|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Logo  Description automatically generated** | **Региональное подготовительное собрание к ВКРЭ-21 для стран СНГ (РПС-СНГ) виртуальное, 21-22 апреля 2021 года** | | | A close up of a sign  Description automatically generated |
|  | | |  | |
|  | | **Документ** **RPM-CIS21/INF/5-R** | | |
|  | | **7 апреля 2021 г.** | | |
|  | | **Только на русском** | | |
| Директор Бюро развития электросвязи | | | | |
| ИССЛЕДОВАНИЕ МСЭ-D ПОТЕНЦИАЛЬНЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ  РЕГИОНА СНГ В ПЕРИОД 2022-2025 - КИБЕРБЕЗОПАСНОСТЬ | | | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отчет

**«Исследование МСЭ-D потенциальных направлений развития региона СНГ в период 2022-2025.**

**Направление - Кибербезопасность»**

*Версия 1.0*

*7 апреля 2021*

*Версия для публикации*

**Содержание**

[Введение 4](#_Toc68701624)

[1 Тенденции в области спама и вредоносного программного обеспечения, включая меры по смягчению их воздействия 5](#_Toc68701625)

[1.1Положение дел в области спама и вредоносного программного обеспечения 5](#_Toc68701626)

[1.2Спам и вредоносное программное обеспечение: статистика, тенденции, развитие и воздействие на сети электросвязи 6](#_Toc68701627)

[1.3Методы, применяемые для борьбы со спамом и вредоносным программным обеспечением и снижения их воздействия 6](#_Toc68701628)

[2 Тенденции в совершенствовании средств кибербезопасности на национальном уровне: повышение осведомленности и создание потенциала 8](#_Toc68701629)

[2.1Создание соответствующих национальных органов по вопросам кибербезопасности 8](#_Toc68701630)

[2.2Группы реагирования на нарушение компьютерной защиты (CERT)/группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/группы реагирования на компьютерные инциденты (CIRT) 11](#_Toc68701631)

[2.3Кампании, направленные на повышение осведомленности 12](#_Toc68701632)

[2.4Системы управления рисками в области кибербезопасности 14](#_Toc68701633)

[2.5Государственно-частное партнерство 16](#_Toc68701634)

[2.6Меры/инициативы по усилению потенциала 18](#_Toc68701635)

[3 Вызовы в области кибербезопасности, которые стоят на пути новых технологий, таких как интернет вещей и облачные вычисления 18](#_Toc68701636)

[3.1Введение 18](#_Toc68701637)

[3.2Угрозы кибербезопасности, ее субъекты и их мотивы 20](#_Toc68701638)

[3.3Существующие и появляющиеся решения 29](#_Toc68701639)

[4 Как кибербезопасность может способствовать защите персональных данных 34](#_Toc68701640)

[4.1Введение 34](#_Toc68701641)

[4.2Правовая база и передовой опыт Государств-Членов 35](#_Toc68701642)

[4.3Извлеченные уроки и дальнейшие действия 39](#_Toc68701643)

[5 Глобальный индекс кибербезопасности МСЭ (v3): обзор по региону СНГ 40](#_Toc68701644)

[5.1Обзор 40](#_Toc68701645)

[5.2Сравнение в региональном разрезе 40](#_Toc68701646)

[6 Предложения по работе по направлению кибербезопасности в регионе СНГ и потенциальные партнеры 49](#_Toc68701647)

[6.1Мандат МСЭ 49](#_Toc68701648)

[6.2Создание и усовершенствование национальных Групп реагирования на инциденты в области кибербезопасности (CIRT) 49](#_Toc68701649)

[6.3Учения по кибербезопасности 50](#_Toc68701650)

[6.4Целевые региональные и национальные тренинги 51](#_Toc68701651)

[6.5Глобальный индекс кибербезопасности 51](#_Toc68701652)

[6.6Обмен опытом по национальным стратегиям кибербезопасности 52](#_Toc68701653)

Введение

Для содействия подготовки к следующей Всемирной конференции по развитию электросвязи (ВКРЭ-21) в 2021 году Региональное отделение МСЭ для региона СНГ проводит исследование потенциальных приоритетных областей, которые наиболее часто запрашивались Государствами-Членами в последние годы. В настоящем отчете представлены результаты исследования потенциальных приоритетных областей направления «Кибербезопасность», которые будут направлять программную деятельность МСЭ-D в цикле работы 2022–2025 годов.

С учетом чувствительности темы для многих Государств-Членов МСЭ, а также различиях в позициях при ее обсуждении на площадке МСЭ, в настоящем отчете используется только текст и данные, которые уже ранее уже представлялись и обсуждались на собраниях МСЭ, а именно:

* Документы, описывающие глобальную деятельность МСЭ по направлению кибербезопасности
* Документы Исследовательских комиссий МСЭ-D
* Публикация МСЭ-D «Глобальный индекс кибербезопасности (3 версия, редакция 2018 года)»
* Спам и вредоносное программное обеспечение, а также меры по смягчению их воздействия
* Совершенствование национальных средств кибербезопасности путем повышения осведомленности и создания потенциала
* Проблемы в области кибербезопасности, связанные с появляющимися технологиями, такими как интернет вещей (IoT) и облачные вычисления
* Как кибербезопасность может способствовать защите персональных данных

В **Разделах 1-4** также приведены лучшие практики по каждой из рассматриваемых областей.

В **Разделе 5** выполнен обзор уровня вовлеченности стран региона СНГ в решение вопросов кибербезопасности на национальном уровне в соответствии с публикацией МСЭ-D «Глобальный индекс кибербезопасности (3 версия, редакция 2018 года)». В апреле 2021 года ожидается публикация 4 версии Глобального индекса кибербезопасности, настоящий документ будет обновлен в соответствии с этой публикацией.

В **Разделе 5** также приведены наиболее интересные практики как стран региона, так и стран, с которыми у региона СНГ налажено активное сотрудничество и обмен опытом.

В **Разделе 6** представлены предложения по работе по направлению кибербезопасности в цикле реализации 2022-2025 гг. Предложения подготовлены на основе сопоставления направлений деятельности МСЭ (предложение) и запросов Государств-Членов МСЭ, полученных Региональным отделением МСЭ (спрос).

1. Тенденции в области спама и вредоносного программного обеспечения, включая меры по смягчению их воздействия

## Положение дел в области спама и вредоносного программного обеспечения

Несмотря на отсутствие какого-либо общепринятого определения в большинстве случаев под термином спам имеют в виду незатребованные массовые электронные сообщения, передаваемые по электронной почте или в виде текстовых сообщений с помощью компьютера или мобильного телефона[[1]](#footnote-1). Потребители обычно сталкиваются со спамом в виде рекламы, в том числе "мусора" или нежелательных рекламных сообщений электронной почты, текстовых сообщений и контактов в социальных сетях.

Хотя спам, как правило, предполагает поиск потенциальных клиентов в коммерческих целях, он может также преследовать преступные цели, включая фишинг, используя аналогичные данные, генерируемые пользователем. Выдавая себя за доверенные третьи лица, злоумышленники используют фишинговые сообщения электронной почты, с тем чтобы побудить адресатов раскрыть свои персональные данные (учетные записи доступа, пароли и т. д.) и/или банковские данные.

Спам создает риски для безопасности подключенных пользователей и организаций, и это связано не только с тем, что он легко распространяется через интернет и службы электронной связи (электронная почта, веб-сайты, социальные сети, SMS и MMS), но и с тем, что он может нести в себе вредоносное программное обеспечение. Страны внедряют различные технические и регуляторные механизмы для борьбы со спамом, и это дает определенные результаты.

Вредоносное программное обеспечение, в свою очередь, переживает значительный бум в последнее время благодаря развитию интернета, в частности мобильного интернета. Вредоносное программное обеспечение – это общий термин для программного обеспечения, предназначенного специально для нанесения вреда компьютерам или компьютерным системам[[2]](#footnote-2).

Кроме того, расширение возможностей для установления соединений, появление новых технологий и рост числа пользователей открыли новые возможности для создания и использования вредоносного программного обеспечения. Такая парадигма усложняет обеспечение кибербезопасности, обнажая проблематичные места и расширяя область атаки, подверженную угрозам, исходящим от вредоносного программного обеспечения. В дополнение к традиционным вредоносным программам (вирусам, червям, троянам, программам-шпионам и программам, содержащим рекламу, спаму, руткитам и т. д.) появились новые, более изощренные виды вредоносного программного обеспечения, как, например, бот-сети, программы-вымогатели и мобильные вредоносные программы.

Иными словами, борьба со спамом и вредоносным программным обеспечением имеет жизненно важное значение для безопасности пользователей и развития предприятий.

## Спам и вредоносное программное обеспечение: статистика, тенденции, развитие и воздействие на сети электросвязи

По состоянию на март 2020 года доля спама в мировом трафике сообщений электронной почты составляла 53,95%[[3]](#footnote-3). В последние годы этот показатель значительно снизился – с 69% в 2012 году до 55% в 2018 году, что, вероятно, обусловлено повышением уровня осведомленности о кибербезопасности и технологическим прогрессом. Большая часть спама, приходящего в адрес пользователей, носит рекламный характер, включая характер маркетинговой информации. Согласно результатам одной из оценок, спам обходится предприятиям почти в 20,5 миллиардов долларов США в год в виде потери производительности и технических расходов. Предполагается, что эта сумма может вырасти до 257 миллиардов долларов США в год, если спам продолжит расти текущими темпами[[4]](#footnote-4).

По одной из оценок, на различные аферы и мошенничество приходится около 2,5% всего спама, при этом значительная часть таких операций (92%) может иметь вредоносный характер, т. е. может быть связанной с использованием вредоносного программного обеспечения для причинения вреда пользователям или нарушения безопасности их ИТ-систем в тех или иных целях[[5]](#footnote-5). Согласно другой оценке, в 2018 году было выявлено около 812,67 миллионов различных случаев заражения вредоносным программным обеспечением[[6]](#footnote-6). Доля вредоносных программ для мобильных устройств увеличилась на 54%, а программ-вымогателей – на 350%; при этом ежегодные финансовые потери, связанные с заражением программами-вымогателями, оцениваются в 6 миллиардов долларов США (до 2021 года).

Поскольку спам и вредоносное программное обеспечение могут генерировать значительный трафик, они могут оказывать существенное негативное воздействие на инфраструктуру и операторов сетей и, следовательно, на пользовательский опыт потребителей. Кроме того, вызванные спамом проблемы, включая обусловленные ими проблемы в работе сетей, могут нанести ущерб репутации операторов.

Для решения таких проблем, включая потенциально массивные потоки нежелательного трафика, и обеспечения качества сети операторам может потребоваться разработать новые инструменты, в том числе инвестировать в защиту и расширение существующей инфраструктуры. Так, поставщики услуг могли бы инвестировать в антиспамовые фильтры для повышения качества предлагаемых ими услуг. В результате у операторов и поставщиков услуг электронной связи могут возникнуть дополнительные затраты.

## Методы, применяемые для борьбы со спамом и вредоносным программным обеспечением и снижения их воздействия

**Технические методы борьбы со спамом и вредоносным программным обеспечением и снижения их воздействия.**

Незатребованные сообщения электронной почты – это один из основных каналов передачи вредоносного программного обеспечения. Для эффективной борьбы со спамом и вредоносными программами необходимо разорвать цепочку передачи. По мере развития технологий такие инструменты, как антиспамовые фильтры и антивирусное программное обеспечение, остаются эффективными механизмами для борьбы со спамом и вредоносными программами. Эффективность таких инструментов можно повысить, если использовать их вместе с новыми технологиями, такими как искусственный интеллект. Учитывая это, один из методов надлежащей практики для пользователей предполагает регулярное обновление антиспамовых фильтров и антивирусного программного обеспечения.

Кроме того, для сокращения таких цепочек передачи поставщики услуг могут прибегнуть к применению соответствующей политики, как, например, в отношении инфраструктуры политики отправителя, идентификации почты с использованием доменных ключей, [аутентификации сообщений, создания отчетов и определения соответствия по доменному наименованию](https://tools.ietf.org/html/rfc7489), а также к внесению в списки блокировки в режиме реального времени[[7]](#footnote-7).

Операторы сетей электронной связи и поставщики услуг интернета также могут принимать определенные меры для решения проблем, связанных с блокировкой IP-адресов. Одним из примеров таких мер является применение протокола безопасности граничных шлюзов с использованием инфраструктуры открытых ключей ресурсов[[8]](#footnote-8).К числу других инициатив относятся:

* Взаимосогласованные нормы безопасности маршрутизации, предназначенные для совместного предотвращения перехвата маршрутов, подмены IP-адресов и других вредоносных действий на основе новейших технологий, которые могут привести к распределенным атакам типа "отказ в обслуживании" (DDoS), перехвату информации, потере доходов, нанесению вреда репутации и т. д.[[9]](#footnote-9);
* Рабочая группа по борьбе со злоупотреблениями рассылкой сообщений, вредоносным ПО и мобильной связью, регулярно публикующая примеры передового опыта борьбы со злонамеренными сообщениями, всеми типами вредоносных программ (включая бот-сети), спамом, вирусами, атаками типа "отказ в обслуживании" (DoS) и любыми другими видами злоупотреблений в сети[[10]](#footnote-10).

Среди других инициатив, направленных на борьбу со спамом и вредоносным программным обеспечением, – Общество Интернета[[11]](#footnote-11), Ассоциация глобальной системы подвижной связи[[12]](#footnote-12), проект Spamhaus[[13]](#footnote-13), Рабочая группа по борьбе с фишингом[[14]](#footnote-14) и Коалиция против шпионского ПО[[15]](#footnote-15).

**Регуляторные подходы к борьбе со спамом и вредоносным программным обеспечением и снижению их воздействия.**

Учитывая проблемы и затраты, с которыми сопряжена борьба со спамом и вредоносным программным обеспечением, в последние годы некоторые регионы и страны приняли новую или укрепили существующую законодательную базу, с тем чтобы обеспечить наличие инструментов для активизации борьбы с такими атаками. При разработке законодательства и политики страны руководствуются внутренними требованиями, такими как Общий регламент Европейского союза по защите данных, согласно которому для сбора данных необходимо получить согласие соответствующего пользователя.

Еще одним примером является Конвенция Африканского союза о кибербезопасности и защите личных данных (Конвенция Малабо), согласно которой государствам-участникам в Африканском регионе рекомендуется включить предлагаемый комплекс стандартов в национальное законодательство. Статья 4.3 Конвенции гласит, что "на территории государств-участников запрещается осуществление прямого маркетинга на основе любых форм связи с использованием в какой бы то ни было форме сведений о лице, не предоставившем предварительного согласия на получение услуг или продуктов упомянутого прямого маркетинга с помощью таких средств". Тем не менее Конвенция разрешает осуществлять прямой маркетинг при определенных условиях. В частности, "прямой маркетинг с помощью электронной почты разрешается при условии, что: a) сведения об адресате были получены непосредственно от него (нее); b) получатель дал согласие на то, чтобы с ним связались маркетинговые партнеры; iii) прямой маркетинг касается аналогичных продуктов или услуг, предоставляемых одним и тем же физическим или юридическим лицом" (п. 4.4).

По мере внедрения как Общего регламента Европейского союза по защите данных, так и Конвенции Малабо можно будет оценить и определить всю полноту их воздействия на снижение масштабов спама и использования вредоносного программного обеспечения.

# **Тенденции в** **совершенствовании средств кибербезопасности на национальном уровне: повышение осведомленности и создание потенциала**

На протяжении последних лет ИКТ переживают стремительное развитие и внедрение инновационных решений. Во всем мире они играют важную роль, позволяя странам расширять свою цифровую экономику и поддерживать социальное процветание. Кроме того, как показала пандемия COVID-19, в своей повседневной жизни люди все больше зависят от ИКТ. Учитывая такие реалии, странам крайне необходимо не сворачивать принятие значимых мер, направленных на совершенствование и повышение качества средств кибербезопасности на национальном уровне для защиты от связанных с ней рисков и преодоления соответствующих вызовов.

В настоящей главе рассматриваются ключевые направления деятельности по совершенствованию средств кибербезопасности на национальном уровне, в том числе:

* создание соответствующих национальных органов по вопросам кибербезопасности;
* группы реагирования на нарушение компьютерной защиты (CERT)/группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/группы реагирования на компьютерные инциденты (CIRT);
* кампании, направленные на повышение осведомленности в области кибербезопасности;
* системы управления рисками в области кибербезопасности;
* государственно-частное партнерство;
* прочие инициативы по созданию потенциала.

## Создание соответствующих национальных органов по вопросам кибербезопасности

Появление новых достижений и инновационных решений в секторе ИКТ происходит на фоне усугубления рисков и вызовов в области кибербезопасности. Для преодоления таких вызовов правительствам необходимо непрерывно осуществлять оценку и доработку существующих на национальном уровне средств и стратегий в области кибербезопасности, в том числе создавая соответствующие национальные органы по вопросам кибербезопасности. В течение исследовательского периода Государства-Члены рассказали о своих подходах к созданию таких органов. В разных странах применяются разные подходы, что обусловлено внутренними структурами управления, правилами, положениями и политикой.

Органы, занимающиеся вопросами кибербезопасности, обладают разным опытом и специализацией, однако, как правило, выполняют одни и те же ключевые функции, включая разработку и координацию внедрения регуляторной политики, разработку и проведение кампаний, направленных на повышение уровня осведомленности о кибербезопасности, предоставление пользователям (от крупных организаций до отдельных лиц и малых предприятий) актуальной информации, а также подготовку заявлений и руководящих указаний по инцидентам в области кибербезопасности. Учитывая весь спектр вопросов, подпадающих под сферу кибербезопасности, правительствам крайне важно создать условия, необходимые для координации действий и поддержания сотрудничества между различными органами и структурами, а также между государственным и частным секторами.

Например, Национальный центр кибербезопасности Соединенного Королевства сотрудничает с другими компетентными государственными органами и руководит усилиями, направленными на обеспечение ощутимого снижения воздействия, вызванного атаками с помощью программ-вымогателей[[16]](#footnote-16). В случае возникновения такой атаки организациям рекомендуется обращаться в Национальное агентство по борьбе с преступностью, сертифицированную компанию по реагированию на киберинциденты или инициативу "Партнерство по обмену информацией в области кибербезопасности". Национальный центр кибербезопасности в сотрудничестве с Национальным агентством по борьбе с преступностью руководил усилиями, пред принимавшимися в Соединенном Королевстве в ответ на атаку с использованием программы-вымогателя WannaCry. При возникновении каждого инцидента центр публикует заявления и руководящие указания как для крупных организаций, так и для домашних пользователей и малых предприятий. Наиболее актуальная информация также размещается на странице учетной записи центра в Twitter (@NCSC).

Бразилия представила общую информацию о своей Национальной стратегии в области кибербезопасности (E-Ciber), которая была ратифицирована президентом Бразилии и опубликована в феврале 2020 года[[17]](#footnote-17). При разработке этой прогрессивной стратегии, представляющей собой внедряемую федеральным правительством концепцию кибербезопасности на период 2020‑2023 годов, Бразилия применила исчерпывающий и всеобъемлющий подход с привлечением многочисленных заинтересованных сторон, в том числе представителей правительства, частного сектора и академических организаций. Ратифицировав E-Ciber, Бразилия дополнила законодательную базу ранее отсутствовавшим компонентом. В соответствии с E-Ciber Бразилия определила 10 стратегических направлений, наметив в каждом из них определенные меры и инициативы. К таким направлениям, в частности, относятся следующие:

* усиление управления деятельностью в сфере кибербезопасности;
* внедрение модели централизованного управления национальной кибербезопасностью;
* доработка национальной правовой базы в сфере кибербезопасности;
* расширение международного сотрудничества Бразилии в области кибербезопасности.

Еще одним примером является Бенин, рассказавший о различных государственных структурах, участвующих в управлении ИКТ в стране[[18]](#footnote-18). Агентство по информационным услугам и системам (ASSI), бывшее Бенинское агентство по информационно-коммуникационным технологиям (ABETIC), – это национальный орган, отвечающий за практическую реализацию программ и разработку стратегий развития защищенных цифровых информационных систем и услуг в Бенине. В сферу его ответственности входит ряд ключевых направлений деятельности, в том числе:

* реализация ключевых проектов в области "умного" управления и электронной коммерции;
* разработка, обновление и практическая реализация генеральных планов национальных информационных систем;
* обеспечение технической, прикладной и финансовой согласованности национальных информационных систем и услуг;
* обеспечение хостинга и контроля важнейших данных и информации государства и операторов важнейшей инфраструктуры, а также безопасного доступа к таким данным и информации.

В Чаде Национальное управление информационной безопасности и электронной сертификации (ANSICE), созданное в феврале 2015 года, подчиняется непосредственно администрации президента[[19]](#footnote-19). Управление функционирует с января 2018 года и обладает широкими полномочиями и компетенцией, в том числе в области обеспечения безопасности информационных систем и сетей по всей стране.

Соединенное Королевство также представило информацию об обновленном исследовании внедрения надлежащей практики обеспечения безопасности устройств IoT пользователей. В частности:

* был опубликован Свод правил и норм по обеспечению безопасности пользователей IoT, в котором изложены 13 общих принципов (доступен также на немецком, испанском, французском, японском, корейском, китайском и португальском языках);
* были проведены общественные консультации по предлагаемым нормативным и законодательным актам;
* было поддержано внедрение первого всемирно применимого стандарта безопасности в области интернета вещей ETSI EN 303 645, который был опубликован Европейским институтом стандартизации в области электросвязи (ETSI). Многие организации уже внедрили данный и предшествовавший ему стандарт, ETSI TS 103 645, при производстве своей продукции и организации механизмов сертификации;
* заинтересованным сторонам было предложено представить свое мнение о регуляторных предложениях Соединенного Королевства в отношении сферы применения, обязательств, требований безопасности и подхода к обеспечению соблюдения;
* Министерству цифровых технологий, культуры, средств массовой информации и спорта и Национальному центру кибербезопасности было поручено совместно разработать руководящие указания и онлайновые вебинары для производителей продукции в области IoT, которые неоднократно проводились с учетом различных часовых поясов;
* было обеспечено обновление ситуационной карты с нанесением на нее существующих стандартов, а также было оказано содействие организациям во внедрении надлежащей практики во всех сферах IoT[[20]](#footnote-20).

## Группы реагирования на нарушение компьютерной защиты (CERT)/группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/группы реагирования на компьютерные инциденты (CIRT)

Национальный потенциал для реагирования на инциденты (в виде CERT/CSIRT/CIRT) – это ключевой инструмент для решения оперативных задач в области кибербезопасности. Он способствует координации действий, направленных на сбор и обработку информации, касающейся кибербезопасности, а также на принятие мер реагирования на инциденты в области безопасности. В течение исследовательского периода исследовательская комиссия получила ключевые вклады по данной теме от Государств-Членов и Членов Секторов МСЭ, при этом многие них высказали единое мнение о том, что национальные группы CERT/CSIRT/CIRT должны выполнять функцию основного контактного центра по вопросам кибербезопасности и координационного центра по реагированию на возникающие инциденты.

Так в апреле 2016 года была учреждена Бутанская группа реагирования на компьютерные инциденты (BtCIRT) для усиления кибербезопасности в стране путем содействия координации действий, направленных на сбор и обработку информации, касающейся кибербезопасности, и создания национального потенциала для борьбы с инцидентами в области компьютерной безопасности[[21]](#footnote-21). BtCIRT является подразделением, действующем при Департаменте информационных технологий и электросвязи Министерства информации и связи. В соответствии со своим мандатом BtCIRT выступает в качестве национального контактного центра по вопросам кибербезопасности и представляет страну на международных форумах. Передача одной организации функции по координации всех инициатив в области кибербезопасности позволяет предотвратить дублирование предпринимаемых мер и достигаемых результатов. Поскольку большинство международных форумов и групп, занимающихся вопросами кибербезопасности, взаимодействуют с группами CIRT, уполномоченными осуществлять деятельность на национальном уровне, правительствам необходимо определить CIRT или назначить одну организацию, которая будет руководить реализацией национальных инициатив и планов в области кибербезопасности.

Несмотря на то, что BtCIRT была создана как контактный центр по вопросам кибербезопасности в Бутане, ей было нелегко завоевать доверие заинтересованных сторон, главным образом вследствие того, что она была относительно новым органом и имела ограниченные технические возможности. Кроме того, крупные корпорации, такие как операторы электросвязи и банки, уже обладают надежной инфраструктурой ИКТ и необходимыми техническими возможностями, что затрудняет сотрудничество между ними и правительством. Сотрудничество и взаимодействие между заинтересованными сторонами, особенно поставщиками услуг интернета и CIRT, необходимо для поиска и внедрения согласованных решений по безопасности пользователей интернета. Бутан обратился к международным организациям с просьбой оказать помощь в наращивании жизненно необходимого технического потенциала BtCIRT.

Наконец, литовская компания NRD Cyber Security предложила, чтобы национальные и отраслевые группы CSIRT не только выступали в качестве основного контактного центра по инцидентам в области кибербезопасности, но и координировали реагирование на них, а также способствовали созданию и стимулировали формирование в стране дополнительного независимого и распределенного потенциала для противодействия киберугрозам[[22]](#footnote-22).

## Кампании, направленные на повышение осведомленности

В мире наблюдается широкое использование ИКТ со стороны различных заинтересованных сторон – от правительств и коммерческих организаций до организаций местного уровня и отдельных граждан. Однако многие пользователи не в полной мере осознают сопряженные с этим риски с точки зрения кибербезопасности. Для некоторых развивающихся стран недостаточный уровень осведомленности пользователей является наиболее труднопреодолимым вызовом. Во вкладах, полученных в течение исследовательского периода, прослеживается общее понимание того, что кампании по повышению осведомленности о кибербезопасности играют важную роль в преодолении таких вызовов. Основная цель таких кампаний заключается в том, чтобы стимулировать внедрение моделей безопасного поведения в онлайновой среде.

Страны и предприятия стремятся найти креативные пути разработки эффективных кампаний, в том числе для охвата широкого круга пользователей.

Так, Мексика поделилась своим опытом разработки и проведения обследования среди пользователей интернета, который можно взять за основу для внедрения различных подходов к проведению кампаний по повышению осведомленности о кибербезопасности[[23]](#footnote-23).

В некоторых странах провели обследования, с тем чтобы выявить основные проблемы граждан и на основе полученных результатов разработать кампании по повышению осведомленности. Опираясь на свой опыт, Мексика также представила следующие извлеченные уроки:

* установите и обновите антивирусную защиту;
* регулярно меняйте пароли и следите за тем, чтобы они были надежными (т. е. используйте комбинацию цифр, букв и специальных символов);
* регулярно создавайте резервные копии данных;
* подключайтесь только к защищенным общественным сетям.

Еще один пример представил Бутан, где BtCIRT разработала программы повышения осведомленности, направленные на удовлетворение потребностей в области кибербезопасности, возникающих в связи с повседневной профессиональной и персональной деятельностью конечных пользователей по стране в целом[[24]](#footnote-24). Участникам было показано, как осуществляют атаки мошенники, использующие социальную инженерию и фишинг, как безопасно общаться с помощью электронной почты и в социальных сетях и каковы общие угрозы и меры, направленные на их устранение. Разработанные Бутаном программы повышения осведомленности оказались весьма успешными в плане информирования пользователей о рисках в области безопасности и получили положительные отзывы. В настоящее время в центре внимания BtCIRT находятся государственные служащие, однако группа надеется расширить свою целевую аудиторию, включив в нее детей и пользователей, представляющих уязвимые группы населения.

Еще один пример креативного подхода, приведенный Бутаном, – учреждение ежегодного национального конкурса веб-сайтов, организованного Департаментом информационных технологий и электросвязи Министерства информации и связи[[25]](#footnote-25). Участие в конкурсе принимают все государственные веб-сайты, лучший из которых определяется по следующим основным критериям:

* практичность и надежность;
* контент и актуальность;
* безопасность и время безотказной работы;
* внешний вид;
* интерактивный дизайн.

Аналогичным образом в ноябре 2019 года Бразилия в лице Национального агентства электросвязи (ANATEL) приступила к реализации кампании по повышению уровня осведомленности в области кибербезопасности под названием "Safe Connection" (#ConexãoSegura)[[26]](#footnote-26). В рамках кампании потребителям были даны рекомендации по защите персональных данных и созданию безопасных паролей. Кампания была разработана в ответ на жалобы потребителей о попытках мошенничества, а также с тем чтобы развеять сомнения относительно того, как защитить персональные данные. С началом пандемии COVID-19 и резким увеличением числа новых афер в помощь пользователям были созданы новые посты о мошенничестве и махинациях в связи коронавирусом. Они были размещены в социальных сетях Anatel, включая Facebook, Twitter, Instagram и LinkedIn. Ниже приведены некоторые примеры передового опыта, использованного в ходе кампании:

* используйте все возможности для обеспечения безопасности, предоставляемые мобильными приложениями, как, например двухфакторная аутентификация;
* создавайте надежные и безопасные пароли, комбинируя прописные и строчные буквы, цифры и специальные символы;
* опасайтесь сообщений электронной почты и других сообщений с прикрепленными счетами и всегда обращайтесь в отдел по работе с клиентами компании для проверки подлинности документа;
* не предоставляйте персональные данные или пароли, отвечая на звонки неизвестных лиц[[27]](#footnote-27).

Соединенное Королевство представило исследование передового опыта обеспечения устойчивой системы кибербезопасности малых и средних предприятий, рассказав об усилиях, предпринимаемых для повышения киберустойчивости организаций по всей стране[[28]](#footnote-28). Одним из примеров таких усилий является коммуникационная кампания "Киберосведомленность", которая не ограничивается лишь повышением уровня осведомленности, а направлена на повсеместное внедрение базовых моделей поведения для обеспечения кибербезопасности. Реализация ориентированной на общественность и малые предприятия кампании была начата в апреле 2020 года, после того как кампания была оперативно доработана с учетом изменения характеристик киберугроз в связи пандемией COVID-19. В рамках этой кампании велась пропаганда действенных мер по смягчению воздействия угроз, в дополнение к которым были разработаны новые руководящие указания по обеспечению безопасности при выполнении работы на дому, переводе деятельности предприятий в онлайновую среду и использовании видеоконференцсвязи. Среди других инструментов:

* "Руководство для малого бизнеса: кибербезопасность";
* "Руководство для малого бизнеса: реагирование и восстановление", содержащее план последовательных действий, с помощью которого МСП могут подготовиться к киберинцидентам и смягчить их потенциальное воздействие;
* Exercise in a Box, бесплатный онлайновый инструмент, направленный на то, чтобы помочь МСП проверить свою киберустойчивость и пройти микрокурс, не имея при этом каких-либо основательных технических знаний;
* Руководство по COVID-19, призванное помочь предприятиям обеспечить свою безопасность при адаптации к пандемии и охватывающее такие темы, как работа на дому и перевод деятельности предприятия в онлайновую среду.

Соединенное Королевство также представило подробную информацию о поддерживаемой правительством программе сертификации Cyber Essentials, которая направлена на то, чтобы предприятия могли защитить свои товары от кибератак без необходимости соблюдения многочисленных сложных стандартов. Cyber Essentials была разработана таким образом, чтобы участие в ней могли принимать все организации, включая те, которые не обладают какими-либо начальными знаниями в области кибербезопасности или не имеют в своей структуре специальной кибергруппы.

## Системы управления рисками в области кибербезопасности

Системы управления рисками в области кибербезопасности имеют жизненно важное значение как для правительственных, так и для неправительственных организаций. Такие системы, как правило, предусматривают добровольное участие и обеспечивают управление цифровыми рисками на основе руководящих указаний и примеров передового опыта. В течение исследовательского периода исследовательская комиссия получила вклады от организаций, в которых были представлены различные примеры систем управления рисками в области кибербезопасности и методы их внедрения.

Так, Национальный институт стандартов и технологий Соединенных Штатов Америки недавно обновил свою Систему для укрепления кибербезопасности важнейшей инфраструктуры[[29]](#footnote-29). Данная система представляет собой направляемую бизнесом проактивную основу для добровольного управления киберрисками, которая предназначена для компаний всех размеров, работающих в различных секторах экономики. Она обеспечивает общую отправную точку и язык для оценки киберрисков. Система может легко адаптироваться, позволяя организациям, независимо от их размера, степени риска нарушения кибербезопасности или опыта в области кибербезопасности, применять принципы и передовой опыт управления рисками для укрепления безопасности и способности к восстановлению важнейшей инфраструктуры.

Система была разработана в результате успешного сотрудничества государственного и частного секторов в области управления рисками нарушения кибербезопасности, вклад в которое в течение года на добровольных началах внесли свыше 3000 заинтересованных сторон в лице предприятий, академических организаций, правительства и международных партнеров.

В основе системы лежат действующие международные стандарты и руководящие указания, а также передовой опыт предприятий, которые доказали свою эффективность с точки зрения защиты систем ИТ от киберугроз, обеспечения конфиденциальности коммерческой информации и защиты неприкосновенности частной жизни и гражданских свобод и которые направлены на содействие защите важнейшей инфраструктуры на основе управления рисками. Кроме того, данная система обеспечивает структуру для организации практической работы, а также инструменты, помогающие применять и внедрять стандарты и методы. Благодаря ссылкам на всемирно признанные стандарты кибербезопасности, система имеет универсальный характер и может служить в качестве международной модели управления киберрисками.

Принимая во внимание замечания и предложения заинтересованных сторон, Национальный институт стандартов и технологий внес следующие обновления в версию 1.1 данной системы:

* заявление о применимости данной системы к "технологиям", включая, как минимум, информационные и операционные технологии, киберфизические системы и IoT;
* доработка руководящих указаний для обеспечения возможности применения системы к управлению рисками, связанными с деятельностью цепочек поставок;
* изложение в краткой форме информации об актуальности и пользе предусмотренных системой показателей для проведения организацией самооценки;
* предоставление дополнительной информации о проведении самооценки для выявления рисков в области кибербезопасности;
* усиление учета требований к авторизации, аутентификации, проверке идентичности и раскрытию информации об уязвимостях;
* предоставление административных обновлений к информационным ссылкам для отражения прогресса, достигнутого частными и государственными организациями с точки зрения соблюдения стандартов и руководящих указаний.

Кроме того, в Бутане Королевский орган регулирования денежного обращения (центральный банк) издал директиву, направленную на содействие внедрению системы кибербезопасности для финансовых учреждений в целях повышения устойчивости банковской системы к неизвестным и сложным киберрискам[[30]](#footnote-30). Данная директива предусматривает следующее:

* все банки-участники должны стремиться соблюдать Отраслевой стандарт безопасности данных платежных карт, направленный на защиту среды данных о держателях карт. Кроме того, в дополнение к своим собственным мерам кибербезопасности банки должны внедрить стандарт ISO/IEC 27001:2013, касающийся систем управления информационной безопасностью;
* в директиве говорится о необходимости создания группы реагирования на киберинциденты в финансовых учреждениях для содействия активному сотрудничеству и эффективному обмену информацией по вопросам кибербезопасности между банками и Королевским органом регулирования денежного обращения. Группа будет активно отслеживать киберугрозы, планировать и координировать меры по противодействию им в целях предотвращения рисков для кибербезопасности и в кратчайшие сроки сообщать о всевозможных инцидентах соответствующему руководителю или органу. Недавно была сформирована кибергруппа для банков, ведущую роль в деятельности которой играет Королевский орган регулирования денежного обращения;
* банки-участники должны также внедрить соответствующую систему контроля за обеспечением кибербезопасности и принять безотлагательные ответные меры по обеспечению базовой информационной безопасности.

В качестве отдельного примера можно привести создание в Китае индекса оценки национальных перспектив с точки зрения планирования, разработки и внедрения компонентов сетевой безопасности на основе трехуровневых показателей с возрастающей степенью сложности[[31]](#footnote-31). На первом уровне оцениваются пять показателей:

* политика: национальные стратегии, законодательство, государственные учреждения, международное сотрудничество;
* промышленность: развитие сектора обеспечения безопасности сетей в среде, определяемой рыночными факторами, включая условия развития, масштаб, конкурентоспособность предприятий и самодостаточность;
* технологии: уровень исследований, разработок и применения технологий в области обеспечения национальной безопасности, включая научно-исследовательские проекты, инвестиции, технические стандарты и подготовку персонала;
* потенциал: уровень защиты и предотвращения угроз безопасности сетей, включая восприятие рисков, защиту безопасности, меры реагирования в чрезвычайных ситуациях и активную защиту;
* ресурсы: ресурсы, необходимые для поддержки создания потенциала, включая ресурсы сетевой инфраструктуры, осведомленность в вопросах безопасности и международное влияние.

Индексом также предусмотрены 19 показателей второго уровня и 53 показателя третьего уровня. Согласно системе оценки индекса, каждый показатель оценивается по шкале от 0 до 1 балла; при этом количество баллов не должно превышать 53. Расчеты по каждому показателю основаны на официальной информации, находящейся в открытом доступе и опубликованной на национальных и международных веб-сайтах, а также научно-исследовательскими учреждениями.

## Государственно-частное партнерство

Без посторонней помощи государственные органы не в состоянии улучшить положение дел в области национальной кибербезопасности. Для достижения успеха при осуществлении мер и проектов в области кибербезопасности необходимо выстроить прочные партнерские отношения между субъектами государственного и частного секторов.

Национальный институт стандартов и технологий Соединенных Штатов Америки разработал Систему для укрепления кибербезопасности важнейшей инфраструктуры на основе коллективных усилий в рамках государственно-частного партнерства[[32]](#footnote-32). Как было отмечено в более подробной форме в Разделе 2.4, институт обеспечил привлечение всех заинтересованных сторон к разработке обновленной версии, тем самым побудив их максимально придерживаться предусмотренных системой принципов. Благодаря тому, что заинтересованные стороны участвовали в разработке версии 1.1 системы и их предложения и замечания были учтены при этом, повысилась вероятность соблюдения и внедрения ими передовой практики, руководящих указаний и стандартов, содержащихся в ней.

В Республике Корея Министерство науки и информационно-коммуникационных технологий разработало Базовый план национальной кибербезопасности на 2019 год для частного сектора по результатам консультаций с соответствующими заинтересованными сторонами, включая академические организации, предприятия и общественные организации[[33]](#footnote-33). Планом было предусмотрено выполнение двух задач: обеспечение безопасности киберпространства и развитие отрасли информационной безопасности. Основные стратегические проекты в рамках этих усилий были направлены на расширение сети кибербезопасности, содействие развитию отрасли информационной безопасности и усиление инфраструктуры информационной безопасности.

Учитывая стремительно меняющуюся среду ИКТ, министерство намерено обновлять план на ежегодной основе. Кроме того, дважды в год проводятся заседания Консультационного совета государственного и частного секторов Республики Корея, на которых отслеживается ход выполнения плана и выявляются области, требующие улучшения.

Еще одним примером того, насколько важную роль партнерство между государственным и частным секторами играет в разработке всеобъемлющих национальных стратегий кибербезопасности, как указано в Разделе 2.1, является национальная стратегия кибербезопасности Бразилии E-Ciber. Государственно-частному партнерству выделено особое место среди ключевых стратегических направлений, предусмотренных E-Ciber. Среди них – содействие созданию условий для сотрудничества, широкого участия, обеспечения безопасности и формирования доверительных отношений между государственным и частным секторами и гражданским обществом, а также расширение партнерства в области кибербезопасности между ними, академическими организациями и гражданским обществом.

В качестве еще одного наглядного примера государственно-частного партнерства Бразилия представила обзорную информацию о своем опыте проведения в 2018 году национальных тренировочных занятий по кибербезопасности, известных как учения "Киберстража", в рамках которых акцент был сделан на важнейшей национальной инфраструктуре[[34]](#footnote-34). В 2019 году Бразилия провела последующие учения, значительно расширив круг участников за счет включения в него представителей министерств обороны, юстиции и иностранных дел, Управления ведомственной безопасности, вооруженных сил, органов федеральных правительственных учреждений, таких как Anatel, национальных CSIRT, Центрального банка Бразилии, государственных и частных банков, компаний в области ядерной энергетики, электроэнергетики и электросвязи, научных работников и приглашенных региональных и международных наблюдателей.

Еще одним примером государственно-частного партнерства являются группы CERT/CSIRT/CIRT. Благодаря им, государственные учреждения и частный сектор имеют возможность объединить усилия для урегулирования инцидентов, связанных с кибербезопасностью. В то же время для поддержания эффективности таких групп необходимы взаимодействие и доверительные отношения.

## Меры/инициативы по усилению потенциала

**Создание учебных заведений по вопросам кибербезопасности.**

Осознав, что для борьбы с растущими проблемами в области кибербезопасности необходимо инвестировать средства в подготовку кадров и образование в области кибербезопасности, многие правительства создали учебные учреждения для подготовки следующего поколения специалистов по вопросам кибербезопасности. Авторы нескольких вкладов, полученных от Государств – Членов МСЭ в рамках исследовательского периода, признали необходимость принятия соответствующих мер, в том числе путем укрепления отношений между государственными заинтересованными сторонами, университетами и научно-исследовательскими центрами.

Так, в 2015 году в Чаде была создана Национальная высшая школа информационных и коммуникационных технологий (ENASTIC), что стало наглядной демонстрацией наличия у высших органов власти страны политической воли к созданию основы для обеспечения повышения квалификации в области ИКТ (в том числе путем предоставления степеней в области кибербезопасности, сетей, электросвязи и т. д.)[[35]](#footnote-35).

Аналогичным образом, в Сенегале была создана ориентированная на региональный уровень Национальная школа кибербезопасности (ENC), цель которой заключается в наращивании потенциала и повышении уровня осведомленности лиц, ответственных за принятие решений, старших офицеров министерства обороны и других лиц, участвующих в функционировании цифровой экосистемы региона[[36]](#footnote-36).

Перед школой стоят, в том числе, следующие ключевые задачи:

* подготовка и повышение уровня осведомленности государственных должностных лиц, сенегальских и иностранных сотрудников и студентов, а также представителей государственного и частного секторов кибербезопасности в целях улучшения понимания рисков и угроз;
* регулярное обучение специализированных сотрудников CERT/CSIRT, с тем чтобы помочь им реагировать на самые изощренные кибератаки;
* периодическая подготовка сотрудников государственных и субрегиональных учреждений, с тем чтобы предоставить им возможность и знания, необходимые для подготовки к инцидентам, защиты от них, реагирования на них и восстановления после них.

# **Вызовы в области кибербезопасности, которые стоят на пути новых технологий, таких как интернет вещей и облачные вычисления**

## Введение

Экспоненциальный рост технологического потенциала привел к тому, что степень цифровизации мира, его подключения к интернету и его взаимосвязанности неуклонно увеличивается. По данным Всемирного экономического форума, эпоха, известная как "Глобализация 4.0", в которой цифровые активы и услуги составляют основу экономики и экспорта, уже началась[[37]](#footnote-37).

Под действием инновационных решений меняется ход технологического развития, что обусловлено необходимостью удовлетворения новых производственных нужд и практических потребностей. Наряду с технологией 5G устройства IoT получает все большее распространение: по оценкам, к 2025 году в мире будет насчитываться 41,6 миллиарда подключенных устройств[[38]](#footnote-38). Роль облачных решений в осуществлении тех или иных операций приобрела жизненно важное значение, в связи с чем их применяют 94% предприятий по всему миру[[39]](#footnote-39).Учитывая растущую доступность и точность данных, искусственный интеллект также продолжает находить более широкое применение.

В то же время появление новых технологий усиливает необходимость обеспечения кибербезопасности. Цифровые инновации привели к увеличению числа продуктов и их значительному усложнению, в результате чего выросла вероятность использования различных уязвимостей и недостатков.

Число киберугроз непрерывно увеличивается. В 2018 году ежедневно совершалось 80 000 кибератак, что составляло свыше 30 миллионов атак в год[[40]](#footnote-40). В 2019 году ежедневно регистрировалось более 90 миллиардов попыток похищения конфиденциальной информации[[41]](#footnote-41). Киберугрозы также становятся все более изощренными, угрожая целому миру и экономике, ориентированным на цифровые технологии, включая киберфизические системы в домах, "умных" городах, транспортных средствах, производственных системах и объектах важнейшей инфраструктуры. Эксперты доказали, что можно взломать даже медицинские устройства, имплантированные в человеческий организм, такие как кардиостимуляторы и дозаторы инсулина[[42]](#footnote-42).

Такой рост числа атак обусловлен также распространением в даркнете хакерства как услуги, которая зачастую предоставляется по приемлемой цене. Киберпреступность все больше коммерциализируется, превратившись в крупный сектор, где хакеры продают широкий спектр вредоносных инструментов и услуг, начиная от кражи паролей невысокой сложности и заканчивая сложными наборами эксплойтов и технологиями совершения атак, такими как DDoS, вредоносные программы, программы-вымогатели и программы-шпионы[[43]](#footnote-43). Кроме того, новые технологии, которые часто применяются для усовершенствования киберзащиты, могут использоваться злоумышленниками в целях повышения эффективности и расширения сферы применения инструментов взлома[[44]](#footnote-44). Искусственный интеллект, автоматизированные бот-сети, IoT и "облачные" решения все чаще используются в крупномасштабных кибератаках, а применение новых методов взлома, таких как инструменты для автоматизированного фишинга, вместе с новыми технологиями расширило спектр киберрисков.

Серьезной проблемой кибербезопасности является общая нехватка профессиональных навыков и недостаточная осведомленность сотрудников. По мере того, как киберугрозы становятся все более изощренными, организации с трудом набирают квалифицированных экспертов в области кибербезопасности, способных обеспечить защиту их систем[[45]](#footnote-45). В 2017 году 82% работодателей сообщили о том, что их сотрудники не обладают достаточными навыками в области кибербезопасности. К 2021 году 3,5 миллиона профессиональных должностей в сфере кибербезопасности останутся незанятыми[[46]](#footnote-46). Кроме того, персонал общего назначения демонстрирует слабый уровень знаний о киберугрозах. Человеческий фактор играет ключевую роль в обеспечении кибербезопасности и, как оказалось, несет значительную долю ответственности за допущенные инциденты. По результатам одного из исследований, в 2018 году 99% цифровых инцидентов были непреднамеренно инициированы сотрудниками, ставшими жертвами социальной инженерии; при этом лишь 1% таких инцидентов был вызван исключительно технологическими сбоями или эксплуатацией оборудования[[47]](#footnote-47).

Кибербезопасность – это динамично развивающаяся сфера, и организации должны осуществлять непрерывную проверку применяемых ими средств кибербезопасности для защиты от возникающих угроз. Для создания более безопасной среды необходимо привлечь заинтересованные стороны к обсуждению вопросов кибербезопасности и управления рисками, связанными с неприкосновенностью частной жизни, обеспечить проверку, расширение и совершенствование существующих процессов управления рисками в области кибербезопасности и неприкосновенности частной жизни, а также определить ключевые факторы кибербезопасности и неприкосновенности частной жизни, которые могут быть характерны для тех или иных технологических решений и условий. В настоящей главе рассматривается множество угроз кибербезопасности, связанных с появляющимися технологиями, включая IoT, облачные вычисления, 5G, искусственный интеллект и четвертую промышленную революцию (известную как "Промышленная революция 4.0"). В ней также изложены существующие тенденции, проблемы и возможные решения, направленные на устранение угроз, которые могут свести на нет успехи, достигнутые благодаря внедрению цифровых инноваций.

## Угрозы кибербезопасности, ее субъекты и их мотивы

Цель киберугроз заключается в том, чтобы подорвать три традиционные задачи кибербезопасности, а именно обеспечение конфиденциальности, целостности и доступности. Конфиденциальность защищает информацию от всех, кроме тех, кто имеет к ней доступ. Целостность обеспечивает точность и достоверность информации и предотвращает несанкционированное изменение данных. Доступность означает возможность доступа к данным и информации, когда это необходимо.

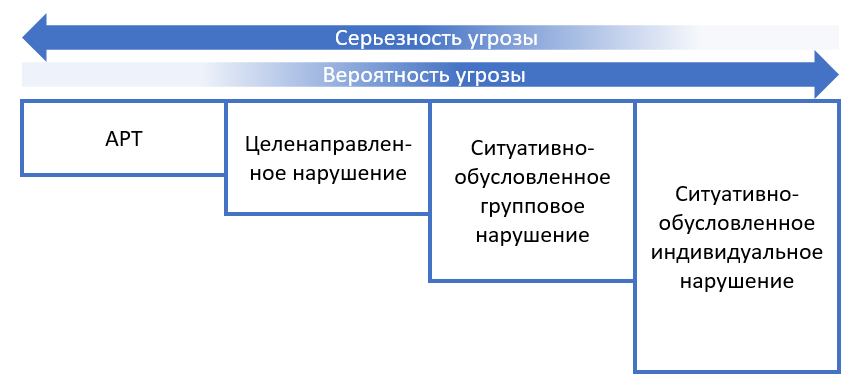
Ландшафт киберугроз – это неоднородная среда, в которой существуют различные субъекты, преследующие разные цели и располагающие разными возможностями. В целом злоумышленников можно классифицировать следующим образом:

* **инсайдеры:** согласно последним данным, около 40% инцидентов совершаются внутренним персоналом, зачастую недовольными сотрудниками, которые стремятся отомстить своим работодателям[[48]](#footnote-48). Инсайдеры могут быть особенно опасны, поскольку они имеют прямой доступ к данным, информации и цифровым активам;
* **хактивисты:** это люди, действия которых обусловлены политическими и социальными мотивами. Как правило, они крадут и распространяют конфиденциальную информацию, с тем чтобы поставить в неловкое положение политических лидеров или знаменитостей, а также раскрывают проприетарные и секретные данные во имя свободы слова. Кроме того, они часто искажают веб-сайты и совершают атаки типа DDoS на определенные службы или веб-сайты[[49]](#footnote-49);
* **киберпреступники:** это преступники, мотивированные финансовыми выгодами. Их цель – завладеть информацией об отдельных лицах, компаниях или организациях для получения денежной выгоды. Как правило, они шантажируют своих жертв, совершают эксфильтрацию и продажу данных и объектов прав интеллектуальной собственности на черном рынке, а также совершают атаки с помощью программ-вымогателей. Как уже говорилось выше, киберпреступления превратились в услугу, в рамках которой различные группы продают причиняющие вред товары и услуги, начиная с системных эксплойтов и заканчивая полноценными атаками;
* **устойчивые угрозы нового уровня (APT):** согласно определению Национального института стандартов и технологий Соединенных Штатов Америки, такие угрозы исходят от весьма изощренных и находчивых нарушителей, способных закрепиться в сети жертвы для достижения таких целей, как эксфильтрация информации, саботаж или препятствование осуществлению жизненно важных аспектов поставленной жертвой цели или причинение ущерба цифровым активам жертвы[[50]](#footnote-50). Устойчивые угрозы нового уровня адаптируются к системам защиты жертв благодаря тому, что атака совершается сразу по нескольким векторам; при этом выполнение предусмотренной такой атакой задачи может осуществляться в скрытном режиме в течение длительного периода времени. Такие нарушители являются наиболее сложными с точки зрения необходимых для этого технических навыков, финансирования и организационных ресурсов, поэтому их деятельность часто спонсируют государства для обеспечения своих геополитических интересов.

Несмотря на то, что все злоумышленники выбирают своей целью нарушение конфиденциальности, целостности и доступности информации и активов, вторжение в сеть может иметь широкий спектр последствий. Универсальный термин "кибератака" охватывает целый ряд действий, начиная с таких нарушений, как искажение веб-сайта или атака типа DoS, и заканчивая уничтожением важнейших данных и систем путем совершения атак с применением "оружия".

Злоумышленники и их атаки отличаются степенью изощренности и вредоносности, а также продолжительностью. Несмотря на то, что защититься от всех угроз не представляется возможным, организации могут распознавать соответствующие угрозы по их характеристикам, а также связанным с ними рискам и контексту, используя для этих целей модель угроз. На **Рисунке** 1 приведена общая модель киберугроз, показывающая, что большинство организаций, как правило, сталкиваются с ситуативно-обусловленными и менее изощренными угрозами, которые не требуют использования сложных средств защиты.

Рисунок 1. Модель угрозы



Напротив, крупные предприятия, организации, осуществляющие свою деятельность в жизненно важных и стратегических секторах, а также субъекты, управляющие ценной информацией и активами, с большей вероятностью подвергнутся атакам, исходящим от целенаправленных угроз или устойчивых угроз нового уровня.

В настоящем разделе представлен общий обзор существующих в киберпространстве угроз. В оставшейся части главы содержится информация о том, как такие угрозы применяются в отношении появляющихся технологий и какие доступны действенные стратегии, концепции и решения для защиты от них.

**Угрозы через призму технологий**

Появляющиеся технологии позволяют собирать, обмениваться, хранить и анализировать огромные объемы данных, зачастую с беспрецедентной скоростью. Вместе с тем некоторые факторы, в частности расширение возможностей для установления соединений и усложнение среды взаимодействия данных инструментов, могут породить ряд технологических и организационных проблем в области безопасности.

**Виртуализация**

Виртуализация является ключевым компонентом современной технологической среды, позволяя разработчикам настраивать инфраструктуру в соответствии с потребностями сетевых приложений и осуществлять разработку новых архитектур и протоколов в идеальных условиях[[51]](#footnote-51). В то же время совместное использование каналов связи и маршрутизаторов в мультиарендной архитектуре сопряжено с рядом рисков для обеспечения безопасности[[52]](#footnote-52).

* Риск несанкционированного раскрытия данных, как преднамеренного, так и непреднамеренного характера, усугубляется в виртуальной среде, где физические ресурсы совместно используются несколькими клиентами или пользователями. Вредоносные действия, такие как перехват и сбор "мусора" (поиск остатков данных в сети для получения информации), легче осуществить, если система позволяет проводить перекрестную проверку различных пользователей.
* Мультиарендная архитектура может увеличить риски, обусловленные наличием цепочки поставок, что затрудняет защиту от вторжений. Злоумышленники могут получить привилегии и вторгнуться в сеть жертвы, используя в качестве вектора вторжения ресурсы на том же физическом уровне, но с более низкой степенью защиты.
* В виртуализированной среде результаты обработки персональных данных имеют особенно сложный характер ввиду высокой иерархичности систем администрирования привилегий. Такие особенности открывают злоумышленникам возможности для совершения мошеннических действий с персональными данными и повышения уровня привилегий.
* Совместное использование ресурсов может также увеличить риск злонамеренных или непреднамеренных сбоев в работе системы, которые могут негативно сказаться на предоставлении услуг. В частности, перегрузка физических ресурсов может снизить производительность виртуальных сетей с последующим нарушением связи.

**Безопасность облачных вычислений**

В облачных решениях предоставление услуг и ресурсов на основе ИТ, включая связанные с ними функции и обязанности по обеспечению безопасности, осуществляется с привлечением поставщика облачных услуг. Благодаря этому появляется возможность оперативно расширить масштаб внедрения новых технологий и повысить их безопасность, так как поставщик, применяя принцип экономии за счет масштаба, потенциально может предложить более высокий уровень защиты и контроля. В то же время облачные уязвимости могут оказаться привлекательными для киберзлоумышленников ввиду того, что один-единственный успешный взлом может дать несанкционированный доступ ко множеству клиентов. Облачные решения включают в себя нескольких уровней абстракции (а именно: приложение, операционная система, архитектура и сеть), что позволяет злоумышленникам атаковать их по нескольким направлениям:

* уязвимостями программного обеспечения можно воспользоваться путем внедрения кода на языке структурированных запросов и применения других механизмов для совершения атак. В этом сценарии потребителям облачных услуг важно понимать, кто отвечает за внесение тех или иных исправлений (в частности поставщик облачных решений – за решения в отношении программного обеспечения как услуги, а потребитель – за решения в отношении инфраструктуры как услуги и платформы как услуги);
* поставщики облачных решений предлагают широкий спектр услуг и подключенных к интернету интерфейсов прикладного программирования, что позволяет их клиентам администрировать и контролировать свои активы. Такая возможность установления соединений делает облачные решения потенциальной мишенью для сетевых атак, таких как выслеживание/прослушивание сетевого трафика, атаки типа DoS и атаки через посредника;
* если злоумышленнику удается незаконно получить учетные данные пользователей, он может получить доступ к интерфейсу управления, используемому администраторами для управления большим количеством активов. Учитывая это, необходимо создать надежные механизмы аутентификации и авторизации, особенно для высоко привилегированных сотрудников;
* мультиарендная архитектура увеличивает риск нарушения сохранности или утечки данных в случае сбоя или взлома системы раздельного управления (нарушение изолированности);
* при переходе на облачные решения клиенты, как правило, теряют с точки зрения прозрачности и контроля над своими данными и активами. Это увеличивает риски, связанные с безопасным удалением данных, хранящихся на нескольких устройствах инфраструктуры поставщика облачных решений. Поэтому необходимо убедиться, что данные были надежно и тщательно удалены. Данная проблема усугубляется при применении мультиоблачных решений;
* привязка к поставщику, в результате которой клиенты сталкиваются с трудностями при переходе к другому поставщику облачных решений, может представлять серьезные риски для безопасности. Пользователям необходимо предусмотреть планы в отношении смены поставщика при разработке стратегий обеспечения непрерывности бизнес-процессов, а также хранить все данные в стандартном формате, позволяющем без труда осуществить их передачу;
* по данным Регуляторного органа связи Намибии, хранение данных клиентов в центрах обработки данных поставщиков облачных услуг, расположенных за пределами границ государства, представляет собой острую проблему. Юрисдикция органов регулирования не распространяется на страны, где размещены серверы данных, поэтому на их территории они практически не могут осуществлять надзор за обеспечением защиты клиентов и кибербезопасности в случае совершения кибератак, что приводит к краже идентичности, утечке персональных данных и, в некоторых случаях, потере потенциального дохода. Кроме того, законодательство таких стран может отличаться в том, что касается доступа к информации, защиты данных и законного мониторинга, в результате чего клиенты могут подвергаться несанкционированному доступу к персональным данным[[53]](#footnote-53).

**Интернет вещей**

Поскольку культура безопасности, закладываемой на этапе проектирования, еще только начинает получать распространение, одной из наиболее тревожных тенденций с точки зрения рисков является расширение возможностей для установления соединений, которое создает значительные проблемы в области безопасности[[54]](#footnote-54):

* "умные" объекты, начиная с камер, дверей и холодильных установок и заканчивая системами кондиционирования воздуха и носимыми устройствами, собирают огромное количество информации (как данных, так и метаданных). Подслушивая данные, получаемые "умными" объектами своей жертвы, злоумышленники могут многое узнать о ее жизни;
* новой угрозой для IoT являются программы-вымогатели. "Умные" устройства создают заманчивые возможности для вымогательства со стороны злоумышленников, и это обусловлено не только широким выбором "легкой" добычи, но и тем, что атаки такого рода могут нарушить работоспособность устройств, тем самым причиняя жертве неудобства и заставляя ее платить выкуп[[55]](#footnote-55);
* устройства IoT особенно уязвимы для атак типа DoS и DDoS, поскольку большинство из них имеют ограниченные технические возможности (память, хранение, центральный процессор и т. д.). Злоумышленники могут без труда перегрузить их ограниченные ресурсы, вызвав сбои в функционировании;
* ограниченность ресурсов в устройствах IoT создает очень существенную проблему, если возникает необходимость предусмотреть в них возможность принятия мер по обеспечению безопасности, поскольку последние могут требовать большого объема вычислительной работы[[56]](#footnote-56);
* ключевым фактором обеспечения безопасности IoT является уровень сложности. В устройствах применены различные технологии, такие как виртуализация, облачные вычисления, датчики и сети, которые имеют свои собственные уязвимости. Обеспечить безопасность IoT означает обеспечить безопасность всей цепочки таких компонентов. Аналогичным образом, IoT применяется в нескольких областях (бытовая автоматика, здравоохранение, предметы одежды и т. д.), в которых существуют различные потребности в отношении обеспечения безопасности и которые подвержены различным угрозам;
* несмотря на то, что наиболее распространенными являются интернет-атаки, устройства IoT также могут стать объектом физических атак. В местах, где наблюдение совсем или практически не ведется, злоумышленники могут без труда получить доступ к устройствам IoT и взломать их;
* устройства IoT также могут использоваться в качестве векторов для совершения атак типа DDoS. Так, в 2016 году известный поставщик систем доменных имен стал жертвой атаки типа DDoS, которая исходила от десятков миллионов IP-адресов, причем большая часть вредоносного трафика поступала с устройств IoT, таких как принтеры, маршрутизаторы и камеры[[57]](#footnote-57);

**5G**

Технологии связи пятого поколения, известные как 5G, повысят надежность и качество соединений за счет высокой скорости и малого времени задержки, что позволит получить максимальную отдачу от применения приложений на основе появляющихся технологий в таких областях, как энергетика, здравоохранение и производство. Соответствующие активы привлекают и злоумышленников, а присущие им уязвимости делают задачу по обеспечению кибербезопасности особенно сложной. Кроме того, поскольку решения на основе 5G все еще находятся на этапе экспериментального внедрения, существующих данных и информации о случаях совершения кибератак недостаточно, что еще больше усложняет понимание потенциальной угрозы[[58]](#footnote-58):

* ландшафт угроз, связанных с 5G, широк и неоднороден; сочетая в себе различные технологии, он также наследует сопряженные с ними уязвимости и угрозы. В частности, сети и активы 5G могут подвергаться атакам вследствие использования унаследованных уязвимостей технологий второго, третьего и четвертого поколений, а также традиционных IP-уязвимостей и уязвимостей технологии виртуализации. Злоумышленники также могут нацелиться на активы, характерные для 5G, такие как ядро, точка доступа и граничные элементы;
* атаки на технологии 5G могут включать в себя попытки кражи или уничтожения данных, манипулирования ими, перехвата сообщений или нарушения функционирования средств связи, повреждения физических активов или нарушения предоставления услуг. 5G соединит широкий спектр секторов и вертикалей, что, скорее всего, изменит условия кибербезопасности и, таким образом, вызовет появление новых уязвимостей;
* критический фактор угрозы исходит от цепочки поставок, в частности от подвергшихся атаке поставщиков товаров и услуг. Риск заключается в том, что поставщик может злонамеренно оставить в своей продукции скрытые обходные пути, недоработки программного обеспечения или критические ошибки. Внедрение автоматических (и неконтролируемых) обновлений и манипулирование функциональными возможностями также создают проблемы для обеспечения безопасности. Взаимосвязь между 5G и национальной безопасностью очевидна, поэтому к отбору поставщиков необходимо подойти серьезно, применив ориентированный на риски подход.

**Искусственный интеллект**

Распространение решений на основе искусственного интеллекта в различных сферах жизнедеятельности общества будет влиять на условия обеспечения кибербезопасности по нескольким направлениям. Такие активы могут стать мишенью для злоумышленников или использоваться ими и теми, кто им противостоит:

* активами на основе ИИ можно манипулировать, изменяя автоматизированные решения и поведение, в частности, путем искажения данных, фальсификации моделей классификации и использования обходных путей[[59]](#footnote-59). Все эти методы используют возможности для обучения системы, с тем чтобы оказать отрицательное воздействие на результат, введя в систему ошибочные данные и информацию[[60]](#footnote-60);
* хакеры прибегают к решениям на основе искусственного интеллекта, с тем чтобы расширить охват своих действий и возможности. Искусственный интеллект можно использовать для создания вредоносных программ, способных обходить меры защиты в автономном режиме, адаптируя применяемые методы на основе полученных положительных результатов и непрерывно совершенствуя свои действия;
* искусственный интеллект также является важным оборонительным ресурсом. Он может значительно повысить устойчивость системы путем усиления типичных мер защиты, таких как обнаружение угроз и аномалий, реагирование на инциденты и анализ угроз.

**Угрозы через призму Промышленной революции 4.0**

Парадигма Промышленной революции 4.0 предполагает применение автоматизации наряду с IoT, решениями в области виртуализации, аналитикой и искусственным интеллектом в различных вертикалях. Указанные технологии позволяют собирать, хранить, совместно использовать и интерпретировать огромные объемы данных и могут способствовать достижению существенного прогресса с точки зрения скорости, действенности, экономической эффективности и предоставления услуг. Предусмотренные Промышленной революцией 4.0 принципы применимы в различных отраслях, каждая из которых подвержена характерным для нее угрозам и рискам для безопасности.

**"Умные" дома**

"Умные" дома – это одна из множества вертикалей, где можно применить принципы, предусмотренные Промышленной революцией 4.0, в частности в области "умного" энергопотребления, освещения и отопления. "Умные" дома включают в себя широкий спектр "умных" объектов, которые используют датчики и исполнительные механизмы и управляются дистанционно через интернет[[61]](#footnote-61). Подключение устройств к интернету создает ряд рисков для безопасности:

* "умные" дома генерируют огромные объемы данных, которые уязвимы для атак. Как отмечено Министерством почты и новых информационно-коммуникационных технологий Чада, объекты, подключенные к интернету (включая "умные" телевизоры), не защищены от угроз безопасности информационной системы. Так, использование подключенных телевизоров может способствовать доступу к персональным данным через интернет не имеющих таких прав лиц или упростить кражу идентичности через сеть. Подключенные объекты так же уязвимы, как и личный компьютер, подключенный к компьютерной сети. Аналогичным образом, они подвергаются угрозе со стороны вредоносного программного обеспечения[[62]](#footnote-62);
* "умные" устройства имеют слабую защиту, и их можно без труда взломать. Злоумышленники, получившие контроль над устройством, могут перемещаться в боковом направлении в пределах внутренней сети, чтобы взять под контроль другие узлы;
* "умные" устройства, как правило, обладают ограниченными вычислительными ресурсами, что делает их особенно уязвимыми для атак типа DoS и DDoS, в результате которых устройство или сеть становятся временно недоступными для предполагаемого пользователя.

**"Умные" города**

Инфраструктура "умных" городов построена на сочетании появляющихся технологий с технологиями интеграции данных и автоматизации задач, что позволяет оптимизировать организацию городов и предложить услуги более высокого качества. В основе функционирования "умных" городов лежит обмен обширными массивами данных между важнейшими службами, такими как транспорт, энергоснабжение и здравоохранение, взаимосвязь которых неуклонно растет. Масштабы производимых данных и роль, которую эти данные играют в функционировании "умных" городов, обуславливают острую потребность в обеспечении кибербезопасности для защиты конфиденциальной информации и целостности цифровых активов от различных угроз безопасности:

* электронное здравоохранение: поскольку зависимость от технологий и объем данных в сфере здравоохранения растут, поставщики медицинских услуг должны защитить конфиденциальную информацию и обеспечить предоставление услуг. Несмотря на то, что информация о каких-либо имевших место инцидентах отсутствует, результаты моделирования подтвердили возможность беспроводного отключения имплантируемых кардиодефибрилляторов[[63]](#footnote-63), взлома дозаторов инсулина в целях введения летальной дозы[[64]](#footnote-64) и даже проникновения в системы мониторинга здоровья пациента для изменения основных показателей состояния его организма в режиме реального времени[[65]](#footnote-65);
* "умные" электросети: это ключевой компонент "умных" городов. В них используются двунаправленные устройства, такие как датчики, исполнительные механизмы и счетчики, которые позволяют поддерживать потоки энергии, идущие от производителей к потребителям, на одинаковом уровне и осуществлять контроль над ними[[66]](#footnote-66). Поскольку "умные" электросети используют протоколы ИКТ и подключение к интернету, они уязвимы для кибератак[[67]](#footnote-67). Хотя "умные" электросети представляют собой заманчивую мишень для совершения атак, они имеют сложную архитектуру, вследствие чего нанесение крупномасштабного ущерба требует технических и организационных ресурсов высокого уровня. На сегодняшний день известно лишь о двух случаях серьезных перебоев в электроснабжении, вызванных кибератаками, – BlackEnergy3 и Crashoverride, за которыми, как полагают, стояли государственные субъекты[[68]](#footnote-68);
* "умный" транспорт: цифровые активы, физические системы, сети связи и автоматизация могут использоваться в сфере транспортной инфраструктуры для оптимизации качества и эффективности. Изменяя данные и информацию, злоумышленники могут препятствовать трафику и даже вызывать инциденты. Кроме того, "умные" транспортные системы предполагают значительный поток персональной и конфиденциальной информации, которую необходимо защищать.

**Промышленный интернет вещей**

Промышленный интернет вещей (IIoT) адаптирует парадигму IoT к условиям промышленности. В сочетании с робототехникой и автоматизацией это может дать промышленным предприятиям важное преимущество, в том числе за счет повышения качества, экономической эффективности и поддержания производственного процесса на должном уровне. Такие киберфизические системы имеют особые характеристики и требования, ввиду чего преобразование традиционных мер обеспечения кибербезопасности становится особенно проблематичным.

Киберфизическая система – это существующая в режиме реального времени материальная среда с высоким уровнем обусловленности и взаимосвязанности, в которой доступность данных имеет выраженный характер по сравнению с целостностью и конфиденциальностью данных[[69]](#footnote-69). В таких системах цифровые компоненты взаимодействуют с физическими процессами, такими как движение объектов, химические реакции, выделение веществ и процессы охлаждения, а потоки данных служат в качестве ресурсов, необходимых для выполнения задач. В таких условиях внедрение общих средств обеспечения безопасности, таких как антивирусные программы, шифрование или брандмауэры, может замедлить поток данных и нарушить ход выполнения действий, что приведет к задержкам, которые могут существенно повлиять на осуществление деятельности, несмотря на то что они не являются значимыми с количественной точки зрения[[70]](#footnote-70).

Кроме того, большая часть оборудования в киберфизических системах не может справиться с осуществлением сложных мер безопасности и внедрением обновлений, что приводит к тому, что подключенные к интернету активы оказываются потенциально уязвимыми. Кибератаки на промышленные киберфизические системы могут нанести серьезный экономический ущерб, нарушив их функционирование и, как следствие, производственный процесс на заводе.

В то же время ключевая проблема заключается в том, что, манипулируя потоком данных, злоумышленники, совершающие кибератаки, могут изменять функционирование системы до тех пор, пока не произойдет ее механическое разрушение, что приведет к кинетическому воздействию и может иметь серьезные последствия для безопасности населения. Так, если злоумышленник введет в систему измененные данные, которые покажут диспетчеру, что температура снижается слишком быстро, диспетчер автоматически примет меры для компенсации такого снижения, увеличив температуру нагрева, что приведет к скрытому перегреву[[71]](#footnote-71). В 2014 году, например, злоумышленники взломали систему немецкого сталелитейного завода и не позволили печи выключиться надлежащим образом, чем могли нанести серьезный физический ущерб важнейшим компонентам[[72]](#footnote-72).

Злонамеренные кибердействия, способные оказать физическое воздействие, имеют крайне сложный характер и требуют не только хорошего понимания используемых цифровых активов, но и обширных знаний целевого физического процесса, а также подробных сведений о различных переменных. Таким образом, располагать техническими и организационными ресурсами, необходимыми для осуществления операций такого рода, по всей видимости, могут злоумышленники, стоящие за устойчивыми угрозами нового уровня, и спонсируемые государствами посредники.

## Существующие и появляющиеся решения

Значительная часть устройств IoT не имеет встроенных базовых функций по обеспечению кибербезопасности. В октябре 2018 года, после 18 месяцев взаимодействия с представителями отрасли и экспертами Национального центра кибербезопасности, Министерство цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства опубликовало Кодекс практики по безопасности потребительских устройств IoT[[73]](#footnote-73). В кодексе содержатся 13 добровольных руководящих указаний, которые являются базовыми для устройств IoT и которые производители должны учитывать при разработке своей продукции, чтобы обеспечить ее "безопасность по замыслу". Кодекс способствовал разработке первого применимого на глобальном уровне стандарта безопасности IoT – ETSI TS 103 645[[74]](#footnote-74).

Algérie Télécom также отметил необходимость предоставления руководящих указаний и рекомендаций по обеспечению безопасности появляющихся технологий, таких как облачные вычисления и IoT, которые должны стать основной движущей силой развития информационной системы и цифровой экономики[[75]](#footnote-75).

В **Таблице 1** и **Таблице 2** приведен перечень Рекомендаций МСЭ-Т, которые имеют отношение к защите облачных вычислений и IoT, соответственно, с точки зрения инфраструктуры, приложений, данных и конфиденциальности.

Таблица 1. Архитектура безопасности для защиты инфраструктуры, приложений и данных, а также обеспечения конфиденциальности в сфере облачных вычислений

| Название | Тема | Учреждение | Ссылка |
| --- | --- | --- | --- |
| Обзор безопасности облачных вычислений | | | |
| МСЭ-T X.1601 | Основы безопасности облачных вычислений | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613> |
| **Проектирование безопасности облачных вычислений** | | | |
| МСЭ-T X.1602 | Требования по безопасности прикладной среды программного обеспечения как услуги | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615> |
| МСЭ-T X.1603 | Требования к безопасности данных для услуги мониторинга облачных вычислений | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406> |
| МСЭ-T X.1604 | Требования к безопасности сети как услуге (NaaS) в среде облачных вычислений | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093> |
| МСЭ-T X.1605 | Требования к безопасности открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094> |
| МСЭ-T X.1631 | Информационные технологии - Методы обеспечения безопасности - Свод правил для управления информационной безопасностью, в основе которого лежит стандарт ISO/IEC 27002 для облачных услуг | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490> |
| **Передовой опыт и руководящие указания в области облачных вычислений** | | | |
| МСЭ-T X.1641 | Руководящие указания по безопасности данных потребителей облачных услуг | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853> |
| МСЭ-T X.1642 | Руководящие указания по эксплуатационной безопасности облачных вычислений | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616> |

Таблица 2. Архитектура безопасности для защиты инфраструктуры, приложений и данных, а также обеспечения конфиденциальности в сфере IoT

| **Название** | **Тема** | **Учреждение** | **Ссылка** |
| --- | --- | --- | --- |
| Безопасность интернета вещей (IoT) | | | |
| МСЭ-T X.1361 | Структура безопасности интернета вещей на основе модели с использованием шлюза | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607> |
| МСЭ-T X.1362 | Простая процедура шифрования для среды интернета вещей (IoT) | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196> |
| МСЭ-T X.1364 | Требования безопасности и структура безопасности узкополосного интернета вещей | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088> |
| МСЭ-T X.1365 | Методика обеспечения безопасности при использовании криптографии на основе идентичности в поддержку услуг интернета вещей (IoT) в сетях электросвязи | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089> |
| МСЭ-T серия X, Доб. 31 | МСЭ-T X.660 – Добавление “Руководящие указания по использованию идентификаторов объектов для интернета вещей“ | МСЭ | <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411> |

**Прочие появляющиеся методы и системы обеспечения безопасности**

* Приложения в области искусственного интеллекта, в том числе машинного и глубокого обучения, могут значительно повысить действенность и экономическую эффективность стратегий обеспечения кибербезопасности. С помощью регрессии, классификации и кластеризации эти решения выявляют аномалии, определяют различные типологии атак и разрабатывают возможные ответные меры для устранения их последствий. Системы на основе искусственного интеллекта также могут усилить эффект от мер реагирования на инциденты, предложив конкретные меры в ответ на те или иные инциденты. Кроме того, они могут повысить уровень управления рисками путем присвоения новым уязвимостям и ошибкам конфигурации значений показателей риска в автоматическом режиме на основе их описания, а также самостоятельно предупреждать атаки, значительно ускоряя извлечение, обработку и применение данных об угрозах, исполнителях, атаках, вредоносном программном обеспечении, уязвимостях и индикаторах компрометации[[76]](#footnote-76).
* Особенности технологии распределенного реестра (DLT) также являются перспективными с точки зрения использования приложений по обеспечению безопасности[[77]](#footnote-77). Во-первых, хранение данных с помощью DLT осуществляется децентрализовано, что значительно снижает риск обширной утечки данных, поскольку злоумышленники больше не могут получить доступ ко всем хранящимся данным через одну-единственную точку доступа. Аналогичным образом, децентрализация приносит существенные преимущества в области безопасности сетям IoT, организация которых традиционно построена на логике "клиент-серверная модель", предусматривающей управление данными и устройствами в сети центральным органом. С помощью DLT-приложений устройства IoT могут выявлять аномалии и изолировать узлы, которые ведут себя странным образом. Кроме того, DLT может способствовать формированию доверия к сетям IoT, обеспечивая непрерывную доступность, контролируемость, подотчетность, целостность и конфиденциальность подлежащих обмену данных[[78]](#footnote-78).
* Метод оркестровки, автоматизации и реагирования на угрозы безопасности (SOAR) включает в себя решения, предусматривающие установление соединений между инструментами и системами безопасности для обеспечения комплексности и органичности действий, таких как управление уязвимостями, реагирование на инциденты и автоматизация операций по обеспечению безопасности. Автоматизация процессов по обеспечению безопасности позволяет системе осуществлять мероприятия по устранению нарушений и проведению регламентных работ (сканирование уязвимостей, мониторинг доступа и ведение журнала регистрации) без вмешательства со стороны человека.
* Еще один вариант предусматривает использование модели нулевого доверия, в которой внутренняя сегментация сетевой среды и администрирование доступа осуществляются по принципу наименьших привилегий. Иными словами, каждый модуль, включая пользователей, устройства, интерфейсы прикладного программирования и устройства IoT, имеет доступ только к тем ресурсам, данным и активам, которые необходимы для их правомерного функционирования. Модели нулевого доверия значительно повышают уровень внутренней безопасности, затрудняя боковое перемещение злоумышленников и повышение ими своих привилегий благодаря тому, что заставляют их атаковать сразу несколько устройств для получения доступа ко всей сети.
* "Брокеры" безопасности облачного доступа – это точки применения правил, функционирующие на уровне между пользователями и поставщиками облачных услуг. В частности, принудительное применение правил безопасности может включать в себя аутентификацию, однократную регистрацию входа, авторизацию, сопоставление регистрационных данных, составление профилей устройств, шифрование, токенизацию, ведение журнала регистрации, оповещение, а также обнаружение/предупреждение применения вредоносного программного обеспечения[[79]](#footnote-79).
* Управление привилегированным доступом – это мониторинг и защита привилегированных учетных записей, таких как учетные записи администратора, используемые для доступа к важнейшим активам, данным и ресурсам, с помощью комплекса инструментов и решений. Такие решения изолируют важнейшие учетные записи в безопасном и контролируемом репозитории, тем самым снижая риск кражи регистрационных данных.
* Организациям следует перейти от подхода, ориентированного на разработку и эксплуатацию (DevOps), к подходу, ориентированному на разработку, обеспечение безопасности и эксплуатацию (DevSecOps), согласно которому функция обеспечения безопасности является неотъемлемой частью разработки и эксплуатации. В системах и инструментах DevSecOps обеспечение безопасности не привязывается к созданию конечного продукта (такого как программное обеспечение и приложения), а рассматривается как неотъемлемая и существенная функция, начиная с самого раннего этапа разработки. Такой подход повышает надежность мер по обеспечению безопасности, снижает риски и сокращает расходы на обеспечение соответствия нормативным требованиям.
* Разработанная Гартнером Адаптивная система непрерывной оценки риска и доверия (CARTA) предлагает адаптивный подход к обеспечению безопасности, в котором принятие решений осуществляется исходя из рисков и эффективности[[80]](#footnote-80). CARTA предполагает три этапа действий: "выполнение", в рамках которого основные усилия направлены на анализ основных угроз; "построение", который относится к угрозам и уязвимостям, выявленным в ходе разработки продуктов и их эксплуатации; и "планирование", в рамках которого используются аналитические методы для определения рисков безопасности и оценки того, не окажет ли их снижение негативного влияния на производительность[[81]](#footnote-81).

**Экономически эффективные решения**

* По данным Министерства цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства, начать борьбу с последствиями кибератак в широких масштабах и получить при этом значительные выгоды на глобальном уровне можно путем воздействия на окупаемость инвестиций в совершение наиболее типичных и наименее замысловатых атак. Программа активной киберзащиты была разработана для снижения окупаемости соответствующих инвестиций преступников вследствие повышения стоимости и рисков совершения кибератак на товары Соединенного Королевства[[82]](#footnote-82). В 2018 году программа обеспечила наибольший эффект от своей реализации благодаря своей ликвидационной службе, отвечающей за выявление вредоносных веб-сайтов (те, которые непосредственно участвуют в совершении атак или обеспечивают инфраструктурную поддержку их совершения) и уведомление их владельца или лица, предоставляющего услуги хостинга, о необходимости удаления таких веб-сайтов из интернета: таким образом было ликвидировано в общей сложности 192 256 мошеннических веб-сайтов; причем 64% этих веб-сайтов были ликвидированы в течение 24 часов. Кроме того, были ликвидированы 22 133 фишинговых кампании, размещавшихся в переданном Соединенному Королевству IP-пространстве (в общей сложности 142 203 индивидуальных атаки), а также 14 124 связанных с правительством фишинговых веб-сайта[[83]](#footnote-83).
* По мнению литовской компании NRD Cyber Security, для достижения значительных положительных результатов с точки зрения обеспечения безопасности национальной цифровой среды национальные и отраслевые группы CSIRT должны не только выполнять функции контактных лиц, аналитиков и координаторов мер реагирования на инциденты, но и вдохновлять на развитие и способствовать формированию дополнительного независимого потенциала в области кибербезопасности на уровне отраслей, профессиональных сообществ, образовательных центров, исследований, мероприятий, собраний, конференций, а также частных и ведомственных CSIRT[[84]](#footnote-84).
* По мнению эстонской компании Guardtime, киберучения имеют первостепенное значение для обеспечения киберустойчивости в долгосрочной перспективе, так как они помогают группам понять, какие процессы необходимы для смягчения последствий киберкризиса. Эстония рекомендует разработать программу управления киберустойчивостью, предусматривающую принятие соответствующих мер в области образования, проведения профессиональной подготовки и организации киберучений, включая как мероприятия местного значения, так и национальные учения, разработанные с учетом конкретных потребностей и проводимые на регулярной основе. Такие программы должны учитывать различные аспекты национальной организационной структуры и социально-экономической ситуации, функции и обязанности различных заинтересованных сторон, национальную нормативно-правовую базу, региональные и международные партнерские связи страны, а также различные риски, с которыми сталкивается страна в условиях меняющегося ландшафта киберугроз[[85]](#footnote-85).

# **Как кибербезопасность может способствовать защите персональных данных**

## Введение

С развитием новых информационных технологий появляются все новые и все более удобные услуги для использования в повседневной жизни. В то же время появление новых информационных технологий также приводит к тому, что риски, с которыми сталкиваются отдельные лица в контексте обеспечения конфиденциальности и защиты данных, изменяются на двусторонней основе. Персональные данные подвергаются все новым и новым угрозам, однако есть несколько способов, как минимизировать такие риски или избежать их. Для этого необходимо уделять больше внимания кибербезопасности и технологиям, которые направлены на усиление конфиденциальности и могут помочь защитить персональные данные, таким как псевдонимизация и "конфиденциальность по замыслу".

Псевдонимизация – это процедура управления данными и деидентификации данных, с помощью которой поля персональной идентификационной информации в записи данных заменяются одним или несколькими искусственными идентификаторами или "псевдонимами". Использование одного псевдонима вместо каждого замененного поля или целого ряда замененных полей снижает вероятность идентификации лица по такой записи данных; при этом оставшаяся часть записи данных остается пригодной для анализа и обработки данных[[86]](#footnote-86). Псевдонимизация может способствовать защите персональных идентификационных данных и уменьшить нагрузку на организации, которые собирают и хранят такие данные.

При применении принципа "конфиденциальность по замыслу" для принятия мер по обеспечению безопасности не нужно ждать совершения нарушения. Вместо этого разработчики прогнозируют или предугадывают угрозу конфиденциальности, или предотвращают ее возникновение с помощью превентивных мер, таких как планирование или проектирование услуг[[87]](#footnote-87).

Разница между двумя указанными выше подходами заключается в том, что псевдонимизация требует принятия определенных технических мер, в то время как принцип "конфиденциальность по замыслу" предоставляет операторам персональных данных свободу определения того, какие дополнительные технические меры могут наилучшим образом обеспечить безопасность и конфиденциальность данных.

## Правовая база и передовой опыт Государств-Членов

В Бразилии в недавно принятом Общем законе о защите данных содержится определение различных типов персональных и текущих данных, определены правовые основания для обработки данных на внутреннем и международном уровнях и основные права субъектов данных, а также предусмотрено создание национального органа по защите данных[[88]](#footnote-88). Законом установлены принципы минимизации данных, предотвращения их утечки и обеспечения их безопасности, а также конкретные правила, регулирующие деятельность в соответствующих сферах. Закон также предусматривает применение принципа "безопасность по замыслу", в соответствии с которым меры безопасности, необходимые для защиты персональных данных, применяются, начиная с этапа разработки продукции или услуг и заканчивая их предоставлением.

В 2017 году Китай официально представил комплекс национальных стандартов по техническим характеристикам безопасности персональных данных на основе технологии информационной безопасности, которые дополняют требования по безопасности персональных данных, изложенные в Законе о кибербезопасности. Стандарты содержат руководящие указания и инструкции по эксплуатации. Китай продолжает исследования и разработку стандартов в области защиты персональных данных[[89]](#footnote-89).

В Китае местные компании, осуществляющие деятельность по обеспечению безопасности данных, также активно исследуют и разрабатывают продукты и услуги в области безопасности, в том числе в области предотвращения потери данных, аудита безопасности баз данных, сканирования баз данных на предмет утечки данных, шифрования баз данных и маскирования данных, в целях предоставления технической поддержки в сфере защиты персональных данных.

Республика Корея внесла существенную поправку в свой Закон о защите персональных данных, которая предусматривает принятие технических мер для защиты персональных данных[[90]](#footnote-90). Данная поправка включала в себя изменения, направленные на упорядочение нормативного надзора и введение понятия "псевдонимизированных данных", что позволяет диспетчерам и операторам обработки данных осуществлять обработку данных более безопасным образом, сводя при этом к минимуму риск ненадлежащего использования и утечки данных за счет принятия других технологических и организационных мер, таких как "защита данных по замыслу" и "защита данных по умолчанию".

Кроме того, правительство Республики Корея опубликовало руководящие указания для защиты персональных данных при их автоматической обработке. Несмотря на то, что новые технологии, такие как анализ больших данных на основе применения искусственного интеллекта и датчики, используемые в устройствах IoT для сбора данных, делают предоставление инновационных услуг возможным, понимание потока обработки персональных данных сталкивается с определенными трудностями, а принятие последующих мер реагирования – с определенными ограничениями. Согласно руководящим указаниям, при автоматической обработке персональных данных, полученных с устройств IoT, рекомендуется применять принцип "конфиденциальность по замыслу", в соответствие с которым возможность утечки персональных данных тщательно учитывается на протяжении всего жизненного цикла данных, начиная с самых первых действий на этапе планирования.

Указанными руководящими указаниями предусмотрены следующие 10 правил защиты персональных данных при их автоматической обработке:

* Этап планирования
* Правило 1: подтверждение персональных данных, необходимых для предоставления услуг
* Правило 2: подтверждение соблюдения правовых норм при сборе персональных данных
* Этап проектирования
* Правило 3: минимизация данных и обработка только необходимых персональных данных
* Правило 4: применение соответствующих мер безопасности на каждом этапе обработки персональных данных
* Правило 5: прозрачное внедрение процедур и методов обработки персональных данных
* Правило 6: установление гарантий того, что субъекты данных могут легко реализовывать свои права
* Правило 7: четкие инструкции субъектам данных по предоставлению и передаче персональных данных третьим лицам
* Правило 8: уничтожение персональных данных и предотвращение их дальнейшего сбора по окончании предоставление услуг субъектом данных
* Правило 9: планы по гарантированию прав субъектов данных при прекращении бизнес-деятельности
* Этап оценки
* Правило 10: изучение факторов риска, связанных с утечкой персональных данных до начала предоставления услуг.

Ввиду недавно возникшей необходимости отслеживать подтвержденные случаи COVID-19 по всему миру Республика Корея приняла различные институциональные и технические меры для защиты персональных данных. Помимо обеспечения правовой основы для отслеживания пациентов с подтвержденным диагнозом путем пересмотра соответствующих нормативных актов, принимаются технические меры по разделению данных и управлению идентификационной информацией в целях предотвращения возможной утечки персональных данных. Отдельные данные используются для эпидемиологических исследований исключительно в случае подтверждения того или иного случая; при этом информация о пользователях и посетителях обрабатывается таким образом, который позволяет обеспечить ее безопасность, например путем автоматического уничтожения через четыре недели после того, как был проведен ее сбор[[91]](#footnote-91).

Итальянская компания разработала и запатентовала методологию, которую организации могут без труда использовать для составления перечня технических мероприятий по приведению облачной инфраструктуры (частной, общественной или гибридной) в соответствие с нормами конфиденциальности[[92]](#footnote-92). Данная методология, в том числе, предполагает разработку общих руководящих указаний, на основе которых Государства-Члены могли бы создать национальных конфигураторов для обеспечения более эффективной и приемлемой в ценовом отношении стандартизации с участием нескольких стран, используя технологию облачных вычислений в качестве мощной платформы для содействия стремительному развитию цифровой экономики.

Еще один пример передового опыта – это Статья 25 о защите данных "по замыслу" и "по умолчанию" Общего регламента по защите данных Европейского союза, согласно которой "конфиденциальность по замыслу" признается как наиболее подходящий способ предупреждения рисков для защиты персональных данных, связанных с устройствами IoT, большими данными, искусственным интеллектом и другими новыми технологиями. Понятие "конфиденциальность по замыслу" подразумевает принятие соответствующих организационных и технических мер для обеспечения безопасности и конфиденциальности персональных данных на протяжении всего жизненного цикла продуктов, услуг, приложений, а также бизнес-процедур и технических процедур организации. Технические меры могут включать, в частности, псевдонимизацию и минимизацию данных[[93]](#footnote-93).

Управление Европейского союза по кибербезопасности представило восемь ключевых принципов содействия применению предприятиями концепции "конфиденциальность по замыслу" в целях изучения различных методов, стратегий и технических факторов защиты персональных данных[[94]](#footnote-94).

Таблица 3. Восемь ключевых принципов применение концепции "конфиденциальность по замыслу"

|  | **Принцип** | **Суть** |
| --- | --- | --- |
| 1 | Минимизировать | Минимизация количества обрабатываемых персональных данных за счет обработки в соответствии с четко поставленными целями, направленными на снижение вероятности нарушения требований конфиденциальности |
| 2 | Скрыть | Скрыть передачу открытого текста при обработке персональных данных для предотвращения доступа извне |
| 3 | Разделить | Разделить и хранить отдельно различные персональные данные для предупреждения дискриминации отдельного лица в базе данных |
| 4 | Агрегировать | Агрегировать большие объемы обрабатываемых персональных данных, с тем чтобы свести к минимуму дискриминацию отдельных лиц, а также распределить результаты обработки данных по категориям, с тем чтобы сделать дискриминацию невозможной |
| 5 | Проинформировать | Информировать субъектов данных обо всем процессе обработки персональных данных, с тем чтобы обеспечить четкое понимание целей использования данных |
| 6 | Установить контроль | Установить контроль за использованием персональных данных. Субъекты данных должны понимать весь процесс обработки персональных данных и иметь возможность реализовать свои права в отношении неправомерного использования их персональных данных или уровней безопасности в соответствии с пятым принципом – "Проинформировать" |
| 7 | Обеспечить соблюдение | Внутренняя политика защиты персональных данных должна отражать правовые и систематические обязанности и должна быть реализована на практике |
| 8 | Продемонстрировать | Продемонстрировать выполнение правовых обязательств, в частности в отношении обеспечения эффективного внедрения политики защиты персональных данных и безотлагательного принятия мер в ответ на инциденты, связанные с утечкой данных |

Управление Европейского союза по кибербезопасности также внесло предложения о проведении различными заинтересованными сторонами мероприятий, направленных на обеспечение конфиденциальности и защиту данных. Управлением рекомендует лицам, ответственным за разработку политики, содействовать и поддерживать разработку новых стимулов для усовершенствования услуг по защите персональных данных, а также группам, занимающимся научно-исследовательской и опытно-конструкторской деятельностью, исследовать технические методы защиты персональных данных на основе междисциплинарного подхода и распространить результаты исследований через лиц, ответственных за разработку политики, и средства массовой информации. Наконец, управление рекомендует разработчикам программного обеспечения создать технологию, которая могла бы на интуитивном уровне осуществлять обновление свойств конфиденциальности и позволяла бы обеспечить защиту персональных данных в рамках общедоступных и совместно разработанных инфраструктурных проектов.

Федеральная торговая комиссия Соединенных Штатов Америки (FTC) придает особое значение практическим и процессуальным принципам обеспечения конфиденциальности, таким как "конфиденциальность по замыслу" и упрощенный выбор потребителя, а также материально-правовым и процессуальным принципам, таким как гарантированная прозрачность. Комиссия также делает акцент на защите конфиденциальности потребителей в контексте деятельности коммерческого предприятия, продукции и всех этапов развития услуг[[95]](#footnote-95).

Управление по защите данных Испании (AEPD) опубликовало руководство по применению принципа "конфиденциальность по замыслу", в котором подчеркивается необходимость учитывать фактор конфиденциальности и принципы защиты данных с самого начала обработки каких бы то ни было данных. В руководстве также представлены основные принципы и стратегии обработки персональных данных[[96]](#footnote-96).

Таблица 4. Взаимосвязь между целями обеспечения конфиденциальности и принципами проектирования конфиденциальности

| **Цели обеспечения конфиденциальности** | **Принципы обеспечения конфиденциальности, ориентированные на данные** | **Принципы обеспечения конфиденциальности, ориентированные на процесс** |
| --- | --- | --- |
| Невозможность установления связи | Минимизировать, извлечь, разделить, скрыть |  |
| Установить контроль |  | Установить контроль, обеспечить соблюдение, продемонстрировать |
| Прозрачность |  | Проинформировать |

## Извлеченные уроки и дальнейшие действия

Скорость кибератак, утечки данных и несанкционированного использования персональных данных растет в геометрической прогрессии. Сейчас как никогда важно понять права и обязанности отдельных лиц и организаций в отношении персональных данных; особенно это касается организаций, которые работают с информацией, позволяющей установить личность.

В этой главе представлен обзор правовых изменений и технических мер обеспечения кибербезопасности, которые были внедрены на территории Государств-Членов для защиты персональных данных. В ней также приведены примеры передовой практики, с тем чтобы помочь Государствам-Членам выполнять меняющиеся требования в отношении конфиденциальности данных, а также изложена роль технологий кибербезопасности в снижении рисков и содействии соблюдению установленных требований.

Изучив различные технологии кибербезопасности и передовой опыт, применяемые Государствами-Членами для защиты персональных данных, можно извлечь следующие уроки:

* институциональные механизмы псевдонимизации, применения принципа "конфиденциальность по замыслу" и принятия других технологических мер способствуют формированию более безопасной среды;
* предприятиям, которые собирают и используют персональные данные, необходимо предпринимать активные усилия по внедрению технических мер, направленных на обеспечение более основательной защиты персональных данных;
* различным заинтересованным сторонам, в том числе субъектам данных, гражданскому обществу, научно-педагогическому составу академических организаций и представителям промышленности, необходимо обсуждать использование технологий и прилагать усилия для повышения осведомленности и улучшения безопасности на коллективной основе.

# **Глобальный индекс кибербезопасности МСЭ (v3): обзор по региону СНГ**

## Обзор

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Государство-Член | Оценка GCI | Правовой | Технический | Организационный | Наращивание потенциала | Сотрудничество |
| Российская Федерация | 0,836 | 0,197 | 0,162 | 0,177 | 0,166 | 0,135 |
| Казахстан | 0,778 | 0,179 | 0,143 | 0,174 | 0,160 | 0,122 |
| Узбекистан | 0,666 | 0,123 | 0,142 | 0,112 | 0,143 | 0,144 |

Российская Федерация имеет наивысшие баллы практически по всем параметрам, за исключением параметра сотрудничества, где наивысший балл имеет Узбекистан. У Казахстана хорошие результаты: второе место по всем параметрам, кроме сотрудничества.

**Российская Федерация** занимает первое место с хорошей оценкой по правовому уровню, она усилила соблюдение нормативных требований в отношении предотвращения мошенничества и борьбы с ним с использованием электронных платежных систем.

Вся финансовая система страны была усовершенствована для обеспечения безопасности использования электронных платежей в Интернете.

**Казахстан** занимает второе место с высокими баллами по правовому уровню. Казахстан унифицировал требования в области информационно-коммуникационных технологий и информационной безопасности.

**Узбекистан** занимает третье место, демонстрируя высокие баллы в компоненте сотрудничества, страна подписала меморандум о взаимопонимании с различными агентствами в соседних странах. Узбекистан также развил сильное государственно-частное партнерство, в том числе с иностранными компаниями.

## Сравнение в региональном разрезе

В этом разделе представлен анализ количества стран в каждом регионе, которые демонстрируют большую заинтересованность в конкретных показателях направления. Это помогает получить обзор регионов, которые нуждаются в принятии дополнительных мер по усилению определенных показателей.

Информация и передовой опыт, упомянутые в этом разделе, предоставлены странами.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель | Африка | Америка | Арабские страны | Азиатско-Тихоокеанский регион | СНГ | Европа |
| Законодательство по кибербезопасности | 38 | 32 | 18 | 35 | 9 | 45 |
| Регулирование кибербезопасности | 37 | 32 | 17 | 31 | 9 | 45 |
| Ограничение спама | 22 | 10 | 10 | 15 | 5 | 40 |

Направление хорошо развито в европейском регионе, который также имеет самые высокие значения по всем трем показателям. Из 46 Государств-Членов в 45 есть законы о киберпреступности, в 45 – законодательство по кибербезопасности, а в 40 действуют правила по ограничению спама.

**Литва –** Парламент принял Закон о кибербезопасности, вступивший в силу с 1 января 2015 года. Закон имеет ряд исполнительных актов, таких как Национальный план управления киберинцидентами, Организационные и технические требования кибербезопасности, применимые к критически важной информационной инфраструктуре, и государственные информационные ресурсы, Методология идентификации критически важной информационной инфраструктуры и т. д. Закон наделяет Национальный центр кибербезопасности полномочиями принимать меры в случае злонамеренных действий. Новая редакция Закона о кибербезопасности была представлена в Парламент Литвы с целью транспонирования Директивы (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года о мерах по обеспечению высокого общего уровня безопасности сетей и информационных систем по всему Союзу.

С момента принятия закона Бюро криминальной полиции Литвы (ответственное за расследование криминальных киберинцидентов) в сотрудничестве с CERT-LT успешно выявляло и расследовало киберинциденты, связанные с IP-адресами, участвующими в деятельности ботнета. CERT-LT имеет возможности запросить предоставить список вредоносных IP-адресов, и Бюро отправит обязательные указания соответствующим поставщикам услуг, администрирующим данные IP-адреса, с просьбой исправить проблему. Если проблема не будет устранена в течение 48 часов, то доступ в Интернет для такого IP-адреса может быть заблокирован. Не взирая на то, что приказ о блокировке доступа в Интернет должен быть одобрен судом, с момента принятия закона было «очищено» более 100 IP-адресов.

Государственная инспекция по защите данных Литовской Республики (далее - SDPI) создала онлайн-форму для сообщения об инцидентах кибербезопасности, связанных с утечкой персональных данных, с использованием системы электронных услуг SDPI.

**Молдова –** в контексте построения информационного общества Правительство Республики Молдова утвердило стратегические и законодательные рамки для развития области ИКТ в Молдове, наиболее важной из которых является Национальная стратегия развития информационного общества «Цифровая Молдова 2020».

Программа кибербезопасности на 2016-2020 годы предлагает систематический и комплексный подход к реализации действий, необходимых для обеспечения кибербезопасности в Республике Молдова, на основе лучших международных практик посредством их гармонизации с европейским законодательством. Программа включает семь направлений: безопасная обработка, хранение и доступ к данным; безопасность и целостность сетей электросвязи и электронных услуг; возможности предотвращения и реагирование на чрезвычайные ситуации; предотвращение киберпреступности и борьба с ней; усиление киберзащиты; образование и информирование; международное сотрудничество и взаимодействие. В целях реализации программы подготовлено и утверждено Постановление Правительства «Об утверждении обязательных требований кибербезопасности» (Постановление Правительства № 201 от 28 марта 2017 г.). Эти минимальные требования к кибербезопасности применяются к Государственной канцелярии, министерствам и другим центральным административным органам в отношении уже существующих ИТ-систем, информационных ресурсов и систем, а также тех, которые находятся в стадии разработки, тестирования и внедрения, для обеспечения адекватной системы защиты информации.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Национальный CERT | Стандарты по кибербезопасности | Орган по стандартизации | Технические механизмы и возможности по ограничению спама | Использование облака | Меры по защите детей в онлайн среде |
| Африка | 13 | 9 | 18 | 5 | 10 | 19 |
| Америка | 17 | 14 | 21 | 7 | 8 | 12 |
| Арабские страны | 10 | 12 | 13 | 5 | 10 | 12 |
| Азиатско-Тихоокеанский регион | 24 | 17 | 18 | 15 | 18 | 17 |
| СНГ | 5 | 5 | 7 | 5 | 4 | 6 |
| Европа | 39 | 35 | 37 | 30 | 27 | 38 |

Как показано на гистограмме, в Африке несмотря на то, что она не является лидером в технической области, 19 Государств-Членов принимают участие в мерах по защите детей в Интернете, сразу после Европы, в которой данное направление развивается в 38 из 46 Государств-Членов. В Северной и Южной Америке и Арабских странах меры по защите детей в Интернете приняты примерно в 12 странах из каждого региона, в Азиатско-Тихоокеанском регионе – в 17, а в СНГ – в 6 из 9 Государств-Членов.

**Беларусь –** уполномоченные поставщики Интернет-услуг предоставляют услуги хостинга для реализации механизмов, обеспечивающих контроль целостности Интернет-ресурсов. К таким механизмам относятся использование программных средств для обнаружения ошибок работы операционных систем, вызванных наличием в системе вредоносных программ, таких как «ARKIT» - программа, защищающая от вредоносного ПО, несанкционированного доступа и межсетевой экран (CANOE).

**Эстония –** в сентябре 2017 года CERT-EE был выдан Certification Certificate и сертификат качества от Trusted Introducer. В мире существует более 300 CERT, 22 из которых признаны Certification Certificate. Шесть из признанных субъектов являются национальными, включая Эстонию.

**Монголия –** Главное разведывательное управление, Национальный центр данных и НПО MN-CERT несут ответственность за предотвращение кибератак и реагирование на них, однако в стране не существует единой системы для реализации этой функции на национальном уровне. В 2017 году правительство Монголии начало написание технико-экономического обоснование создания CERT и системы аудита ИТ-безопасности для Монголии. Проект технико-экономического обоснования направлен на определение состояния среды кибербезопасности, такой как организация/персонал, инфраструктура ИКТ, правовая среда и стандарты, процесс ИТ-безопасности/аудита, а также изучение плана развития. Кроме того, данный проект направлена на формирование будущей модели CERT Монголии.

**Украина –** команда CERT-UA постоянно предпринимает шаги для взаимодействия с другими группами CERT Государств-Членов, а также с Cisco Talos Intelligence Group по вопросам, связанным с преодолением последствий кибератак на критически важную информационную инфраструктуру, выявлением причин и обстоятельств киберинцидентов. Кроме того, учитывая свое членство в международных организациях, принимая во внимание взятые на себя обязательства и важность государственно-частного партнерства в сфере кибербезопасности, CERT-UA помогает устранять угрозы для частного сектора Украины, а также для государственного и частного секторов за рубежом.

Следует отметить, что Закон Украины «Об основных принципах кибербезопасности Украины» среди прочего определяет задачи CERT-UA на законодательном уровне. В соответствии с этим Законом, CERT-UA и Центр по борьбе с киберпреступностью будут играть координирующую роль в мерах, направленных на оперативное (кризисное) реагирование на кибератаки и киберинциденты, а также внедрение контрмер, направленных на минимизацию уязвимости систем связи. Государственная служба связи участвует в работе Агентства ЕС по кибербезопасности и Европейском центре исследований и компетенции в области кибербезопасности, а также запланированы учения по внедрению Оперативной схемы совместного реагирования ЕС и Государств-Членов на крупномасштабные кибератаки. Система реагирования на кризисы в области кибербезопасности будет способствовать расширению возможностей Центра реагирования на кибератаки и групп CERT-UA.

В 2018 году **Грузия** начала исследовательский проект – портал онлайн-кибер-упражнений. CyberLab – новый онлайн-ресурс, созданный Группой реагирования на компьютерные чрезвычайные ситуации (CERT.GOV.GE) и Грузинской ассоциацией научных и образовательных сетей (GRENA) при поддержке проекта EaPConnect, финансируемого ЕС. Портал помогает студентам учебных заведений, изучающим информационные технологии и заинтересованных в тематике кибербезопасности, углубить свои практические навыки, для лучшего обнаружения киберинцидентов и лучшего реагирования на них. Портал также поможет ИТ-персоналу из государственного и частного секторов, где готовность к кибератакам критически важна, обеспечить устойчивость в киберпространстве и повысить квалификацию. Упражнения, доступные на портале, разнообразны и включают в себя: криптографию, анализ вредоносного кода реальных инцидентов, анализ файлов журнала киберинцидентов, произошедших на реальных серверах, обратный инжиниринг, анализ недостатков сети, кибер-аналитику и т. д.

Из двадцати баллов, распределенных по организационной составляющей, стратегии кибербезопасности и процент стран, в которых есть ответственные за кибербезопасность агентства, получают более высокие баллы. Регион Европы показывает наибольшее количество по каждому показателю, за ним следует Азиатско-Тихоокеанский регион и СНГ. Все регионы представляют большое количество стран, в которых есть агентства, ответственные за кибербезопасность.

**Нидерланды –** новый Центр цифрового доверия расширит обмен информацией и станет платформой увеличения уровня кибербезопасности второстепенных секторов и компаний. Цель состоит в том, чтобы создать киберэкосистему, которая предоставляет информацию и перспективы для действий. Кроме того, будет создана общенациональная сеть партнерств по вопросу кибербезопасности для более широкого, эффективного и действенного обмена информацией о кибербезопасности между государственным и частным сектором. Целью этой общенациональной сети является усиление возможностей государственных и частных лиц.

Другие передовые методы включают пилотные проекты с двумя крупными портами - Роттердам (FERN) и Схипхол (CYSSIC), согласованное раскрытие уязвимостей и постоянное совершенствование агентств по обмену информацией.

**Сингапур –** Агентство кибербезопасности Сингапура (CSA) было создано как единое национальное агентство для надзора за всеми вопросами кибербезопасности, включая стратегию кибербезопасности, работу и образование, информационно-пропагандистскую деятельность и развитие экосистемы. Как описано в Сингапурской национальной стратегии кибербезопасности, CSA, будучи центральным агентством, наблюдает за защитой важнейших секторов информационной инфраструктуры, государственным образованием и информационно-пропагандистской деятельностью, развитием отрасли и международным сотрудничеством. CSA создало национальную структуру, способную поддерживать централизованный надзор и оказывать поддержку национальной кибербезопасности, но при этом сохранять гибкость в реагировании отраслевых потребностей с помощью своей трехуровневой модели (страницы 16-17 Национальной стратегии кибербезопасности Сингапура).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Кампании по информированию общественности по вопросам кибербезопасности | Рамки для сертификации и аккредитации | Профессиональные тренинги/курсы по вопросам кибербезопасности | Образовательные программы или академические дисциплины | Научно-исследовательские программы | Механизмы стимулирования наращивания потенциала | Отечественная индустрия кибербезопасности |
| Европа | 40 | 26 | 41 | 41 | 42 | 27 | 36 |
| СНГ | 6 | 3 | 8 | 8 | 6 | 7 | 5 |
| Азиатско-Тихоокеанский регион | 25 | 15 | 24 | 19 | 22 | 14 | 19 |
| Арабские страны | 12 | 7 | 15 | 15 | 15 | 10 | 10 |
| Америка | 21 | 6 | 17 | 21 | 16 | 7 | 11 |
| Африка | 25 | 9 | 17 | 22 | 22 | 6 | 11 |

Только 1 из 9 Государств-Членов в регионе СНГ не имеет четкой информации об образовательных программах/академических дисциплинах по кибербезопасности, график также показывает, что регион Европы (синий) сохраняет высокие позиции по большинству показателей, за ним следует регион СНГ. В Государствах-Членах особенно заметны улучшения в национальной промышленности – 47 процентов по сравнению с 32 процентами в 2017 году.

**Турция** – в январе 2017 года было организовано онлайн-соревнование по кибербезопасности Cyber Star. Было получено более 27 000 заявок, участие приняло около 15 000 человек. Конкурс выявил экспертов по кибербезопасности в стране, а некоторые из победителей были наняты в TRCERT (Национальный CERT Турции). TRCERT участвовал в учениях НАТО по управлению кризисными ситуациями CMX-2017 в октябре 2017 года и в национальных учениях по киберзащите в ноябре 2017 года.

Центр безопасного Интернета (SIC) был создан для повышения осведомленности о правильном и безопасном использовании Интернета. SIC управляет «горячей линией» Интернета и сайтом Safe Web, на котором семьи могут найти советы о том, как наилучшим образом использовать Интернет. Проект «Безопасный Интернет» предоставляет детям и молодым людям, имеющим ограниченный доступ к ИКТ, платформу, где они могут близко познакомиться с технологиями и изучить возможности, которые они предоставляют. Проект повышает осведомленность о безопасном использовании Интернета для детей и состоит из шести областей: область технологического опыта, область роботизированного кодирования, область виртуальной реальности, область осознанного и безопасного использования Интернета, область обучения и область соревнований. SIC также управляет специализированным веб-сайтом для детей, который включает игры, различные активности, конкурсы и тренинги. Компания SIC организовала мероприятие «День безопасного Интернета», основная тема которого – «Создавайте, объединяйте и делитесь информацией: лучший Интернет начинается с вас». ICTA и Университет Бахчешехир запустили конкурс компьютерных игр, чтобы побудить молодых людей в возрасте от 12 до 18 лет разрабатывать игры, и во время этого мероприятия Facebook и Google провели для студентов семинары по цифровым играм и безопасному Интернету.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Африка | Америка | Арабские страны | Азиатско-Тихоокеанский регион | СНГ | Европа |
| Двусторонние соглашения | 12 | 14 | 12 | 16 | 5 | 40 |
| Многосторонние или международные соглашения | 17 | 12 | 9 | 19 | 7 | 44 |
| Участие в международных ассоциациях | 32 | 27 | 15 | 32 | 7 | 41 |
| Государственно-частное партнерство | 16 | 9 | 9 | 17 | 7 | 37 |
| Межведомственное партнерство | 14 | 13 | 7 | 20 | 7 | 35 |

Все регионы принимают активное участие в международных форумах, в то время как у многих стран мало двусторонних соглашений, межведомственных партнерств и государственно-частных партнерств. Только 2 из 46 Государств-Членов в европейском регионе не имеют многосторонних соглашений по кибербезопасности. Все регионы указывают среднее количество стран по всем показателям.

**Эстония –** являясь одной из первых стран в мире, которая разработала стратегию кибербезопасности (в 2008 году), текущая стратегия действует до конца 2018 года, в настоящее время ведутся консультации и работа над стратегией следующего поколения (четвертой), которая начнет действовать 1 января 2019 года и будет действительна на протяжении четырех лет. Эстонская ассоциация информационной безопасности (EISA) была официально основана в январе 2018 года. Роль EISA заключается в активизации межотраслевого сотрудничества в Эстонии между академическими кругами и частным сектором, а также с правительством, включая поддержку договорного партнерства государственного и частного секторов ЕС (cPPP) по построению модели кибербезопасности. Совместные усилия направлены на формализацию существующих связей и усиление научно-исследовательской деятельности в области информационной безопасности и кибербезопасности в Эстонии. EISA также станет частью стратегии нового поколения «Стратегия кибербезопасности Эстонии на 2019-2022 годы».

**Оман** в полной мере участвует в международных форумах, например, представитель страны является сопредседателем 17-й Исследовательской комиссии МСЭ по стандартизации в области кибербезопасности, проведение семинара по кибербезопасности на Всемирном саммите МСЭ по информационному обществу (WSIS) в сотрудничестве с Международным вычислительным центром Организации Объединенных Наций. В Омане проводятся мероприятия, пропагандирующие важность вопросов кибербезопасности, такие как День безопасного Интернета, которые были опубликованы на европейском портале BIK в связи с их успешностью. Оман также проводит ежегодный региональный саммит по кибербезопасности для региона Арабских стран, в дополнение к региональному симпозиуму ITU-FIRST для регионов Африки и Арабских стран и учениям по кибербезопасности в Танзании. Оман также разрабатывает сценарии и проводит ежегодные региональные учения по кибербезопасности и семинары по данной тематике в сотрудничестве со сторонними организациями, такими как Chathom House.

OmanCERT получил международную аккредитацию для национальной лаборатории цифровой криминалистики, страна входит в число 100 лучших руководителей информационной безопасности (CISO) в категории женщин-руководителей в регионе и заняла третье место в региональном конкурсе хакеров CTF (захват флага). Через Арабский региональный центр кибербезопасности МСЭ (ITU-ARCC) Оман поддерживает другие страны как в регионе Арабских стран, так и на международном уровне, делясь своим опытом, и помогая странам получить членство в FIRST (Форум по реагированию на инциденты и группа безопасности), спонсируя других CIRTs.

**Узбекистан –** подписаны соглашения о сотрудничестве с Государствами-Членами Содружества Независимых Государств (СНГ) по борьбе с преступлениями в сфере информационных технологий, а также Соглашение о противодействии региональной антитеррористической структуре Шанхайской организации сотрудничества (ШОС) по направлению кибербезопасности.

# **Предложения по работе по направлению кибербезопасности в регионе СНГ и потенциальные партнеры**

## Мандат МСЭ

Задачей 2 Плана действий Буэнос-Айреса является содействие развитию инфраструктуры и услуг, в том числе укреплению доверия и безопасности при использовании электросвязи/ИКТ.

Для ее реализации была дополнена Резолюция 69 (пересм. Буэнос-Айрес, 2017) «Содействие созданию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничеству между ними».

Как основной координатор Направления действия C5 ВВУИО, МСЭ отвечает за помощь заинтересованных в укреплении доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях.

В дополнение Резолюция 130 Полномочной конференции МСЭ (пересм. Пусан, 2014) «Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий» поручает Директору Бюро развития электросвязи (БРЭ) оказывать поддержку Государствам-Членам в создании организационных структур, таких как группы CIRT, для выявления киберугроз, управления ими и реагирования на них, а также механизмов сотрудничества на региональном и международном уровнях.

ВКРЭ-17 также призывает оказывать помощь Государствам-Членам в создании организационных киберструктур, таких как группы реагирования на компьютерные инциденты (CIRT) для определения киберугроз, управления операциями и реагирования в случае киберугроз, а также участия в механизмах сотрудничества на региональном и международном уровнях.

## Создание и усовершенствование национальных Групп реагирования на инциденты в области кибербезопасности (CIRT)

CIRT играет ключевую роль в решении вопросов обеспечения кибербезопасности на национальном уровне, в частности, в обнаружении, управлении и реагировании на киберинциденты в случае их возникновения. Однако, создание такого механизма требует финансирования, человеческих ресурсов, обучения, технических возможностей, взаимоотношений между государственным и частным сектором и соответствующего законодательства. Эти требования часто становятся препятствием для развивающихся стран с их ограниченными человеческими, институциональными и финансовыми ресурсами.

Создание CIRT и разработка соответствующих процессов может также стать основой для следующей деятельности:

* Создание базы знаний для поддержки реализации Национальной стратегии по кибербезопасности, а также подходов к защите критической информационной инфраструктуры;
* Поддержка создания национальной культуры кибербезопасности и сопутствующих информационных кампаний;
* Поддержка разработки национальных платформ кибербезопасности, таких как Инфраструктура публичных ключей (PKI), услуг электронного правительства, национальных идентификаторов и управления доступом;
* Дальнейшее совершенствование возможностей по реагированию и управлению инцидентами.

Формальная структура работы МСЭ по направлению CIRT включает в себя четыре этапа:

При работе с заинтересованными Государствами-Членами в регионе СНГ МСЭ следует данному алгоритму. В частности, первым шагом в подготовке потенциального проекта является проведение страновой оценки готовности к созданию или усовершенствованию CIRT, которая выполняется экспертами МСЭ в рамках физической миссии. Результатом оценки является отчет о готовности страны к созданию или усовершенствованию CIRT, на основе которого МСЭ и страна-бенефициар в дальнейшем выполняют подготовку проектного документа и мобилизацию партнеров и финансовых ресурсов.

## Учения по кибербезопасности

Целью учений МСЭ ко кибербезопасности является создание потенциала и совершенствование возможностей участвующих групп обмениваться информацией и реагировать на инциденты, а также обеспечение на уровне регионов непрерывных совместных усилий национальных групп реагирования на компьютерные инциденты (CIRT) и групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) в вопросах борьбы с киберугрозами. Учения открыты для национальных CIRT/CSIRT, министерств, регуляторных органов, операторов электросвязи, университетов и общеобразовательных учреждений, производителей оборудования электросвязи, исследовательских и проектных учреждений, разработчиков программного обеспечения и других заинтересованных сторон из Государств − Членов МСЭ, а также для Членов Сектора. Рекомендуется, чтобы на учениях присутствовали по крайней мере два члена технической группы и один сотрудник руководящего звена.

Длительность учений в физическом формате как правило составляет пять дней. В первые два дня мероприятия проводится целевые тренинги (например, подготовка по управлению CIRT/CSIRT, совместно с Форумом групп реагирования на инциденты и обеспечения безопасности (FIRST)). В третий день проходит высокоуровневый форум по вопросам кибербезопасности, который представляет собой открытую площадку, где специалисты в области ИКТ и руководящие работники из государственных органов, промышленных, научных и неправительственных организаций смогут обсудить идеи по улучшению кибербезопасности. Практические занятия по кибербезопасности проходят в последние два дня и посвящены различным сценариям, включающим наиболее распространенные виды кибератак.

Учения по кибербезопасности могут проходить в следующих форматах:

* Глобальные (пример – [онлайн-учения в 2020 году](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx))
* Межрегиональные (пример – [учения для Азиатско-Тихоокеанского региона и региона СНГ в 2019 году](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) в Куала-Лумпур, Малайзия)
* Региональные (пример – [учения для региона СНГ в 2018 году](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/Events/2018/09_Baku/09_Baku.aspx) в Баку, Азербайджан)
* Национальные (пример – первые национальные учения по кибербезопасности в Кыргызстане в 2021 году)

С учетом крайне высокой востребованности такого формата работы целесообразно продолжать активную работу с заинтересованными Государствами-Членами МСЭ из региона МСЭ, а также выделить дополнительные ресурсы на поддержку данного направления.

## Целевые региональные и национальные тренинги

В рамках программы по созданию потенциала МСЭ оказывает поддержку странам в подготовке и переподготовке специалистов как технического, так и управленческого профиля. Предлагается продолжать такую работу исходя из конкретных интересов Государств-Членов МСЭ. Финансирование таких тренингов может осуществляться как из бюджета Оперативного плана, так и из бюджетов отдельных проектов. Примеры запросов стран по целевым тренингам:

* Сетевая безопасность (CND)
* Администрирование Linux/Unix (LPI C1)
* Обратный инжиниринг программного обеспечения
* Управление проектами (PMP)
* Управление информационной безопасностью (ISC2 (CISSP))

## Глобальный индекс кибербезопасности

Глобальный индекс кибербезопасности измеряет приверженность стран кибербезопасности, предоставляя ориентиры для улучшения, побуждая страны улучшать свою позицию в области кибербезопасности, обмениваясь передовым опытом, который может быть воспроизведен другими странами, и предоставляя актуальную информацию исследователям кибербезопасности.

После публикации отчета о третьей итерации выводов GCI и ее включения в Резолюцию 130 (Пересм. Дубай, 2018 г.) четвертая итерация GCI (GCIv4) была запущена в октябре 2019 года во время собрания Вопроса 3 2-й Исследовательской комиссии. По официальному приглашению 168 стран назначили координатора для участия в вопроснике, ответы на который должны были быть получены в сентябре 2020 года.

В октябре 2020 года было проведено заседание экспертной группы GCI Weightage для обсуждения подхода к рекомендации весов индикаторов GCIv4, субиндикаторов и микропоказателей на основе относительной важности мер кибербезопасности в модели GCI. Группа экспертов включала 76 участников из Государств-Членов, членов Сектора МСЭ-D, научных кругов и частного сектора. Полученные 43 рекомендованных весовых коэффициента были объединены для определения весов по каждому вопросу GCIv4.

Группа по кибербезопасности БРЭ выполнила необходимую работу по проверке 146 представленных ответов и сбору данных для не ответивших стран для охвата всех Государств-Членов МСЭ. Проверенные данные возвращаются странам-участницам для утверждения перед использованием данных в целях анализа и составления отчета для окончательной публикации.

Публикация четвертой итерации отчета GCI запланирована на конец апреля во время одного из вебинаров ВВУИО, в котором будут освещены новые выводы, улучшены меры и изучены места, где существует разрыв между странами и регионами.

## Обмен опытом по национальным стратегиям кибербезопасности

В условиях пандемии COVID-19 многие страны пришли к пониманию необходимости пересмотра или же создания национальной стратегии кибербезопасности. Такая стратегия должна предлагать адекватные меры реагирования на существенно изменившийся характер киберугроз, а также смещать фокус на защиту ИКТ-инфраструктуры и информационных систем в здравоохранении и образовании, которые приобрели критическую важность в 2020 году.

В связи с этим, целесообразно стимулировать международное и региональное сотрудничество и обмен опытом по этому направлению, а также проводить целевые тренинги для заинтересованных.

1. См. Рекомендации МСЭ-T серии X.1230/X.1240, <https://www.itu.int/itu-t/recommendations/index.aspx?ser=X>. [↑](#footnote-ref-1)
2. См. Рекомендацию МСЭ-T X.1205, Доб. 9, <https://www.itu.int/rec/T-REC-X.Sup9> [↑](#footnote-ref-2)
3. <https://www.statista.com/statistics/420391/spam-email-traffic-share/> [↑](#footnote-ref-3)
4. <https://www.spamlaws.com/spam-stats.html> [↑](#footnote-ref-4)
5. <https://dataprot.net/statistics/spam-statistics> [↑](#footnote-ref-5)
6. <https://purplesec.us/resources/cyber-security-statistics> [↑](#footnote-ref-6)
7. <https://www.dmarcanalyzer.com/spf>; <http://dkim.org>; <https://dmarc.org> [↑](#footnote-ref-7)
8. <https://www.rfc-editor.org/info/rfc6480> [↑](#footnote-ref-8)
9. <https://www.manrs.org/> [↑](#footnote-ref-9)
10. <https://www.m3aawg.org/about-m3aawg> [↑](#footnote-ref-10)
11. <https://www.internetsociety.org/spamtoolkit/> [↑](#footnote-ref-11)
12. <https://www.gsma.com/security/> [↑](#footnote-ref-12)
13. <http://www.spamhaus.org/> [↑](#footnote-ref-13)
14. <https://apwg.org/> [↑](#footnote-ref-14)
15. <https://www.antispywarecoalition.org/> [↑](#footnote-ref-15)
16. *Соединенное Королевство,* Документ [SG2RGQ/155](https://www.itu.int/md/D18-SG02.RGQ-C-0155), "Исследование передового опыта по уменьшению риска программ-вымогателей в Соединенном Королевстве" [↑](#footnote-ref-16)
17. *Бразилия*, Документ [SG2RGQ/216](https://www.itu.int/md/D18-SG02.RGQ-C-0216), "Национальная стратегия в области кибербезопасности Бразилии (E-Ciber)” [↑](#footnote-ref-17)
18. *Бенин*, Документ [2/152](https://www.itu.int/md/D18-SG02-C-0152), "Кибербезопасность в эпоху цифровой экономики в Бенине" [↑](#footnote-ref-18)
19. *Чад*, Документ [2/136](https://www.itu.int/md/D18-SG02-C-0136), "Положение дел в области кибербезопасности в Республике Чад" [↑](#footnote-ref-19)
20. *Соединенное Королевство*, Документ [SG2RGQ/241](https://www.itu.int/md/D18-SG02.RGQ-C-0241), "Обновленное исследование обеспечения безопасности устройств интернета вещей (IoT) пользователей в Соединенном Королевстве" [↑](#footnote-ref-20)
21. *Бутан*, Документ [SG2RGQ/79](https://www.itu.int/md/D18-SG02.RGQ-C-0079), "Вызовы, проблемы и рекомендации Бутана: взгляд со стороны развивающихся стран" [↑](#footnote-ref-21)
22. *NRD Cyber Security (CS) (Литва)*, Документ [2/172](https://www.itu.int/md/D18-SG02-C-0172), "Развитие национальных и секторальных CSIRT как способ укрепления среды кибербезопасности, по данным за 2019 год" [↑](#footnote-ref-22)
23. *Мексика*, Документ [2/165](https://www.itu.int/md/D18-SG02-C-0165), "Представление о кибербезопасности пользователей фиксированного и/или мобильного интернета" [↑](#footnote-ref-23)
24. *Бутан*, Документ [SG2RGQ/79](https://www.itu.int/md/D18-SG02.RGQ-C-0079), "Вызовы, проблемы и рекомендации Бутана: взгляд со стороны развивающихся стран" [↑](#footnote-ref-24)
25. *Бутан*, Документ [SG2RGQ/135](https://www.itu.int/md/D18-SG02.RGQ-C-0135), "Инициативы по кибербезопасности в Бутане" [↑](#footnote-ref-25)
26. *Бразилия*, Документ [SG2RGQ/215](https://www.itu.int/md/D18-SG02.RGQ-C-0215), "Кампании по повышению осведомленности "#Безопасное соединение (#ConexãoSegura)” [↑](#footnote-ref-26)
27. С более подробной информацией о кампании "Безопасное соединение", проводимой Anatel, можно ознакомится на следующем веб-сайте: <https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais>. [↑](#footnote-ref-27)
28. *Соединенное Королевство*, Документ [SG2RGQ/272](https://www.itu.int/md/D18-SG02.RGQ-C-0272), "Исследование конкретного примера в Соединенном Королевстве: передовой опыт обеспечения кибербезопасности МСП" [↑](#footnote-ref-28)
29. Соединенные Штаты Америки, Документ [SG2RGQ/151](https://www.itu.int/md/D18-SG02.RGQ-C-0151), "Версия 1.1 Системы для укрепления кибербезопасности важнейшей инфраструктуры NIST" [↑](#footnote-ref-29)
30. *Бутан*, Документ [SG2RGQ/135](https://www.itu.int/md/D18-SG02.RGQ-C-0135), "Инициативы по кибербезопасности в Бутане" [↑](#footnote-ref-30)
31. *Китай*, Документ [2/155](https://www.itu.int/md/D18-SG02-C-0155), "Разработка индекса оценки потенциала обеспечения безопасности сетей" [↑](#footnote-ref-31)
32. Соединенные Штаты Америки, Документ [SG2RGQ/151](https://www.itu.int/md/D18-SG02.RGQ-C-0151), "Версия 1.1 Системы для укрепления кибербезопасности важнейшей инфраструктуры NIST" [↑](#footnote-ref-32)
33. *Республика Корея*, Документ [2/168](https://www.itu.int/md/D18-SG02-C-0168), "Комплексный план по кибербезопасности на 2019 год для частного сектора" [↑](#footnote-ref-33)
34. *Бразилия*, Документ [SG2RGQ/214](https://www.itu.int/md/D18-SG02.RGQ-C-0214), "Национальное тренировочные занятия по кибербезопасности Бразилии – учения "Киберстража" [↑](#footnote-ref-34)
35. *Чад*, Документ [2/136](https://www.itu.int/md/D18-SG02-C-0136), "Положение дел в области кибербезопасности в Республике Чад" [↑](#footnote-ref-35)
36. *Сенегал*, Документ [SG2RGQ/146](https://www.itu.int/md/D18-SG02.RGQ-C-0146), "Обзор Национальной школы кибербезопасности с региональной ориентацией" [↑](#footnote-ref-36)
37. *Klaus Schwab*, "Globalization 4.0 - What Does It Mean?", World Economic Forum, 5 November 2018, <https://www.weforum.org/agenda/2018/11/globalization-4-what-does-it-mean-how-it-will-benefit-everyone/>. [↑](#footnote-ref-37)
38. *Business Wire*, “The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast”, 18 June 2019, <https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast> [↑](#footnote-ref-38)
39. *Kim Weins*, “Cloud Computing Trends: 2019 State of the Cloud Report”, Flexera Blog, 21 May 2020, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/> [↑](#footnote-ref-39)
40. *PurpleSec*, “2019 Cyber Security Statistics Trends & Data: The Ultimate List of Cyber Security Stats”, *PurpleSec* (blog), accessed 27 April 2020, <https://purplesec.us/resources/cyber-security-statistics/> [↑](#footnote-ref-40)
41. *Check Point*, “Prepare for a New Cyber Cold War in 2020, Warns Check Point”, 24 October 2019, <https://www.checkpoint.com/press/2019/prepare-for-a-new-cyber-cold-war-in-2020-warns-check-point/> [↑](#footnote-ref-41)
42. *Lily Hay Newman*, “These Hackers Made an App That Kills to Prove a Point”, Wired, 16 July 2019, <https://www.wired.com/story/medtronic-insulin-pump-hack-app/>; *Dan Goodin*, “Insulin Pump hack delivers fatal dosage over the air”, The Register, 27 October 2011, <https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/> [↑](#footnote-ref-42)
43. *Armor*, “The Dark Market Report: The New Economy”, 28 September 2020, <https://www.armor.com/resources/the-black-market-report/> [↑](#footnote-ref-43)
44. *Deloitte*, “Protecting against the changing cybersecurity risk landscape: Future of risk in the digital era”, <https://www2.deloitte.com/us/en/pages/advisory/articles/advanced-cyber-threats.html> [↑](#footnote-ref-44)
45. *William Crumpler and James A. Lewis*, “The Cybersecurity Workforce Gap”, 29 January 2019, <https://www.csis.org/analysis/cybersecurity-workforce-gap> [↑](#footnote-ref-45)
46. *Varonis*, “110 Must-Know Cybersecurity Statistics for 2020”, 26 October 2020, <https://www.varonis.com/blog/cybersecurity-statistics/> [↑](#footnote-ref-46)
47. *Proofpoint*, “Proofpoint’s Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click”, 9 September 2019, <https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more> [↑](#footnote-ref-47)
48. *Verizon*, “2019 Data Breach Investigations Report”, <https://enterprise.verizon.com/resources/reports/dbir/> [↑](#footnote-ref-48)
49. *Lillian Ablon*, “Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data”, RAND Corporation, 2018, <https://doi.org/10.7249/CT490> [↑](#footnote-ref-49)
50. *United States National Institute of Standards and Technology, Joint Task Force Transformation Initiative*, “NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View”, March 2011, <https://doi.org/10.6028/NIST.SP.800-39> [↑](#footnote-ref-50)
51. *Leonardo Richter Bays et al*, “Virtual network security: threats, countermeasures, and challenges”, Journal of Internet Services and Applications 6, article no. 1 (2015), <https://doi.org/10.1186/s13174-014-0015-z> [↑](#footnote-ref-51)
52. *European Union Agency for Cybersecurity (ENISA)*, “Security aspects of virtualization”, 10 February 2017, <https://www.enisa.europa.eu/publications/security-aspects-of-virtualization> [↑](#footnote-ref-52)
53. *Намибия,* Документ [SG2RGQ/75](https://www.itu.int/md/D18-SG02.RGQ-C-0075), "Обеспечение кибербезопасности, осложненное предоставлением облачных услуг" [↑](#footnote-ref-53)
54. *Amit Ashbel*, “The rise of IoT and the associated security risks”, 7 July 2016, <https://www.itproportal.com/2016/07/07/the-rise-of-iot-and-the-associated-security-risks/> [↑](#footnote-ref-54)
55. *Syed Rameem Zahra and Mohammad Ahsan Chishti*, “RansomWare and Internet of Things: A New Security Nightmare”, 2019 9th International Conference on Cloud Computing, Data Science Engineering(Confluence), <https://doi.org/10.1109/CONFLUENCE.2019.8776926> [↑](#footnote-ref-55)
56. *Ammar Rayes and Samer Salam*, “Internet of Things From Hype to Reality: The Road to Digitization”, Cham: Springer International Publishing, 2019, <https://doi.org/10.1007/978-3-319-99516-8> [↑](#footnote-ref-56)
57. *Nicole* *Perlroth*, “Hackers Used New Weapons to Disrupt Major Websites Across U.S.”, The New York Times, 21 October 2016, <https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html> [↑](#footnote-ref-57)
58. *European Union Agency for Cybersecurity (ENISA)*, “ENISA threat landscape for 5G Networks”, 21 November 2019, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks> [↑](#footnote-ref-58)
59. *Battista Biggio and Fabio Roli*, “Wild patterns: Ten years after the rise of adversarial machine learning”, Pattern Recognition vol. 84, December 2018, pp. 317-31, <https://doi.org/10.1016/j.patcog.2018.07.023> [↑](#footnote-ref-59)
60. *Matthew Jagielski et al*, “Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning”, 2018 IEEE Symposium on Security and Privacy (SP), 2018, <https://doi.org/10.1109/SP.2018.00057> [↑](#footnote-ref-60)
61. *Ado Adamou Abba Ari et al*, “Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges”, Applied Computing and Informatics, 31 July 2020, <https://doi.org/10.1016/j.aci.2019.11.005> [↑](#footnote-ref-61)
62. *Чад*, Документ [2/140](https://www.itu.int/md/D18-SG02-C-0140), "Уязвимость подключенных телевизиров" [↑](#footnote-ref-62)
63. *Daniel Halperin et al*, “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”, 2008 IEEE Symposium on Security and Privacy (sp 2008), <https://doi.org/10.1109/SP.2008.31> [↑](#footnote-ref-63)
64. *Arundhati Parmar*, “Hacker shows off vulnerabilities of wireless insulin pumps”, MedCityNews, 1 March 2012, <https://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/>; *David C. Klonoff*, “Cybersecurity for Connected Diabetes Devices”, Journal of Diabetes Science and Technology 9, vol. 9, no. 5, 16 April 2015, <https://doi.org/10.1177/1932296815583334> [↑](#footnote-ref-64)
65. *Douglas McKee*, “80 to 0 in Under 5 Seconds: Falsifying a Medical Patient’s Vitals”, McAfee, 11 August 2018, [https://www.mcafee.com/blogs/other-blogs/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/?hilite=%27thou%27](https://www.mcafee.com/blogs/other-blogs/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/?hilite='thou') [↑](#footnote-ref-65)
66. *Lindah Kotut and Luay A. Wahsheh*, “Survey of Cyber Security Challenges and Solutions in Smart Grids”, 2016 Cybersecurity Symposium (CYBERSEC), <https://doi.org/10.1109/CYBERSEC.2016.013> [↑](#footnote-ref-66)
67. *Muhammed Zekeriya Gunduz and Resul Das*, “Cyber-security on smart grid: Threats and potential solutions”, Computer Networks, vol. 169, 14 March 2020, <https://doi.org/10.1016/j.comnet.2019.107094> [↑](#footnote-ref-67)
68. *Dragos, Inc*, “CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids”, 12 June 2017, <https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/> [↑](#footnote-ref-68)
69. *Roberto Setola et al*, “Cyber threats for operational technologies”, International Journal of System of Systems Engineering, vol. 10, no. 2, 2020, <https://doi.org/10.1504/IJSSE.2020.10026809> [↑](#footnote-ref-69)
70. *Roberto Setola et al*, “An overview of Cyber Attack to Industrial Control System”, Chemical Engineering Transactions, vol. 77, 2019, <https://doi.org/10.3303/CET1977152> [↑](#footnote-ref-70)
71. *Stephen McLaughlin et al*, “The Cybersecurity Landscape in Industrial Control Systems”, Proceedings of the IEEE, vol. 104, issue 5, May 2016, <https://doi.org/10.1109/JPROC.2015.2512235> [↑](#footnote-ref-71)
72. *Robert M. Lee et al,* “German Steel Mill Cyber Attack”, Industrial Control Systems Defense Use Case Dec 30, 2014, <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf> [↑](#footnote-ref-72)
73. *United Kingdom, Department for Digital, Culture, Media and Sport*, “Code of Practice for Consumer IoT Security”, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf> [↑](#footnote-ref-73)
74. *European Telecommunications Standards Institute (ETSI)*, “ETSI TS 103 645 V1.1.1 (2019-02): CYBER; Cyber Security for Consumer Internet of Things”, <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf> [↑](#footnote-ref-74)
75. *Algérie Télécom SPA (Алжир)*, Документ [2/66](https://www.itu.int/md/D18-SG02-C-0066), "Предложения относительно содержания заключительного отчета по Вопросу 3/2" [↑](#footnote-ref-75)
76. *Padmavathi Ganapathi and D. Shanmugapriya*, “Handbook of Research on Machine and Deep Learning Applications for Cyber Security”, IGI Global, 2019 and *Dave Shackleford*, “Who’s Using Cyberthreat Intelligence and How?”, SANS, 12 February 2015, <https://www.sans.org/reading-room/whitepapers/analyst/membership/35767> [↑](#footnote-ref-76)
77. *Nir Kshetri*, "Blockchain’s roles in strengthening cybersecurity and protecting privacy", Telecommunications Policy, vol. 41, issue 10, November 2017, <https://doi.org/10.1016/j.telpol.2017.09.003> [↑](#footnote-ref-77)
78. *Ben Cole*, “The ‘supply chain of trust’ inherent to IoT data security”, IoT Agenda, 28 November 2016, <https://internetofthingsagenda.techtarget.com/video/The-supply-chain-of-trust-inherent-to-IoT-data-security> [↑](#footnote-ref-78)
79. *Gartner*, “Cloud Access Security Brokers (CASBs)”, <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs> [↑](#footnote-ref-79)
80. *Gartner*, “The Gartner IT Security Approach for the Digital Age”, 12 June 2017, <https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/> [↑](#footnote-ref-80)
81. *Gartner*, “Gartner Keynote: Leverage Automation for Modern Security”, 17 June 2019, <https://www.gartner.com/smarterwithgartner/gartner-keynote-leverage-automation-for-modern-security/> [↑](#footnote-ref-81)
82. *Ian Levy and Maddy S.*, “Active Cyber Defence - The Second Year”, United Kingdom National Cyber Security Centre, 15 July 2019, <https://www.ncsc.gov.uk/files/Active%20Cyber%20Defence-The%20Second%20Year%20(2).pdf> [↑](#footnote-ref-82)
83. *Соединенное Королевство*, Документ [SG2RGQ/175](https://www.itu.int/md/D18-SG02.RGQ-C-0175), ""Принятие последующих мер по результатам исследования реализации Программы активной киберзащиты сетей органов правительства Соединенного Королевства" [↑](#footnote-ref-83)
84. *NRD Cyber Security (CS) (Литва)*, Документ [2/172](https://www.itu.int/md/D18-SG02-C-0172), "Развитие национальных и секторальных CSIRT как способ укрепления среды кибербезопасности, по данным за 2019 год" [↑](#footnote-ref-84)
85. *Guardtime AS (Эстония)*, Документ [SG2RGQ/32](https://www.itu.int/md/D18-SG02.RGQ-C-0032), "На пути к киберустойчивости – роль национальных киберучений" [↑](#footnote-ref-85)
86. <https://en.wikipedia.org/wiki/Pseudonymization> [↑](#footnote-ref-86)
87. Принцип "конфиденциальность по замыслу" применялся и в существующей архитектуре, однако его значение была вторичным. Данный подход начал получать широкое распространение после того, как в середине 1990-х годов о ней упомянула д-р Энн Кавукян, Уполномоченный по вопросам информации и неприкосновенности частной жизни провинции Онтарио, Канада. [↑](#footnote-ref-87)
88. *Бразилия*, Документ [SG2RGQ/143](https://www.itu.int/md/D18-SG02.RGQ-C-0143), "Принятие общего закона о защите данных в Бразилии" [↑](#footnote-ref-88)
89. *Китай*, Документ [2/156](https://www.itu.int/md/D18-SG02-C-0156), "Опыт работы по защите персональных данных" [↑](#footnote-ref-89)
90. *Республика Корея*, Документ [2/342](https://www.itu.int/md/D18-SG02-C-0342), "Внесение Кореей существенной поправки в закон о защите данных и ее последствия" [↑](#footnote-ref-90)
91. *Республика Корея*, Документ [SG2RGQ/268](https://www.itu.int/md/D18-SG02.RGQ-C-0268), "Защита персональных данных в рамках принятия мер в ответ на пандемию COVID-19 (опыт Кореи)" [↑](#footnote-ref-91)
92. *Proge-Software (Италия)*, Документ [SG2RGQ/25](https://www.itu.int/md/D18-SG02.RGQ-C-0025), "Конфиденциальность данных и облачные вычисления…обеспечение соответствия" [↑](#footnote-ref-92)
93. *European Union*, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [↑](#footnote-ref-93)
94. *European Union Agency for Network and Information Security (ENISA)*, “Privacy and Data Protection by Design – from policy to engineering”, December 2014, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport> [↑](#footnote-ref-94)
95. *United States Federal Trade Commission*, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policy-makers”, March 2012,<https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> [↑](#footnote-ref-95)
96. *Agencia Española Protección Datos (AEPD)*, “A Guide to Privacy by Design”, October 2019, <https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf> [↑](#footnote-ref-96)