Проблемы кибербезопасности часто отличаются по секторам. Учитывая критически важную роль финансового сектора, здравоохранения, телекоммуникаций, транспорта и энергетики, целевые программы подготовки для этих субъектов могут обеспечить поддержку общего уровня кибербезопасности страны.

2.3.7 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для молодежи?

Код-GCIv5: CapDev2.3.8

Обоснование-GCIv5: Традиционно правительства принимают меры, чтобы исправить влияние негативных факторов на рынке и для поддержки групп, которые в противном случае обслуживались бы в недостаточной степени. Разработка и поддержка государственных образовательных программ и программ подготовки по кибербезопасности — это та область, в которой частному сектору может не хватать эффективной отдачи для стимулирования участия. Правительство может, помимо прочих вариантов, оказать поддержку в виде финансовых грантов, помощи в обучении, поддержке ученичества. Молодые люди, рассматривающие возможность построения карьеры в области кибербезопасности, могут больше нуждаться в такой поддержке, поскольку им не хватает финансового капитала для самостоятельного инвестирования в образование.

2.3.8 Разрабатывает ли ваше правительство или поддерживает образовательные программы или программы подготовки по кибербезопасности для педагогов, например образовательные программы по защите ребенка в онлайновой среде?

Код-GCIv5: CapDev2.3.9

Обоснование-GCIv5: Педагоги имеют возможность прививать детям и подросткам позитивные модели поведения в области кибербезопасности благодаря своей роли в обучении детей и подростков. Обеспечение подготовки для педагогов по вопросам, связанным с кибербезопасностью, таким как защита детей в интернете, демонстрирует, что страны работают над долгосрочными мерами в области кибербезопасности, поддерживая педагогов, работающих с новым поколением пользователей интернета по мере их появления в онлайновой среде.

3 Образовательные программы по кибербезопасности в рамках национальных образовательных стандартов

Код-GCIv5: CapDev3

Обоснование-GCIv5: Для повышения квалификации населения в области кибербезопасности необходимо включить принципы, играющие важнейшую роль для кибербезопасности, в национальные образовательные стандарты, что может подготовить учащихся всех возрастов к более эффективному противодействию рискам кибербезопасности.

3.1 Разрабатывает ли ваше правительство или поддерживает какие-либо образовательные программы по кибербезопасности, предусмотренные в рамках образовательных стандартов начального образования?

Код-GCIv5: CapDev3.1

Обоснование-GCIv5: Дети в учреждениях начального образования или учащиеся на уровне 1 МСКО начинают обучение в школе и, как правило, осваивают основные навыки чтения, письма и математики[20]. Включение на этом этапе мероприятий по формированию основ кибербезопасного поведения может способствовать повышению осведомленности и кибербезопасности на протяжении всей жизни. Однако дети на этом уровне могут еще не обладать навыками критического мышления и самостоятельной оценки рисков кибербезопасности, и поэтому подвержены особым рискам.[21] Деятельность на этом уровне может включать мероприятия по защите ребенка в онлайновой среде.

3.2 Разрабатывает ли ваше правительство или поддерживает какие-либо образовательные программы по кибербезопасности, предусмотренные в рамках образовательных стандартов среднего образования?

Код-GCIv5: CapDev3.2

Обоснование-GCIv5: Учащиеся учреждений среднего образования, обучающиеся по программам уровней 2 и 3 МСКО, часто вовлечены в образовательную деятельность, целью которой является "заложить фундамент для обучения на протяжении всей жизни и развития человека, на основе которого системы образования могут затем расширить дальнейшие образовательные возможности", а затем "предназначены для завершения среднего образования в рамках подготовки к высшему образованию или для получения навыков, необходимых для трудоустройства, или для того и другого[22]". Введение в курс кибербезопасности на этом этапе может не только помочь подготовить учащихся к тому, чтобы они приобрели навыки более безопасного поведения в онлайновой среде, но и способствовать развитию интереса, который может привести к построению карьеры в области технологий и кибербезопасности.

3.3 Разрабатывает ли ваше правительство или поддерживает какие-либо образовательные программы по кибербезопасности, предусмотренные в рамках образовательных стандартов высшего образования?

Код-GCIv5: CapDev3.3

Обоснование-GCIv5: Студенты, получающие высшее образование, также известное как МСКО 5-8, часто заканчивают обязательные образовательные курсы. Программы высшего образования могут включать курсы, направленные на: получение участниками профессиональных знаний, навыков и

---

[20] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf.

[21] https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/.

[22] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf.

компетенций (МСКО 5); получение участниками промежуточных академических и/или профессиональных знаний, навыков и компетенций, ведущих к получению первой степени или эквивалентной квалификации (МСКО 6); получение участниками продвинутых академических и/или профессиональных знаний, навыков и компетенций, ведущих к получению второй степени или эквивалентной квалификации, такой как степень магистра или эквивалентный уровень (МСКО 7), либо к получению продвинутой научной квалификации, такой как квалификация уровня докторантуры (МСКО 8)[23]. Решение вопросов кибербезопасности на этих образовательных уровнях может содействовать формированию осведомленной и одаренной в вопросах квалификации рабочей силы, а также способствовать развитию потенциала для целей научно-исследовательской деятельности и разработок.

4 Программы исследований и разработок (НИОКР) в области кибербезопасности

Код-GCIv5: CapDev4

Обоснование-GCIv5: Научно-исследовательская деятельность и разработки в государственном, частном и академическом секторах могут обеспечить поддержку усилиям в области кибербезопасности путем развития человеческого потенциала, разработки новых методов и продуктов, а также лучшего понимания рисков и мер по их снижению. Научные исследования и разработки могут охватывать как технические, так и нетехнические решения.

4.1 Проводят ли субъекты частного сектора в вашей стране деятельность по исследованиям и разработкам, связанным с кибербезопасностью?

Код-GCIv5: CapDev4.1

Обоснование-GCIv5: Исследования и разработки под руководством частного сектора демонстрируют готовность частного сектора инвестировать в дальнейший рост и инновации в области кибербезопасности и совершенствовать имеющиеся на рынке решения в области кибербезопасности.

4.2 Проводят ли национальные субъекты государственного сектора в вашей стране деятельность по исследованиям и разработкам, связанным с кибербезопасностью?

Код-GCIv5: CapDev5.2

Обоснование-GCIv5: Активное участие субъектов государственного сектора в деятельности по исследованиям и разработкам, связанным с кибербезопасностью, может способствовать более эффективному выявлению и устранению уязвимостей в инфраструктуре кибербезопасности страны. Оно также может способствовать разработке решений в области кибербезопасности, которые могут быть использованы для защиты критически важной инфраструктуры страны. Научно-исследовательская деятельность государственного сектора, связанная с кибербезопасностью**,** также может обеспечить подготовку к кибератакам. Для целей данного вопроса субъекты государственного сектора должны принадлежать к национальному правительству, а не к правительству штата или местному правительству.

4.3 Проводят ли академические учреждения вашей страны деятельность по исследованиям и разработкам, связанным с кибербезопасностью?

Код-GCIv5: CapDev5.3

Обоснование-GCIv5: Академический сектор играет важную роль в деятельности по исследованиям и разработкам, связанным с кибербезопасностью. Академическое сообщество вносит свой вклад в

---

[23] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf.

передовые исследования и новое мышление, готовит следующее поколение профессионалов и выступает в качестве связующего звена с частным и государственным секторами.

4.4 Существуют ли в вашей стране программы/инициативы по оценке кибербезопасности продуктов ИКТ, например схемы маркировки или сертификации?

Код-GCIv5: CapDev4.2

Обоснование-GCIv5: Схемы сертификации и маркировки, в рамках которых оценивается кибербезопасность продуктов ИКТ, могут способствовать повышению стандартов кибербезопасности производителей, обеспечению подотчетности и облегчению выбора продуктов потребителями. Страны могут применять различные типы схем в зависимости от национальных условий и потребностей.

5 Национальная отрасль кибербезопасности

Код-GCIv5: CapDev5

Обоснование-GCIv5: Развитие и поддержка национальной отрасли кибербезопасности может как поддержать внутренний потенциал для решения и совершенствования проблем кибербезопасности, так и привести к проактивному управлению кибербезопасностью.

5.1 Существует ли в вашей стране отечественная отрасль кибербезопасности?

Код-GCIv5: CapDev5.1

Обоснование-GCIv5: Благоприятная экономическая, политическая и социальная среда, способствующая развитию 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.

5.2 Существуют ли в вашей стране организации или ассоциации, которые способствуют развитию отрасли кибербезопасности в вашей стране?

Код-GCIv5: CapDev5.4

Обоснование-GCIv5: Активная и вовлеченная отрасль кибербезопасности может быть усилена организациями и ассоциациями, в частности путем содействия обмену знаниями, развитию талантов, доступу к инвестициям и финансированию. Эти организации и ассоциации могут получать поддержку от отрасли или поддержку от национальных правительств или других ведомств.

6 Государственные механизмы стимулирования

Код-GCIv5: CapDev6

Обоснование-GCIv5: Инвестиции в безопасность могут служить положительным внешним фактором, что не учитываются теми, кто инвестирует средства или усилия. Для решения проблемы потенциального недостаточного инвестирования или усилий в кибербезопасность правительства могут вмешаться, чтобы создать стимулы для повышения кибербезопасности, такие как финансирование, регулирование или другие механизмы. Это может повысить уровень кибербезопасности в стране по сравнению с тем уровнем, который мог бы сложиться без поддержки.

6.1 Существуют ли какие-либо государственные механизмы стимулирования, которые способствовали бы развитию потенциала в области кибербезопасности?

Код-GCIv5: CapDev6.1

Обоснование-GCIv5: Государственные механизмы стимулирования могут содействовать развитию потенциала в области кибербезопасности, например прохождение обучения, участие в непрерывном образовании или разработка новых программ развития потенциала, такие механизмы стимулирования, как гранты, стипендии, поддержка оплаты, займы или возможности трудоустройства.

6.2 Существуют ли какие-либо государственные механизмы стимулирования для развития или дальнейшего развития индустрии кибербезопасности?

Код-GCIv5: CapDev6.2

Обоснование-GCIv5: Учитывая характер информационных товаров, таких как кибербезопасность, возможно возникновение монополий[24]. Чтобы способствовать появлению новых идей и методов в новых и существующих организациях, а также поощрять участие в обеспечении кибербезопасности различных субъектов и заинтересованных сторон, правительства могут предоставлять стимулы в виде денежных грантов, снижения налогов или сборов, репутационных преимуществ, выгодных договорных условий или побуждать компании, организации и отдельных лиц к участию в экосистеме кибербезопасности.

6.3 Существуют ли в вашей стране государственные механизмы стимулирования для поощрения деятельности по исследованиям и разработкам, связанным с кибербезопасностью?

Код-GCIv5: CapDev6.3

Обоснование-GCIv5: Государственные механизмы стимулирования полезны, когда существующие рыночные силы не дают желаемых результатов. Выгоды от НИОКР, связанных с кибербезопасностью, могут иметь положительный внешний эффект для общества в целом, поэтому правительства могут поощрять НИОКР, связанные с кибербезопасностью, различными способами, такими как, например, предоставление грантов, кредитных продуктов, благоприятных условий для торговой и коммерческой деятельности, контрактов, поддержки университетской деятельности.

Меры в области сотрудничества

Обоснование-GCIv5: Для обеспечения кибербезопасности необходимо привлечение всех отраслей и областей знания и использовать многосторонний подход для решения этой задачи. Сотрудничество укрепляет диалог и координацию, что позволяет сформировать более инклюзивное поле применения принципов кибербезопасности. Учитывая, что кибербезопасность охватывает различные отрасли, географические области и уровни ресурсов, необходимо сотрудничество на частном, государственном, региональном и международном уровнях. Активизация совместных инициатив может обеспечить гораздо более мощный потенциал в области кибербезопасности, помогая сдерживать повторяющиеся и постоянные угрозы в онлайновой среде, а также проводить более эффективное расследование, задержание и судебное преследование злоумышленников.

Сотрудничество на национальном и международном уровнях можно оценить по наличию и количеству партнерств, механизмов сотрудничества и сетей обмена информацией.

1 Двусторонние соглашения по кибербезопасности

Код-GCIv5: Coop1

---

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf.

Обоснование-GCIv5: Двусторонние соглашения (соглашения, заключаемые одной стороной с другой стороной) – это официально признанные национальные партнерства между правительством одной страны и правительством другой страны или региональной межправительственной организацией, направленные на трансграничное совместное использование ресурсов в области кибербезопасности (то есть обмен информацией, квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами) для снижения рисков трансграничных киберконфликтов. Показатель также измеряет, является ли соглашение юридически обязательным или ожидает ратификации. Активы могут обозначать совместное использование специалистов (прикомандирование, размещение или другие временные назначения сотрудников), помещений, оборудования и других инструментов и услуг.

1.1 Двустороннее(ие) соглашение(я) по кибербезопасности с другими странами

Код-GCIv5: Coop1.1

Обоснование-GCIv5: Двусторонние соглашения (соглашения, заключаемые одной стороной с другой стороной) – это официально признанные национальные партнерства между правительством одной страны и правительством другой страны, направленные на трансграничное совместное использование ресурсов в области кибербезопасности (то есть обмен информацией, квалифицированными кадрами или специальными знаниями, а также технологиями и другими ресурсами). Обмен знаниями, квалифицированными кадрами и специальными знаниями между странами может помочь создать мощный потенциал реагирования на инциденты, а также разработать проактивные меры по борьбе с рисками кибербезопасности.

1.1.1 Осуществляется ли в вашей стране обмен информацией по кибербезопасности в рамках двустороннего(их) соглашения (соглашений) с другими странами?

Код-GCIv5: Coop1.1.1

Обоснование-GCIv5: Соглашения по кибербезопасности, которые касаются обмена информацией, демонстрируют повышение обязательств стран в области кибербезопасности, поскольку они облегчают рассмотрение потенциальных рисков, проведение оценки угроз и сотрудничество в области кибербезопасности.

1.1.2 Является ли развитие потенциала кибербезопасности в вашей стране частью двустороннего(их) соглашения (соглашений) с другими странами?

Код-GCIv5: Coop1.1.2

Обоснование-GCIv5: Соглашения, способствующие развитию потенциала в области кибербезопасности на двусторонней основе, расширяют возможности стран по активному противодействию киберрискам путем обмена передовым опытом, повышения квалификации персонала, расширения сотрудничества, повышения осведомленности, разработки и внедрения оперативных процедур, связанных с кибербезопасностью.

1.2 Соглашение(я) по кибербезопасности с международными и региональными организациями

Код-GCIv5: Coop1.2

Обоснование-GCIv5: Учитывая важность региональных межправительственных организаций, страны все чаще заключают соглашения о сотрудничестве в области кибербезопасности для трансграничного обмена средствами кибербезопасности, такого как обмен информацией, экспертными знаниями, технологиями и другими ресурсами, как между отдельными странами, так и в составе их членства в региональной межправительственной организации с другими региональными межправительственными организациями, такими как Европейский союз, АСЕАН, ЭКОВАС, ОАГ, АС и др.

1.2.1 Осуществляет ли ваша страна или региональная межправительственная организация, членом которой является ваша страна, обмен информацией в области кибербезопасности в рамках двустороннего(их) соглашения (соглашений) с другими региональными и международными организациями?

Код-GCIv5: Coop1.2.1

Обоснование-GCIv5: Соглашения по кибербезопасности, которые касаются обмена информацией, демонстрируют повышение обязательств стран в области кибербезопасности, поскольку они способствуют устранению потенциальных рисков, обмену данными по оценке угроз и сотрудничеству в области мер, связанных с кибербезопасностью.

1.2.2 Входит ли развитие потенциала в области кибербезопасности вашей страны или региональной межправительственной организации, членом которой является ваша страна, в двустороннее(ие) соглашение(я) с другими региональными и международными организациями?

Код-GCIv5: Coop1.2.2

Обоснование-GCIv5: Двусторонние соглашения по кибербезопасности, которые касаются развития потенциала в области кибербезопасности между странами и региональными межправительственными организациями, могут повысить потенциал в области кибербезопасности путем обмена передовым опытом, повышения квалификации персонала, расширения сотрудничества, повышения осведомленности, разработки и внедрения оперативных процедур, связанных с кибербезопасностью.

2 Многосторонние соглашения по кибербезопасности с другими странами

Код-GCIv5: Coop2

Обоснование-GCIv5: Участие в письменных многосторонних соглашениях требует согласия по ключевым определениям и параметрам, связанным с кибербезопасностью, и определяет общую повестку дня для достижения прогресса в области кибербезопасности. Они также могут способствовать мерам по укреплению доверия в рамках создания механизмов положительной обратной связи для построения мирных отношений.

2.1 Является ли ваша страна участником многостороннего соглашения по кибербезопасности, включающего обмен информацией о кибербезопасности?

Код-GCIv5: Coop2.1.1

Обоснование-GCIv5: Соглашения по кибербезопасности, которые касаются обмена информацией, демонстрируют повышение обязательств стран в области кибербезопасности, поскольку они облегчают рассмотрение потенциальных рисков, обмен данными о проведении оценки угроз и сотрудничество в отношении мер, связанных с кибербезопасностью.

2.2 Является ли ваша страна участником многостороннего соглашения по кибербезопасности, которое предусматривает совместное развитие потенциала?

Код-GCIv5: Coop2.1.2

Обоснование-GCIv5: Участие в письменных многосторонних соглашениях, включающих развитие потенциала, может поддержать развитие потенциала в странах с более нестабильным положением дел в области кибербезопасности и поддержать меры по укреплению доверия.

3 Договоры о взаимной правовой помощи (ДВПП)[25], связанные с кибербезопасностью

Код-GCIv5: Coop3

***Обоснование* - GCIv5**: Учитывая транснациональный характер кибербезопасности, принятие мер в отношении угроз, затрагивающих суверенитет другого государства, требует четких механизмов сотрудничества, особенно в судебных вопросах. Взаимная правовая помощь, например в форме договоров о взаимной правовой помощи (ДВПП), среди прочих форм помощи, может варьироваться от вручения документов и передачи доказательств до помощи в проведении расследований[26].

3.1 Участвует ли ваша страна в договорах о взаимной правовой помощи (ДВПП) по кибербезопасности в рамках двусторонних или многосторонних соглашений с другими странами, региональными или межправительственными организациями?

Код-GCIv5: Coop3.1

Обоснование-GCIv5: Учитывая транснациональный характер кибербезопасности, принятие мер в отношении угроз, затрагивающих суверенитет другого государства, требует четких механизмов сотрудничества, особенно в судебных вопросах. Взаимная правовая помощь, например в форме договоров о взаимной правовой помощи (ДВПП), среди прочих форм помощи, может варьироваться от вручения документов и передачи доказательств до помощи в проведении расследований[27].

4 Государственно-частное партнерство (ГЧП)

Код-GCIv5: Coop4

Обоснование-GCIv5: Государственно-частное партнерство стало частью тенденции, обусловленной как идеологическими причинами, так и стремлением к рациональному использованию средств[28]. Особенно в области кибербезопасности, где новые инновации часто появляются в частном секторе, участие в ГЧП может помочь правительствам быстрее извлечь выгоду из этих новых инноваций и потенциально улучшить кибербезопасность. Однако ГЧП также сопряжено с рядом проблем, таких как проблемы принципала-агента, управление внешними факторами, сложность переговоров по контракту, гибкость контракта и эффективная оценка[29].

4.1 Участвует ли ваше правительство в ГЧП в области кибербезопасности с отечественными компаниями?

Код-GCIv5: Coop4.1

Обоснование-GCIv5: В силу присущих сетевых эффектов ГЧП с отечественными компаниями может способствовать формированию отечественной экосистемы кибербезопасности, позволяя отечественным субъектам частного сектора развивать и расширять свои навыки, системы и услуги.

---

25 https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html.

26 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL.

27 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL.

28 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5.

29 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66.

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

Код-GCIv5: Coop4.2

Обоснование-GCIv5: На кибербезопасность, как на информационное благо, оказывают влияние сетевые эффекты и экспертные знания, полученные в результате масштабирования[30]. Международные субъекты, обладающие экспертными знаниями в области кибербезопасности, полученным в различных национальных контекстах или в разных странах, могут предложить дополнительные преимущества правительствам, стремящимся повысить национальную кибербезопасность. Правительства, участвующие в ГЧП с иностранными субъектами, могут использовать эти экспертные знания для собственного роста и безопасности.

5 Межведомственные партнерства

Код-GCIv5: Coop5

Обоснование-GCIv5: Любые официальные внутренние партнерские отношения между различными государственными учреждениями в стране могут способствовать реагированию правительства на риски в области кибербезопасности. Партнерства могут включать партнерские отношения для обмена информацией или активами между министерствами, ведомствами, программами и другими учреждениями государственного сектора. Для целей данного раздела не рассматриваются межведомственные партнерства между учреждениями разных стран или межправительственными организациями.

5.1 Существуют ли в вашей стране специальные процессы межведомственной координации по кибербезопасности между различными национальными правительственными органами?

Код-GCIv5: Coop5.1

Обоснование-GCIv5: Любое официальное внутреннее партнерство между различными государственными учреждениями в стране может способствовать реагированию правительства на риски в области кибербезопасности. Партнерства могут включать партнерские отношения для обмена информацией или активами между министерствами, ведомствами, программами и другими учреждениями государственного сектора. Для целей данного раздела не рассматриваются межведомственные партнерства между учреждениями разных стран или межправительственными организациями.

---

30 https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf.

Определения

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
Академические круги		Научное и образовательное сообщество.	Оксфордский словарь английского языка		Tech2; CapDev4.1.3; CapDev6.2
Академические учреждения		Учреждения как часть научного и образовательного сообщества.	Оксфордский словарь английского языка		CapDev4.1.3
Соглашение		Взаимные обязательства между государствами или другими сторонами в письменной форме и регулируемые международным правом, воплощенные в одном документе или в двух или более связанных между собой документах.	Адаптировано по Венской конвенции о праве международных договоров		
Двустороннее соглашение		Письменное соглашение между двумя сторонами, включая государства, региональные органы или организации, подписанное соответствующими лицами, принимающими решения.	GCIv2		Coop1; Coop1.1; Coop1.1.1; Coop1.1.2; Coop1.1.3
Развитие потенциала		Развитие потенциала представляет собой процесс изменений. Это часто приравнивается к расширению штата, обеспечению подготовки и проведению практических семинаров. Индивидуальные программы подготовки и практические семинары могут быть частью комплексного плана развития потенциала, однако их одних недостаточно. Например, обучение отдельного человека не гарантирует, что это обучение будет затем применено на рабочем месте. Развитие потенциала должно быть более широким и охватывать совершенствование систем здравоохранения для повышения эффективности и обеспечения устойчивости. В рамках этого процесса должна проводиться оценка того, как система работает в настоящее время и какие области нуждаются в поддержке; например, разработка и внедрение информационных систем здравоохранения, обучение персонала в области анализа данных, разработка политики и процедур для эффективного финансового управления, или улучшение поставок и распределения ключевых продуктов здравоохранения.	ПРООН https://www.undp-capacitydevelopment-health.org/en/capacities/		Org2.3; CapDev1; CapDev6.1; Coop1.1.2

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
Защита ребенка в онлайновой среде	COP	Защита ребенка в онлайновой среде направлена на защиту детей и молодежи от угроз и рисков, с которыми они могут столкнуться в онлайновой среде. Концепция защиты ребенка в онлайновой среде предполагает принятие целостного подхода к созданию безопасных, соответствующих возрасту, инклюзивных и доступных для всех цифровых пространств для детей и молодежи, характеризующихся: • реагированием, поддержкой и самопомощью в случае угрозы; • предотвращением вреда; • динамическим балансом между обеспечением защиты и предоставлением детям возможности быть цифровыми гражданами; • соблюдением прав и обязанностей как детей, так и общества.	https://www.itu-cop-guidelines.com/		Legal1.3.3; Tech1.2.4 Tech4; Org1.3; Org2.4; CapDev1.6
Критическая инфраструктура (см. также: "Национальная критическая инфраструктура")		Ключевые системы, услуги и функции, нарушение или уничтожение которых окажет разрушительное воздействие на здоровье и безопасность населения, торговлю, национальную безопасность или любое их сочетание.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	К таким системам, среди прочего, относятся системы обороны, банковские и финансовые системы, системы электросвязи, энергетические системы и т. д.	Tech1.2
Критическая информационная инфраструктура	КИИ	Материальные и цифровые активы, сети, услуги и установки, которые в случае нарушения их функционирования или уничтожения окажут серьезное влияние на здоровье, безопасность или экономическое благосостояние граждан и эффективную работу правительства страны.	МЕЖДУНАРОДНЫЙ СПРАВОЧНИК ПО CIIP 2008/2009 ГГ.	К таким системам, среди прочего, относятся пункты телефонной связи, пункты обмена интернет-трафиком, беспроводные сети, спутники и т. д.	
Законодательство в области киберпреступности		Законодательство в области киберпреступности предусматривает правила поведения и стандарты поведения при использовании интернета, компьютеров и связанных с ними цифровых технологий, а также действий общественности, правительства и частных организаций; нормы доказательственного и уголовного процессуального права, а также другие вопросы уголовного правосудия в киберпространстве; регулирование...	https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html		Legal1
Требования проверки кибербезопасности		Проверка безопасности – это систематически и периодически	GCIv4		Legal2.3n

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		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.			
Экосистема кибербезопасности		Сообщество субъектов, действующих в сфере кибербезопасности и около нее, с проходящими совместную эволюцию функциями и обязанностями.	По книге Moore, James. *The Death of Competition (Смерть конкуренции). 1996 г.*	В частности, специалисты в области права, техники, коммерческого сектора и политики, совместно работающие над вопросами, связанными с кибербезопасностью	CapDev5.1, CapDev6.2
Устойчивость в области кибербезопасности		Способность восстанавливаться после нарушения безопасности или атак. Национальный план обеспечения устойчивости в области кибербезопасности гарантирует наличие у страны возможности своевременно и эффективно противостоять последствиям любой угрозы (в том числе 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.	https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc		Tech1.3
Договоры и соглашения по кибербезопасности		Договор или соглашение между двумя странами, организациями или другими группами, связанными непосредственно с кибербезопасностью.	https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478		
Уведомление об утечке данных		Законодательные и нормативные 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.	GCIv2		Legal2.2

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
Незаконный доступ		В случае умышленного деяния неправомерный доступ ко всей или любой части компьютерной системы. Любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным злым умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.	GCIv2		Legal1.1.1
Незаконный перехват		В случае умышленного совершения неправомерный перехват, осуществляемый техническими средствами, непубличных передач компьютерных данных в компьютерную систему, из такой системы или внутри нее, включая электромагнитные излучения от компьютерной системы, несущей такие компьютерные данные.	GCIv2		Legal1.1.3
Незаконное вмешательство		"Неправомерное умышленное повреждение, удаление, порча, изменение или уничтожение компьютерных данных" и "в случае умышленного совершения серьезное неправомерное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или уничтожения компьютерных данных".	GCIv2		Legal1.1.2
Уведомление об инциденте		Уведомление CIRT или других соответствующих заинтересованных сторон об инциденте кибербезопасности.			Legal2.2
Межведомственные партнерства/ соглашения		Любые официальные внутренние партнерские отношения между различными государственными учреждениями в стране могут способствовать реагированию правительства на риски в области кибербезопасности. Партнерства могут включать партнерские отношения для обмена информацией или активами между министерствами, ведомствами, программами и другими учреждениями государственного сектора. Для целей данного раздела не рассматриваются межведомственные партнерства	GCIv2		Coop5

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		между учреждениями разных стран или межправительственными организациями.			
Процессы межведомственной координации		Координация между двумя или более государственными учреждениями по вопросам для работы над согласованными целями и мероприятиями			Coop5.1
Микро-, малые и средние предприятия	ММСП	Определения микро-, малых и средних предприятий могут различаться в зависимости от страны. По возможности следует использовать определения, отслеживаемые Форумом по финансированию МСП.		https://www.smefinanceforum.org/data-sites/msme-country-indicators	CapDev1.1; CapDev2.3.3
Многосторонние соглашения		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). Это может быть ратификация международных соглашений в области кибербезопасности, таких как Конвенция Африканского союза о кибербезопасности и защите личных данных, Будапештская конвенция о киберпреступности и т. д.	GCIV2		Coop3; Coop3.1.1; Coop3.1.2
Национальная критическая инфраструктура (См. также: "критическая инфраструктура")		Ключевые системы, услуги и функции, нарушение или уничтожение которых окажет разрушительное воздействие на здоровье и безопасность населения, торговлю, национальную безопасность или любое их сочетание.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf		Legal2.7; Org1.1.1
Национальная CIRT		CIRT (группа реагирования на компьютерные инциденты), CERT (Группа реагирования на нарушения компьютерной защиты) или CSIRT (Группа реагирования на инциденты в сфере компьютерной безопасности) являются	Из GCI2.		

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		конкретными организационными структурами, на которые возложена ответственность за координацию и поддержку реагирования на события или инциденты в области компьютерной безопасности на национальном уровне. На них лежит национальная ответственность за обеспечение возможностей по выявлению киберугроз, защите от них, реагированию на них и управлению киберугрозами, а также укреплению безопасности киберпространства страны. Эта способность должна быть сопряжена со сбором собственной разведывательной информации, а не реализовываться на основании вторичных сообщений об инцидентах безопасности, поступающих как из окружения CIRT, так и из других источников. Может быть военной или гражданской.			
Злоупотребления в онлайновой среде					Legal1.3.2
Домогательства в онлайновой среде		Сообщения по электронной почте, прямые сообщения или оскорбительные веб-сайты, имеющие целью запугивание или иное преследование отдельного лица или группы лиц посредством персонализированных нападок.	GCIv4		Legal1.3.2
Безопасность в онлайновой среде		Означает 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.	GCIv4		Legal1.3
Лица с особыми потребностями		Особые требования, обусловленные физическими недостатками, трудностями в обучении или поведении и т. д. (особенно в образовательных контекстах).	Оксфордский словарь английского языка	"особые потребности/обладающий особыми потребностями, сущ. и прил.". Онлайновая версия OED. Июнь 2021 года. Oxford University Press. https://www.oed.com/view/Entry/253889?redirectedFrom=special+needs (доступ 30 августа 2021 г.)	

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
Защита персональных данных		Персональные данные – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Защита персональных данных – это процесс обеспечения сохранности персональных данных.	https://gdpr-info.eu/issues/personal-data/ Определение из GDPR	Добровольный стандарт МСЭ-Т X.1058 | ИСО/МЭК 29151 является ценным ориентиром для правительств и отрасли, поскольку они активизируют свои усилия по обеспечению защиты персональных данных. В стандарте X.1058 установлены цели контроля защиты данных, определены необходимые средства контроля и предоставляет руководство по их применению. В нем показано, как механизмы этого контроля могут соответствовать требованиям, определенным в оценках рисков и воздействия организаций, относящихся к защите персональных данных	Legal2.1a
Политика		Меры политики – это правила, принципы, руководящие принципы или структуры, принятые или разработанные организацией или страной для достижения долгосрочных целей. Обычно они определяются в легкодоступном письменном формате. Меры политики формулируются для того, чтобы стимулировать все основные решения, принимаемые в организации, управлять ими и удерживать всю деятельность в установленных границах.	Новый		Org1.1
Послесреднее невысшее образование (уровень 4 МСКО)	Уровень 4 МСКО	Послесреднее невысшее образование обеспечивает опыт обучения на базе среднего образования, подготавливая к выходу на рынок труда, а также к получению высшего образования. Оно направлена на индивидуальное приобретение знаний, навыков и компетенций ниже уровня сложности, характерного для высшего образования. Программы уровня 4 МСКО, или послесреднее	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.4n

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		невысшее образование, обычно предназначены для лиц, завершивших уровень 3 МСКО и имеющих диплом о невысшем образовании, которым оно необходимо для перехода к высшему образованию или для трудоустройства, если их квалификация уровня 3 МСКО не дает такого доступа.			
Начальное образование (МСКО 1)		Программы уровня 1 МСКО, или начального образования, обычно предназначены для того, чтобы дать учащимся фундаментальные навыки чтения, письма и математики (т. е. грамотности и счета) и заложить прочную основу для изучения и понимания основных областей знаний, личностного и социального развития, в рамках подготовки к обучению на первом этапе среднего образования. Оно ориентировано на обучение на базовом уровне сложности с минимальной специализацией, если таковая вообще имеется... Возраст, как правило, является единственным критерием для поступления на этот уровень. Обычный или законный возраст поступления на учебу составляет обычно не ниже пяти и не выше семи лет.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.1
Защита конфиденциальности		Конфиденциальность 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.	GCIv2		Legal2.1b
Государственно-частное партнерство	ГЧП	Долгосрочный контракт между частной стороной и государственной организацией на предоставление государственного актива или услуги, в котором частная сторона несет значительный риск и ответственность за управление, а вознаграждение связано с результатами деятельности.	https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-		

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		ПРИМЕЧАНИЕ. Не имея официального юридического определения, ГЧП часто характеризуется по функциям. Генеральный секретарь ООН предложил две типологии.11 В первой выделяются пять основных функций: a) политический диалог, например целевая группа по информационно-коммуникационным технологиям, Всемирная комиссия по плотинам, Альянс ГАВИ; b) информационно-пропагандистская деятельность, например партнерство ЮНЭЙДС и СМИ для повышения осведомленности о ВИЧ/СПИДе; c) мобилизация частных средств, например Фонд ООН и Фонд международного партнерства, проект иностранных инвестиций Конференции ООН по торговле и развитию и Международной торговой палаты; d) информация и обучение, например, совместные исследовательские и учебные проекты; и e) оперативная деятельность, например, инициатива ООН и LM Ericsson "Первые на местах", проект ООН и Microsoft по регистрации беженцев (Руководящие принципы ООН, 18−32).12 В второй выделяются четыре функции: a) информационно-пропагандистская деятельность, например Глобальный альянс за улучшение питания, Глобальное ГЧП по пропаганде мытья рук с мылом; b) разработка норм и стандартов, например Глобальная инициатива по отчетности, проект "Кто проявляет заботу − выигрывает" по корпоративной ответственности в финансовой отрасли; c) обмен ресурсами и опытом, например логистическая программа Всемирной продовольственной программы и TNT "Приводя мир в движение"; и d) использование рынков для развития, например Инициатива ЮНИФЕМ и L'Occitane по производству масла ши, проект ЮНИДО и FIAT по производству комплектующих для индийских автомобилей (ГА ООН, доклад Генерального секретаря об укреплении сотрудничества между Организацией Объединенных Наций и всеми соответствующими	e1084?rskey=CTIBOr&result=1&prd=MPIL		

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		партнерами, в частности частным сектором [10 августа 2005 г.] 5).13 Руководящие принципы ООН определяют несколько форм сотрудничества и стандартные правовые механизмы, используемые в каждой из них, или просто определяются как: предприятия между государственным и частным секторами. Этот показатель эффективности может измеряться количеством официально признанных национальных или отраслевых ГЧП для обмена информацией о кибербезопасности (сведения об угрозах) и активами (люди, процессы, инструменты) между государственным и частным секторами (т. е. официальные партнерства для сотрудничества или обмена информацией, опытом, технологиями и/или ресурсами) на национальном или международном уровне.			
Нормативное положение		Правило или принцип, регулирующий поведение или практику; в частности, соответствующая директива, которую составляет и ведет какой-либо орган власти.	Оксфордский словарь английского языка	"нормативное положение, сущ. и прил.". Онлайновая версия OED. Июнь 2021 года. Oxford University Press. https://www.oed.com/view/Entry/161427?redirectedFrom=regulation (доступ 30 августа 2021 г.)	Legal2, Legal 2.1, Legal2.2
Исследования и разработки	НИОКР	Исследования и экспериментальные разработки (НИОКР) включают творческую и систематическую работу, проводимую с целью увеличения запаса знаний, в том числе знаний о человечестве, культуре и обществе, и разработки новых способов применения имеющихся знаний. Термин НИОКР охватывает три вида деятельности: фундаментальные научные исследования, прикладные научные исследования и экспериментальные разработки. Для того чтобы деятельность была отнесена к НИОКР, она должна соответствовать пяти основным критериям. Деятельность должна быть: • новаторской (быть направленной на получение новых результатов); • творческой (основываться на оригинальных,	ОЭСР (2015 г.), Руководство Фраскати 2015 года: Руководящие принципы для сбора и представления данных о научно-исследовательских и опытно-конструкторских разработках http://uis.unesco.org/en/glossary-term/research-and-experimentaldevelopment-rd		CapDev4.1; CapDev4.1.1; CapDev4.1.2; CapDev4.1.3

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		не очевидных концепциях и гипотезах); • неопределенной (быть неопределенной в отношении конечного результата); • систематической (быть спланированной и заложенной в бюджет); • передаваемой и/или воспроизводимой (приводить к результатам, которые могут быть воспроизведены).			
Среднее образование (2 и 3 МСКО)	МСКО 2 и 3	Программы уровня 2 МСКО, или первого этапа среднего образования, как правило, разработаны на основе результатов обучения уровня 1 МСКО. Обычно цель состоит в том, чтобы заложить основу для обучения на протяжении всей жизни и развития человека, на основе которой системы образования могут затем расширять дальнейшие образовательные возможности. Некоторые системы образования уже могут предлагать программы профессионального образования на уровне 2 МСКО, чтобы дать людям навыки, необходимые для трудоустройства. Программы уровня 3 МСКО, или второй этап среднего образования, обычно предназначены для завершения среднего образования в рамках подготовки к высшему образованию или для получения навыков, необходимых для трудоустройства, либо для того и другого. Уровень 3 МСКО начинается после 8–11 лет обучения с начала уровня 1 МСКО.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.2
Высшее образование (уровни 5–8 МСКО)	Уровни 5–8 МСКО	Программы уровня 5 МСКО, или высшее образование короткого цикла, часто предназначены для предоставления участникам профессиональных знаний, навыков и компетенций. Как правило, они основаны на практических знаниях, касаются конкретной профессиональной сферы и готовят учащихся к выходу на рынок труда. Однако эти программы могут также проложить путь к другим программам высшего образования... Программы уровня 6 МСКО, бакалавриата или эквивалентного уровня, часто предназначены для предоставления участникам	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.3

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		промежуточных академических и/или профессиональных знаний, навыков и компетенций, ведущих к получению диплома первой степени или эквивалентной квалификации. Программы уровня 7 МСКО, магистратуры или эквивалентного уровня, часто предназначены для предоставления участникам расширенных академических и/или профессиональных знаний, навыков и компетенций, ведущих к получению диплома второй степени или эквивалентной квалификации. Программы уровня 8 МСКО, докторантура или эквивалентный уровень, предназначены в первую очередь для получения продвинутой научной степени. Программы этого уровня МСКО посвящены углубленному изучению и оригинальным научным исследованиям и обычно предлагаются только ориентированными на научные исследования высшими учебными заведениями, такими как университеты. Программы докторантуры существуют как в академических, так и в профессиональных областях...			
Ксенофобский		Неприязнь или предрассудки по отношению к людям, культурам и обычаям, которые являются иностранными или воспринимаются как иностранные.	Оксфордский словарь английского языка	"ксенофобия, сущ.". Онлайновая версия OED. Июнь 2021 года. Oxford University Press. https://www.oed.com/view/Entry/230996?redirectedFrom=xenophobia (доступ 30 августа 2021 г.)	Legal1.3.1
Национальные инициативы		Деятельность, осуществляемая на национальном уровне для систематического решения конкретной проблемы.	GCIv2	Страновые инициативы обычно разрабатываются для решения конкретной задачи, стоящей перед организацией. Примерами могут служить права человека, образование или окружающая среда. Это могут быть цели или задачи, назначенные одному или нескольким членам через	

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
				интерфейс "создать проект"	
Подлог, связанный с применением компьютеров		Подлог, связанный с применением компьютеров, подразумевает выдачу себя за правомочных лиц, представителей органов власти, ведомств и других организаций в онлайновой среде в мошеннических целях.	https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html#:~:text=Computer%2Drelated%20forgery%20involves%20impersonation,entities%20online%20for%20fraudulent%20purposes		Legal1.2
Незапрашиваемые сообщения, или спам		Электронное сообщение, такое как письмо по электронной почте, SMS, сообщение в социальных сетях или телефонные звонки, не запрашиваемые их получателем. Спам относится к таким незапрашиваемым сообщениям, рассылаемым в массовом порядке.	GCIv2		Legal2.7
Цифровая подпись		Цифровая подпись – это математический метод, используемый для подтверждения подлинности и целостности сообщения, программного обеспечения или цифрового документа.	GCIv2		Legal2.6
Электронная транзакция		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.	GCIv2		
Стандарты кибербезопасности		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		Определение GCIv4 и GCIv2	Legal2.5

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		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, ЕТСИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др. Нормативные 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: ИСО, МСЭ, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ЕТСИ, ISF, RFC, ISA, МЭК, NERC, NIST, FIPS, PCI DSS и др.			
Практические занятия по кибербезопасности (например, тренировочные занятия по кибербезопасности)		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.	GCIv4		Tech1.2.2
Тренировочное занятие по кибербезопасности		Тренировочное занятие по кибербезопасности – это ежегодное мероприятие, в ходе которого выполняется моделирование кибератак, инцидентов информационной безопасности и нарушений других типов, для того чтобы проверить возможности организации в области кибербезопасности: от способности обнаружить инцидент в области безопасности до способности надлежащим образом реагировать на него и минимизировать любое связанное с ним воздействие. Участники тренировочного занятия по кибербезопасности могут проверять стратегии, планы, процедуры, процессы и возможности, обеспечивающие подготовку, предотвращение,	Определение МСЭ	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx	Tech1.2.2

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		реагирование, восстановление и непрерывность деятельности.			
Информационные бюллетени по кибербезопасности		Информационные бюллетени CIRT – донесение до сведения широкой общественности информации о возникающих киберугрозах и рекомендуемых действиях.	GCIv4		Tech1.2.3
Присоединение к FIRST		Статус полноправного или ответственного за взаимодействие члена Форума групп реагирования на инциденты и обеспечения безопасности (www.first.org).	GCIv4		Tech1.3
Присоединение к региональным CIRT/CERT/CSIRT		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.	GCIv4		Tech1.4
Отраслевые CERT/CIRT/CSIRT		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.	GCIv2		Tech2.1
Международное сотрудничество в области кибербезопасности		Сотрудничество между двумя или более правительствами, национальными ведомствами, национальными регуляторными органами, национальными CIRT, организациями гражданского общества или академическими организациями.			Org1.8
Механизмы и возможности отчетности		Такие как национальные линии помощи и горячие линии, подключенные к международной системе линий помощи. Они должны быть связаны с системами получения советов и поддержки.			Org4.3
Кампании по повышению осведомленности населения в области кибербезопасности		Повышение осведомленности населения предусматривает содействие проведению кампаний, охватывающих максимально возможное количество человек, а также использование НПО, учреждений,	GCIv4		CapDev1.

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		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.			
Центр обеспечения безопасности	SOC	SOC представляет собой организационное подразделение, функционирующее в центре всех операций по обеспечению безопасности. Обычно оно рассматривается не как отдельный субъект или система, а как сложная структура для управления общей безопасностью организации и ее повышения. Его функция заключается в обнаружении, анализе угроз и инцидентов в сфере кибербезопасности, а также реагировании на такие угрозы и инциденты с использованием людей, процессов и технологий. Эти виды деятельности могут быть формализованы в семь показателей, или функциональных областей SOC. Несмотря на широкое признание того, что SOC имеют огромное значение для безопасности компаний, они все еще считаются пассивным и реактивным механизмом защиты". "Группа реагирования на инциденты в сфере компьютерной безопасности: этот термин часто используется как взаимозаменяемый для обозначения SOC, хотя в нем основной акцент делается на мерах реагирования после того, как произошла атака. CSIRT представляет собой организационное подразделение, ответственное за координацию и поддержку реагирования на инцидент в сфере компьютерной безопасности. CSIRT классифицируется либо как независимая группа, либо как часть SOC".	https://ieeexplore.ieee.org/document/9296846		

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		"Центр управления сетью: Центр управления сетью (Network Operations Center, NOC) контролирует выявление, расследование, определение приоритетов, эскалацию и решение проблем. Однако проблемы, решаемые в NOC, отличаются, поскольку деятельность NOC главным образом направлена на инциденты, влияющие на производительность и доступность сети организации. Инциденты могут происходить во всех системах, а не только в сетях, поэтому организациям выгодно, когда группы NOC и SOC работают вместе. "Центр аналитически данных в области безопасности: Термин "Центр аналитически данных в области безопасности" (Security Intelligence Center, SIC) был впервые использован в 2017 году для описания преемника SOC. Он призвана обеспечить более целостное и комплексное представление, чем SOC, и может обеспечить полное визуальное представление аналитических данных по безопасности, а также управление ими в одном месте. Таким образом, используется сочетание нескольких технологий (например, информационная безопасность (ИБ), управление знаниями, обработка больших данных)". "Управление информацией о безопасности и администрирование событий: SIEM является неотъемлемой частью многих SOC, покрывая значительную часть технологических требований. Оно отвечает за централизованный сбор данных, имеющих отношение к безопасности. Таким образом, оно обеспечивает возможности анализа в сфере безопасности путем корреляции зарегистрированных уведомлений о событиях. Дополнительные функциональные возможности позволяют обогащать контекстные данные, нормализовать разнородные данные, формировать отчеты и предупреждения [73]. Чтобы обеспечить обмен информацией			

Термин	Аббре-виатура	Определение	Источник	Примеры	Вопросы, на которые даны ссылки (GCIv4)
		об угрозах, SIEM обеспечивает связь с платформами обмена данными о киберугрозах, а также включает работу аналитиков в сфере безопасности, предлагая возможности в области визуального анализа в сфере безопасности. SIEM включает в себя возможности управления зарегистрированными событиями за счет длительного хранения данных о событиях".			