Организация Объединенных Наций A/AC.291/9/Add.1

Генеральная Ассамблея

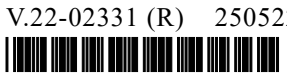
Distr.: General
21 April 2022
Russian
Original: Arabic/English/French/
Russian/Spanish

Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях
Вторая сессия
Вена, 30 мая — 10 июня 2022 года

Подборка представленных государствами-членами предложений и материалов, касающихся положений о криминализации, общих положений и положений о процессуальных мерах и правоохранительной деятельности всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

Добавление

V.22-02331 (R) 250522 310522



Просьба отправить на вторичную переработку

Содержание

		Стр.
III.	Общие положения	3
	Ангола	3
	Австралия	3
	Бразилия	3
	Бурунди	6
	Канада	8
	Колумбия	9
	Египет	11
	Сальвадор	13
	Европейский союз и его государства-члены	14
	Гана	16
	Иран (Исламская Республика)	18
	Япония	20
	Мексика	21
	Новая Зеландия	22
	Норвегия	23
	Российская Федерация, также от имени Беларуси, Бурунди, Китая, Никарагуа и Таджикистана	23
	Южная Африка	26
	Швейцария	29
	Соединенное Королевство Великобритании и Северной Ирландии	30
	Объединенная Республика Танзания	31
	Соединенные Штаты Америки	32
	Венесуэла (Боливарианская Республика)	34
	Вьетнам	35

III. Общие положения

Ангола

[Подлинный текст на английском языке]
[8 апреля 2022 года]

Общие положения

Определения: киберпреступность, электронные доказательства, перехват, компьютерная система, компьютерные данные, метаданные, технические параметры трафика, поставщики услуг, компьютерная программа, сеть электронного обмена информацией, критическая инфраструктура, топография, полупроводниковое изделие, суверенитет киберпространства.

Дополнительные сведения о предложенных здесь понятиях содержатся в упомянутых выше региональных и международных правовых документах[1].

Австралия

[Подлинный текст на английском языке]
[13 апреля 2022 года]

Общие положения должны включать:

- указание цели, четко ориентированной на борьбу с киберпреступностью;
- конкретную и четко определенную сферу применения;
- согласованные определения, которые должны обсуждаться и согласовываться только после достижения договоренности об основных статьях Конвенции.

В отличие от физического пространства, в киберпространстве в силу его природы дополнительно затруднено применение и толкование норм и принципов международного права, включая принцип государственного суверенитета, а также применение территориальной юрисдикции. Австралия предлагает, чтобы обсуждение того, как эти правовые вопросы могут быть рассмотрены в Конвенции, продолжалось параллельно с разработкой основных положений.

Бразилия

[Подлинный текст на английском языке]
[8 апреля 2022 года]

Глава I
Общие положения

Статья 1
Цель[2]

Целью настоящей Конвенции является предупреждение и противодействие киберпреступности путем определения:

[1] Примечание Секретариата: имеются в виду документы, включенные в другой подраздел: Конвенция Африканского союза о кибербезопасности и защите персональных данных, Конвенция Совета Европы о киберпреступности, Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Организации Объединенных Наций против коррупции.

[2] *Источник:* первоначальное предложение, представленное Бразилией.

a) действий, которые Стороны считают правонарушениями и за совершение которых на территории Сторон предусматривается наказание;

b) процессуальных полномочий для своевременного принятия мер национальными органами; и

c) международного сотрудничества.

Статья 2
Сфера применения[3]

1. Настоящая Конвенция применяется к:

a) предупреждению, выявлению, пресечению и расследованию киберпреступлений, уголовному преследованию за них и вынесению по ним судебных решений;

b) осуществлению мер по смягчению последствий киберпреступности; и

c) любому соответствующему международному сотрудничеству по предотвращению и противодействию киберпреступности.

2. Для цели осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений был причинен имущественный вред.

Статья 3
Термины[4]

Для целей настоящей Конвенции:

a) «затронутое лицо» означает любое лицо, поставщика услуг или другого субъекта, на которого повлияла или может повлиять выдача любого распоряжения в этой части;

b) «компьютерные данные» включают любое представление данных или информации, которые были или могут быть сохранены, переданы или иным образом обработаны в компьютерной системе. Они включают трафик абонентов и содержание информации;

c) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы или другого программного обеспечения хранит, передает или иным образом обрабатывает компьютерные данные;

d) «содержание информации» означает любые компьютерные данные, хранящиеся у поставщика услуг, или любую другую информацию, кроме технических параметров трафика или абонентских данных, такую как текст, голос, видео, изображения и звук или данные о содержании обмена информацией;

e) «сеть электронного обмена информацией» означает системы передачи, основанные или не основанные на постоянной инфраструктуре или централизованных административных мощностях, и, где это применимо, оборудование для коммутации или маршрутизации и другие ресурсы, включая неактивные элементы сети, которые позволяют передавать сигналы по проводам, радиоволнам, оптическим или иным электромагнитным способом, включая спутниковые сети, стационарные и мобильные сети и электрические кабельные системы,

[3] Предложение Китая и России с изменениями, внесенными Бразилией.

[4] Совещание группы экспертов по обновлению Типового закона Управления Организации Объединенных Наций по наркотикам и преступности о взаимной правовой помощи в вопросах уголовного правосудия (на 9 марта 2022 года процесс продолжается); с незначительными изменениями, внесенными Бразилией.

если они используются для целей передачи сигналов, независимо от типа передаваемой информации;

f) «электронное доказательство» означает любые данные или информацию, которые создаются, хранятся, передаются или иным образом обрабатываются в электронной форме и которые могут быть использованы для доказательства или опровержения того или иного факта в ходе судебного разбирательства;

g) «электронное наблюдение» означает:

i) мониторинг, перехват, копирование и манипулирование, осуществляемые в отношении сообщений, данных или сигналов, которые хранились, передавались или передаются с помощью электронных средств; или

ii) мониторинг или фиксацию деятельности с помощью электронных средств;

h) «поставщик услуг» означает:

i) любое лицо, государственную или частную организацию, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы или иным образом облегчает обмен информацией посредством сети электронного обмена информацией; или

ii) любое другое лицо, государственную или частную организацию, которая хранит или иным образом обрабатывает компьютерные данные от имени такой службы или пользователей услуг такой службы;

i) «абонентские данные» означают любые компьютерные данные, собираемые поставщиком услуг в ходе его обычной деятельности, относящиеся к имени, дате рождения, почтовому или географическому адресу, сведения о счетах и платежах, идентификаторам устройств, номеру телефона или адресу электронной почты, а также любую другую информацию, такую как IP-адрес, использовавшийся в момент создания учетной записи, которая может служить для идентификации абонента или клиента, а также тип предоставляемой услуги и продолжительность действия договора с поставщиком услуг, кроме технических параметров трафика или содержания информации;

j) «технические параметры трафика» означают любые компьютерные данные, собираемые поставщиком услуг в ходе обычной деятельности, связанные с:

i) типом предоставляемой услуги и ее продолжительностью, если это касается технических данных и данных, идентифицирующих соответствующие технические меры или интерфейсы, используемые абонентом или клиентом или предоставленные ему, а также данных, связанных с подтверждением использования услуги, за исключением паролей или других средств аутентификации, используемых вместо пароля, которые предоставляются пользователем или создаются по просьбе пользователя; или

ii) началом и окончанием сеанса, в ходе которого пользователь имел доступ к услуге, например дата и время использования услуги или время начала и конца сеанса, в ходе которого услуга использовалась; или

iii) метаданные об обмене информацией в том виде, в каком она обрабатывается в сети электронного обмена информацией в целях передачи, распространения содержания электронной информации или обмена им, включая данные, используемые для отслеживания и идентификации источника и адресата сообщения, данные о местонахождении оконечного оборудования, обрабатываемые в контексте предоставления услуг по обмену информацией, а также дата, время, продолжительность и тип обмена информацией.

Бурунди

[Подлинный текст на французском языке]
[8 апреля 2022 года]

Глава I. Определения

Для целей настоящей Конвенции:

a) «неправомерный доступ» означает умышленный противоправный полный или частичный доступ к сети электронного обмена информацией, информационной системе или оконечному оборудованию;

b) «шифрование» означает любой метод преобразования цифровых данных в нечитаемый формат с помощью криптологических методов;

c) «криптология» означает науку о защите информации и обеспечении ее безопасности;

d) «киберпреступление» означает любое незаконное деяние, совершенное с помощью компьютерной системы или сети либо любой другой физической сети, подключенной к информационной системе или связанной с ней;

e) «киберпространство» означает комплекс оцифрованных данных, совокупно формирующих информационно-коммуникационную среду, подключенную к мировой сети автоматизированного оборудования обработки цифровых данных;

f) «кибербезопасность» означает комплекс технических, организационных, правовых, финансовых, кадровых и процедурных мер по предотвращению, защите и сдерживанию, а также иных действий, позволяющих достичь этих целей;

g) «электронный обмен информацией» означает отправку, передачу или прием знаков, сигналов, текста, изображений, звуков или видеозаписей с помощью электромагнитных, оптических или любых других средств;

h) «персональные данные» означают любую информацию любого рода, независимо от носителя, на котором она хранится, включая звук и изображение, относящуюся к физическому лицу, прямо или косвенно идентифицированному или идентифицируемому посредством указания идентификационного номера либо одного или нескольких факторов, присущих физической, физиологической, генетической, психической, культурной, социальной или экономической идентичности этого лица;

i) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию;

j) «электромагнитный» означает результат связанных колебаний электрического поля и магнитного поля, которые изменяются во времени;

k) «поставщик услуг» означает физическое или юридическое лицо, которое предоставляет одну или несколько услуг пользователям телекоммуникационной системы;

l) «информация» означает любой элемент знаний, который может быть воспроизведен с помощью устройств для его использования, сохранения, обработки или передачи. Информация может быть выражена в письменной, визуальной, звуковой, цифровой и других формах;

m) «критическая инфраструктура» означает инфраструктуру, которая необходима для оказания услуг, которые жизненно важны для обеспечения общественной безопасности, экономической стабильности, национальной

безопасности и международной стабильности, а также для поддержания работоспособности и восстановления критически важного киберпространства. Объекты критической инфраструктуры государства состоят из подключенных к интернет-сетям служб, связанных со здравоохранением, внутренней и внешней безопасностью, обороной, финансами и транспортом;

n) «неправомерный перехват» означает противоправный или несанкционированный доступ к данным в сети электронного обмена информацией, в информационной системе или в оконечном оборудовании;

o) «международный шлюз» — общее название устройства, соединяющего два разных типа компьютерных сетей, например локальную сеть и сеть Интернет;

p) «электронные платежные средства» означают средства, с помощью которых держатель может совершать онлайновые электронные платежные операции;

q) «фишинг» означает форму мошенничества, совершаемого по электронной почте, которое заключается в том, что отправляется электронное письмо якобы от имени известной и признанной компании, с тем чтобы убедить получателей изменить или обновить их банковские реквизиты на интернет-страницах, имитирующих страницы компании, образ которой был использован для целей мошенничества;

r) «детская порнография» означает сделанное или произведенное с помощью электронных, механических или иных средств любое визуальное отображение откровенных сексуальных действий, включая любую фотографию, фильм, видео или изображение, при этом:

i) в производстве такого визуального отображения участвует несовершеннолетнее лицо;

ii) таким визуальным отображением является цифровое изображение, компьютерное изображение или созданное на компьютере изображение несовершеннолетнего лица, участвующего в откровенных сексуальных действиях, или изображения половых органов несовершеннолетнего лица, которые производятся или используются главным образом в сексуальных целях и эксплуатируются с ведома или без ведома ребенка;

iii) такое визуальное отображение создается, адаптируется или изменяется, чтобы создать впечатление, что несовершеннолетнее лицо участвует в откровенных сексуальных действиях;

s) «поставщики услуг» означают операторов мобильной связи, интернет-провайдеров и операторов инфраструктуры;

t) «компьютерная программа» означает набор инструкций, выполняемых компьютером для достижения ожидаемого результата;

u) «расизм и ксенофобия в информационно-коммуникационных технологиях» означает любой письменный материал, любое изображение или любое другое представление идей или теорий, в которых пропагандируются или поощряются ненависть, дискриминация или насилие либо содержится подстрекательство к такой ненависти, дискриминации или насилию против какого-либо лица или группы лиц на основании расы, цвета кожи, родового, национального или этнического происхождения или религии;

v) «рассылка спама» означает массовую безадресную рассылку коммерческих сообщений по электронной почте лицам, которые не давали отправителю разрешения на получение таких сообщений, с намерением совершить хищение;

w) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных;

x) «ИКТ» означает информационно-коммуникационные технологии.

Канада[5]

[Подлинный текст на английском языке]
[9 апреля 2022 года]

Общие положения

Цель

Цель настоящей Конвенции заключается в содействии сотрудничеству в деле повышения эффективности предупреждения и расследования киберпреступлений и уголовного преследования за них.

Сфера применения

Настоящая Конвенция применяется, если не указано иное и при условии соблюдения соответствующих гарантий:

a) к содействию принятию и укреплению законодательных и иных мер по предупреждению киберпреступлений и серьезных преступлений, часто совершаемых с использованием компьютерных систем, которые признаны таковыми в соответствии с Конвенцией, расследованию их и уголовному преследованию за них;

b) к поощрению, облегчению и поддержке международного сотрудничества и помощи в связи с предупреждением преступлений, признанных таковыми в соответствии с настоящей Конвенцией, расследованием их и уголовным преследованием за них;

c) к поощрению, облегчению и поддержке оказания эффективной и действенной взаимной правовой помощи в связи с электронными доказательствами, относящимися к правонарушениям, признанным таковыми в соответствии с настоящей Конвенцией, и любым другим уголовно наказуемым деянием; и

d) к поощрению, облегчению и поддержке оказания технической помощи в предупреждении киберпреступности и борьбе с ней.

Условия и гарантии

1. Каждое Государство-участник обеспечивает установление, осуществление и применение положений настоящей Конвенции в соответствии с условиями и гарантиями, предусмотренными нормами его внутреннего законодательства, в полной мере обеспечивающими защиту прав и свобод человека, включая права, вытекающие из обязательств, закрепленных в Международном пакте о гражданских и политических правах и других применимых международных договорах о правах человека, и включающими принципы верховенства права, законности, необходимости и соразмерности.

2. Такие условия и гарантии с учетом характера соответствующих процедур и полномочий включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничения сферы и сроков действия процедур или полномочий.

3. Каждое Государство-участник осуществляет меры, направленные на то, чтобы лучше понять связи между гендерным фактором и киберпреступностью, в том числе различия в воздействии киберпреступности на положение женщин и мужчин. Эти меры направлены на поощрение равенства между женщинами и мужчинами и расширение прав и возможностей женщин, в том числе путем

[5] Примечание Секретариата: Канада представила также список определений. URL: www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

учета этого фактора в соответствующих законах, при разработке политики, в исследованиях, проектах и программах, в надлежащих случаях и в соответствии с основополагающими принципами внутреннего законодательства.

4. Меры, изложенные в настоящей Конвенции, толкуются и применяются таким образом, чтобы не препятствовать свободе выражения мнений, включая свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно, посредством печати или художественных форм выражения, или иными способами по своему выбору, а также применимым правам, касающимся уважения частной жизни и защиты данных. Толкование и применение этих мер осуществляются в соответствии с международно признанными принципами недискриминации.

Участие и покушение

1. Каждое Государство-участник принимает необходимые законодательные и другие меры, с тем чтобы признать в качестве уголовно наказуемого деяния, в соответствии со своим внутренним законодательством, участие в любом качестве, например в качестве сообщника, пособника или подстрекателя, в совершении какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

2. Каждое Государство-участник может принять необходимые законодательные и другие меры, с тем чтобы признать в качестве уголовно наказуемого деяния, в соответствии со своим внутренним законодательством, любое покушение на совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

3. Каждое Государство-участник может принять необходимые законодательные и другие меры, с тем чтобы признать в качестве уголовно наказуемого деяния, в соответствии со своим внутренним законодательством, приготовление к совершению какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

Ответственность юридических лиц

1. Каждое Государство-участник принимает необходимые законодательные и иные меры, соответствующие его правовым принципам, для установления ответственности юридических лиц за участие в совершении преступлений, предусмотренных настоящей Конвенцией.

2. В зависимости от правовых принципов Государства-участника ответственность юридических лиц может быть уголовной, гражданско-правовой или административной.

3. Привлечение к такой ответственности не исключает привлечения к уголовной ответственности физических лиц, совершивших преступления.

4. Каждое Государство-участник, в частности, обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии с настоящей статьей, эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций, включая денежные санкции.

Колумбия

[Подлинный текст на испанском языке]
[9 апреля 2022 года]

Общие положения

Государства-участники, занимаясь предупреждением и пресечением киберпреступности во всех ее проявлениях, поощряют и обеспечивают полное

соблюдение прав женщин и девочек, уделяя при этом особое внимание гендерным вопросам, в частности гендерному насилию, включая насилие в отношении женщин и девочек.

Государства-участники, занимаясь предупреждением и пресечением киберпреступности во всех ее проявлениях, поощряют и обеспечивают соблюдение прав человека и основных свобод. Все положения настоящей конвенции или документа должны толковаться и применяться согласно соответствующим международным обязательствам в области прав человека.

Определения

В соответствии с консенсусом, достигнутым в ходе первого раунда переговоров в отношении необходимости согласования технически нейтральной терминологии и определений, и в соответствии с комментариями, сделанными группой Совета Европы в отношении Будапештской конвенции, определения, изложенные как в Будапештской конвенции, так и во Втором протоколе к ней, являются актуальными, достаточными и адаптируемыми к развитию технологий и, соответственно, могут быть предложены Специальному комитету.

В этой связи предлагаются следующие определения:

a) компьютерная система: «любое устройство или группа соединенных [...] устройств, [...] которые по команде программы производят автоматическую обработку данных»;

b) компьютерные данные: «любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующая программа, дающую компьютерной системе команду выполнить какую-либо функцию»;

c) поставщик услуг: «любая государственная или частная организация, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы, а также любая другая организация, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей такой службы»;

d) технические параметры трафика: «любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер, продолжительность обмена информацией или тип соответствующей услуги»;

e) центральный орган: «орган или органы, назначенные в соответствии с договором или договоренностью о взаимной помощи, опирающимся на единообразное или основанное на взаимности законодательство, действующим в заинтересованных сторонах, или, при отсутствии такового, орган или органы, назначенный Стороной [...], ответственный за направление просьб о взаимной помощи и ответы на них, исполнение таких просьб или их передачу компетентным органам для их исполнения»;

f) компетентный орган: «судебный, административный или иной правоохранительный орган, который в соответствии с внутренним законодательством уполномочен отдавать распоряжение об исполнении мер, санкционировать исполнение мер или исполнять их [...] в целях сбора или представления доказательств в рамках конкретных уголовных расследований или разбирательств»;

g) чрезвычайная ситуация: «ситуация, в которой существует значительный и неизбежный риск для жизни или безопасности любого физического лица»;

h) персональные данные: «информация, относящаяся к физическому лицу, которое идентифицировано или может быть идентифицировано»;

i) передающая сторона: «Сторона, передающая данные в ответ на просьбу или в рамках работы совместной следственной группы, или [...] Сторона, на территории которой находится поставщик услуг передачи данных или организация, предоставляющая услуги по регистрации доменных имен»;

j) сведения об абонентах: «любая имеющаяся у поставщика услуг информация [...] о его абонентах, кроме технических параметров трафика или содержания информации, с помощью которой можно определить: [...] вид используемой услуги обмена информацией, принятые с этой целью меры технического обеспечения и период оказания услуги [...], личность абонента, его почтовый или географический адрес, телефон [...], сведения о счетах и платежах [...], любые другие сведения о месте установки оборудования для обмена информацией».

Египет

[Подлинный текст на арабском языке]
[8 апреля 2022 года]

Глава I. Общие положения

Предлагается включить в эту главу цели конвенции, используемые термины, защиту суверенитета и сферу применения в следующих формулировках.

Статья 1. Цели

Целью настоящей Конвенции является укрепление сотрудничества между государствами — членами Организации Объединенных Наций для противодействия использованию информационно-коммуникационных технологий в преступных целях. Она направлена на пресечение действий, угрожающих целостности и конфиденциальности информационно-коммуникационных технологий, криминализацию неправомерного использования информационно-коммуникационных технологий в незаконных целях, облегчение расследования преступлений и привлечения к ответственности виновных, а также принятие мер по ликвидации последствий таких преступлений. Эти меры включают приостановление операций, связанных с активами, полученными в результате совершения любых противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, и конфискацию и возвращение доходов от таких противоправных деяний. Для этой цели в Конвенции предусмотрены полномочия, достаточные для эффективного противодействия связанным с информационно-коммуникационными технологиями преступлениям путем создания механизмов международного сотрудничества для облегчения выявления и расследования таких преступлений, привлечения к ответственности виновных и выдачи правонарушителей.

Статья 2. Термины

Указанные ниже термины, используемые в настоящей Конвенции, имеют следующее значение:

a) информационные технологии: любое физическое или нематериальное средство или группа взаимосвязанных или несвязанных средств, используемых для хранения, упорядочивания, организации, съема, обработки, получения информации и обмена ею в соответствии с хранящимися в них командами и инструкциями, включая все соответствующие каналы ввода и выхода, по проводам или беспроводной связи, в системе или сети;

b) поставщик услуг: любое физическое или юридическое лицо, государственное или частное, которое предоставляет абонентам услуги обмена информацией посредством информационных технологий или которое обрабатывает или хранит информацию от имени службы обмена информацией или ее пользователей;

c) данные: вся информация, которая может храниться, обрабатываться, генерироваться и передаваться с помощью информационных технологий, например цифры, буквы, символы и т. д.;

d) информационная система: набор программ и инструментов, предназначенных для обработки и управления данными и информацией;

e) информационная сеть: две или более информационные системы, которые связаны между собой для получения информации и обмена ею;

f) сайт: место в информационной сети, где по определенному адресу размещается информация;

g) фиксация: просмотр или получение данных или информации;

h) администратор сайта: любое лицо, которое отвечает за: организацию, мониторинг, обслуживание одного или нескольких сайтов в информационной сети или управление ими, включая права доступа различных пользователей на сайте; дизайн сайта; создание и организацию страниц или содержание информации на сайте; сайт;

i) личный кабинет: набор сведений о физическом или юридическом лице, который предоставляет этому лицу исключительное право доступа к услугам посредством сайта или информационной системы или использования таких услуг;

j) электронная почта: средство обмена электронными сообщениями между несколькими физическими или юридическими лицами по определенному адресу посредством информационной сети или других электронных средств связи, компьютеров и т. д.;

k) перехват: просмотр или получение данных или информации с целью их несанкционированного съема, отключения, хранения, копирования, записи, изменения содержания, противоправного использования, переадресации или перенаправления в незаконных целях;

l) проникновение: доступ к информационной системе, компьютеру, информационной сети и т. д., который является несанкционированным, нарушающим положения соответствующей лицензии или незаконным;

m) содержание информации: любые данные, которые сами по себе или в сочетании с другими данными или информацией приводят к формированию информации или выявлению тенденции, направления, понятия или значения данных или к ссылке на другие данные;

n) цифровое доказательство: любая доказательственная электронная информация, которая хранится или передается, извлекается или получается из компьютеров, информационных сетей и т. д. и которая может быть собрана и проанализирована с помощью специальных технологических устройств, программного обеспечения или приложений;

o) трафик (технические параметры трафика): данные, которые производятся информационной системой и отображают источник, конечную точку, отправителя, адресата, маршрут, время, дату, размер и продолжительность обмена информацией, а также тип услуги.

Статья 3. Защита суверенитета

1. Государства-участники выполняют свои обязательства в рамках настоящей Конвенции в соответствии со своим внутренним законодательством или конституционными принципами, согласно принципам суверенного равенства государств и невмешательства во внутренние дела других государств.

2. Настоящая Конвенция не позволяет какому-либо Государству-участнику осуществлять на территории другого государства юрисдикцию и функции, которыми наделены исключительно органы этого другого государства согласно его внутреннему законодательству.

Статья 4. Сфера применения

1. Настоящая Конвенция должна применяться для пресечения указанных в ней преступлений, если в ней не предусмотрено иное.

2. Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен материальный вред.

3. Каждое Государство-участник рассматривает возможность ограничения своей оговорки, чтобы обеспечить широкое применение вышеуказанных мер.

Сальвадор

[Подлинный текст на испанском языке]
[12 апреля 2022 года]

Терминология

По мнению нашего правительства, в документ необходимо включить ряд уже существующих определений, которые должны быть сформулированы таким образом, чтобы при переводе на шесть официальных языков Организации Объединенных Наций передавались правильные понятия и не возникало никаких сомнений относительно того, о каком понятии идет речь. В этой связи предлагается, чтобы при разработке определений Специальный комитет взял за основу определения, уже закрепленные в документах, с которыми знакомы Государства-члены, таких как Будапештская конвенция и Конвенция Организации Объединенных Наций против транснациональной организованной преступности.

В частности, мы считаем, что необходимо добавить определения следующих терминов:

a) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных;

b) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какое-либо действие;

c) «поставщик услуг» означает любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы, а также любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей такой службы;

d) «технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер, продолжительность обмена информацией или тип соответствующей услуги.

Необходимо добавить вместо «детской порнографии» определение «материалов, содержащих изображение надругательства над детьми», ключевыми словами которого являются производство, воспроизведение, распространение, публикация, импорт, экспорт, предложение, финансирование, продажа, маркетинг, рассылка таких материалов и обладание ими, и в этом определении должно быть учтено участие кажущегося несовершеннолетним лица в откровенных сексуальных действиях или реалистичные изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях; оно должно также

включать не только изображение детей, участвующих в откровенных сексуальных действиях, но и действия, при выполнении которых дети и подростки изображаются в обнаженном виде.

Европейский союз и его государства-члены

[Подлинный текст на английском языке]
[6 апреля 2022 года]

Глава I. Общие положения

Статья 1
Цель

Цели настоящей Конвенции обеспечивают высокий уровень защиты прав человека и основных свобод и заключаются в следующем:

a) содействие принятию и укрепление мер, направленных на повышение эффективности и действенности предупреждения киберпреступности и борьбу с ней;

b) поощрение и облегчение международного сотрудничества;

c) обеспечение высокого уровня защиты прав потерпевших; и

d) поддержка наращивания потенциала и оказание технической помощи в борьбе с киберпреступностью.

Статья 2
Термины

Для целей настоящей Конвенции:

a) «центральный орган» означает орган или органы, назначенные для отправки просьб об оказании взаимной помощи, исполнения таких просьб или их передачи для исполнения компетентным органам, а также для ответа на такие просьбы;

b) «киберпреступность» для целей настоящей Конвенции означает деяния, как это определено в статьях 5–10 настоящей Конвенции;

c) «компетентный орган» означает судебный, административный или иной правоохранительный орган, который в соответствии с внутренним законодательством уполномочен отдавать распоряжение об исполнении мер, санкционировать исполнение мер или исполнять их согласно настоящей Конвенции в рамках конкретных уголовных расследований или разбирательств;

d) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных;

e) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию;

f) «персональные данные» означают информацию, относящуюся к физическому лицу, которое идентифицировано или может быть идентифицировано;

g) «региональная организация экономической интеграции» означает организацию, созданную суверенными государствами какого-либо региона, которой ее государства-члены передали полномочия по вопросам, регулируемым настоящей Конвенцией, и которая должным образом уполномочена в соответствии с ее внутренними процедурами подписывать, ратифицировать, принимать,

утверждать настоящую Конвенцию или присоединяться к ней; ссылки в настоящей Конвенции на «государства-участники» относятся к таким организациям в пределах их компетенции;

h) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы; и

ii) любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей такой службы;

i) «абонентские данные» означают любую содержащуюся в виде компьютерных данных или в любой другой форме информацию, хранящуюся у поставщика, о его абонентах, кроме технических параметров трафика или содержания информации, с помощью которой можно определить:

i) вид используемой услуги обмена информацией, принятые с этой целью меры технического обеспечения и период оказания услуги;

ii) личность абонента, его почтовый или географический адрес, номер телефона и других средств связи и сведения о счетах и платежах, предоставляемые в рамках соглашения или договоренности об обслуживании;

iii) любые другие сведения об оборудовании для обмена информацией и месте его установки, предоставляемые в рамках соглашения или договоренности об обслуживании;

j) «технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, данные, размер, продолжительность обмена информацией или тип соответствующей услуги;

k) «противоправные деяния» означают предусмотренные статьями 5–10 настоящей Конвенции деяния, которые не разрешены владельцем или другим правообладателем компьютерной системы или ее части или не допускаются внутренним законодательством.

Статья 3
Сфера применения

Настоящая Конвенция, если в ней не указано иное, применяется к:

a) предупреждению и расследованию уголовных преступлений, признанных таковыми в соответствии со статьями 5–10 настоящей Конвенции, и преследованию за них;

b) сбору электронных доказательств совершения уголовного преступления, признанного таковым в соответствии со статьями 5–10 настоящей Конвенции, на основе мер, изложенных в главе III настоящей Конвенции;

c) предоставлению и осуществлению технической помощи и наращивания потенциала в вопросах, охватываемых настоящей Конвенцией.

Статья 4
Последствия действия Конвенции

1. Если два или более государств-участников уже заключили соглашение или договор по вопросам, рассматриваемым в настоящей Конвенции, или иным образом установили свои отношения по таким вопросам либо если они сделают это в будущем, они имеют также право применять это соглашение или договор либо регулировать эти отношения соответствующим образом. Однако если

государства-участники устанавливают свои будущие отношения применительно к вопросам, рассматриваемым в настоящей Конвенции, иначе, чем это предусмотрено в ней, они делают это таким образом, чтобы это не противоречило целям и принципам Конвенции.

2. Что касается государств-участников, которые являются членами какой-либо региональной организации экономической интеграции, то эти государства-участники могут в своих взаимоотношениях применять правила этой региональной организации экономической интеграции, регулирующие вопросы, рассматриваемые в настоящей Конвенции.

3. Ничто в настоящей Конвенции не затрагивает других прав, ограничений, обязательств и ответственности Стороны согласно международному праву, в частности праву прав человека.

Гана

[Подлинный текст на английском языке]
[12 апреля 2022 года]

Глава I
Общие положения

Статья 1
Цель

Целью настоящей Конвенции является поощрение и облегчение международного сотрудничества, а также усиление мер по предотвращению использования информационно-коммуникационных технологий в преступных целях и противодействию такому использованию.

Статья 2
Термины

Для целей настоящей Конвенции:

a) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных;

b) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию;

c) «содержание информации» означает коммуникационное содержание обмена информацией, т. е. смысл или цель обмена информацией или сообщения или сведений, передаваемых при обмене информацией, кроме технических параметров трафика;

d) «ребенок» означает лицо, не достигшее 18-летнего возраста. Однако любая Сторона может запросить установление и более низкого возрастного предела, но не ниже 16 лет;

e) «критическая информационная инфраструктура» означает компьютер или компьютерную систему, определенные Государством-членом в своем внутреннем законодательстве как крайне важные для национальной безопасности или экономического и социального благополучия граждан;

f) «запрещенные интимные изображения и визуальная регистрация» включают:

i) движущееся или неподвижное изображение, изображающее:

a. лицо, занимающееся интимной сексуальной деятельностью, которой не принято заниматься публично; или

b. генитальную или анальную область человека, когда генитальная или анальная область обнажена или прикрыта только нижним бельем; и

ii) изображение, которое было изменено таким образом, чтобы казаться содержащим любую из упомянутых в пункте (i) областей, даже если эта область была затемнена цифровым способом, если человек изображен в сексуально вызывающем виде;

g) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы; и

ii) любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей такой службы;

h) «абонент» означает клиента или пользователя сети электронного обмена информацией, службы электронного обмена информацией или службы вещания;

i) «информация об абонентах» означают любую имеющуюся у поставщика услуг информацию о его абонентах, хранящуюся в виде компьютерных данных или в любой другой форме, кроме технических параметров трафика или содержания информации, с помощью которой возможно определить:

i) тип используемой услуги обмена информацией, меры технического обеспечения, принятые в отношении услуги обмена информацией, и период оказания услуги;

ii) личность, почтовый или географический адрес, номер телефона и других средств связи абонента, сведения о счетах и платежах, предоставляемые в рамках соглашения или договоренности об обслуживании; и

iii) любые другие сведения о месте установки оборудования для обмена информацией, предоставляемые в рамках соглашения или договоренности об обслуживании;

j) «технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер или продолжительность обмена информацией или тип соответствующей услуги.

Статья 3
Сфера применения

Настоящая Конвенция применяется, в соответствии с ее положениями, к:

a) предупреждению, расследованию и уголовному преследованию преступлений, признанных таковыми в соответствии со статьями 5–20;

b) сбор электронных доказательств совершения уголовного преступления;

c) предоставлению и осуществлению технической помощи и наращиванию потенциала в вопросах, охватываемых настоящей Конвенцией;

d) замораживанию, аресту, конфискации и возвращению доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 4
Защита суверенитета

1. Государства-члены осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств.

2. Ничто в настоящей Конвенции не наделяет Государство-член правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством.

Иран (Исламская Республика)

[Подлинный текст на английском языке]
[8 апреля 2022 года]

1. Общие положения

Несмотря на исключительные возможности, предоставляемые информационно-коммуникационными технологиями для развития наций, преступники все чаще используют эти технологии для того, чтобы вести незаконную деятельность и достигать противозаконных целей. Методы работы таких преступников становятся все более разнообразными и изощренными, а природа таких преступлений становится все более сложной. Зачастую преступления, совершаемые с использованием информационно-коммуникационных технологий, не знают географических границ, что превращает их в беспрецедентно острую проблему, которую необходимо решить государствам-членам. Поэтому сейчас как никогда необходима активизация коллективного реагирования и сотрудничества на международном уровне на прочной международно-правовой основе.

Смысл создания Специального комитета в соответствии с резолюцией 74/247 Генеральной Ассамблеи заключался в удовлетворении этой острой необходимости и в разработке международно-правового документа, который помогает принимать эффективные меры на различных уровнях в борьбе с использованием информационно-коммуникационных технологий в преступных целях. Для этого в общих положениях конвенции должны быть прописаны ее цели и определена сфера ее действия. В соответствии со сложившейся практикой и учитывая основополагающее значение соблюдения базовых принципов международного права в деле предупреждения преступлений, совершаемых с использованием информационно-коммуникационных технологий, и борьбы с ними в общих положениях таким принципам должен быть также посвящен предметный раздел. Определение в специальном разделе терминов, используемых в конвенции, необходимо для обеспечения общего понимания важных терминов и, в конечном итоге, положений конвенции.

1.1 Цели конвенции

С учетом вышесказанного Исламская Республика Иран подчеркивает, что целью конвенции должны быть укрепление, поддержка и облегчение международного сотрудничества в предупреждении использования информационно-коммуникационных технологий в преступных целях и борьбе с ним, в том числе для возвращения активов, усиления национальных мер, принимаемых в отношении таких преступлений и оказания помощи Государствам-участникам, в частности развивающимся странам, в борьбе с этими преступлениями, в том числе посредством экономического развития, предоставления технической помощи и передачи технологий. В этой связи необходимо учитывать технический контекст при устранении проблем и барьеров, таких как односторонние санкции и низкий уровень развития, которые подрывают способность государств эффективно

бороться с использованием информационно-коммуникационных технологий в преступных целях.

Следует также должным образом учитывать ответственность поставщиков услуг и других аналогичных лиц за сотрудничество с судебными и правоохранительными органами в целях обеспечения эффективных мер предупреждения и пресечения использования информационно-коммуникационных технологий в преступных целях.

Общее понимание преступных явлений и их меняющихся форм имеет огромное значение для принятия эффективных мер в отношении преступлений, совершаемых с помощью информационно-коммуникационных технологий, и поэтому конвенция должна также поощрять и облегчать обмен информацией, экспертными знаниями, специальными знаниями, опытом и примерами положительной практики.

Такие цели будут в полной мере достигнуты, если будет принят подход, предусматривающий для всех государств-членов общее будущее в киберпространстве с равными возможностями и без дискриминации.

1.2 Сфера применения конвенции

Конвенция должна охватывать преступления, которые зависят от информационно-коммуникационных технологий, такие как преступления против конфиденциальности и целостности систем и данных информационно-коммуникационных технологий и преступления против инфраструктуры информационно-коммуникационных технологий, а также преступления, совершаемые с помощью таких технологий, например оскорбление религиозных ценностей, подстрекательство к насилию, побуждение к убийству, распространение преступного и непристойного содержания и сексуальная эксплуатация детей. Тем не менее, в отношении преступлений, совершаемых с помощью информационно-коммуникационных технологий, может потребоваться индивидуальный подход, в котором учитываются разные факторы, связанные с различными формами преступлений, и возможные различия в элементах преступления, которые необходимо принимать во внимание при квалификации преступлений. Кроме того, в соответствующих случаях для определения сферы применения конвенции может потребоваться учет дополнительных элементов: тяжесть преступлений или наказания за них, а также то, были ли данные преступления совершены более чем в одном государстве.

1.3 Защита суверенитета

Исламская Республика Иран подтверждает, что в общие положения должны быть включены конкретные разделы о защите суверенитета, с тем чтобы усилия и меры по предупреждению использования информационно-коммуникационных технологий в преступных целях и борьбе с ним были последовательными и соответствовали основополагающим принципам международного права и принципам, изложенным в Уставе Организации Объединенных Наций, в частности принципам равенства суверенитета, территориальной целостности государств и невмешательства. Такая практика сложилась при разработке конвенций в области предупреждения и пресечения преступлений; в качестве примера можно привести термин «защита суверенитета», который используется в таких конвенциях, как Конвенция Организации Объединенных Наций против коррупции.

Исламская Республика Иран, как и раньше, настороженно относится к попыткам отрицать и игнорировать важность соблюдения таких принципов в борьбе с преступлениями, идущим вразрез со сложившейся практикой международного сообщества.

Япония

[Подлинный текст на английском языке]
[8 апреля 2022 года]

2. Общие положения

2.1 Цель

Мы поддерживаем три цели, изложенные на первой сессии Специального комитета в предложении Председателя: a) содействие принятию и укрепление мер предупреждения киберпреступности и борьбы с ней, b) поощрение, облегчение и укрепление международного сотрудничества; c) предоставление практических инструментов для расширения технической помощи и наращивания потенциала национальных органов власти.

2.2 Термины

Исходя из того, что конвенция будет эффективно использоваться долгое время, используемые в настоящей конвенции термины должны иметь четко определенные, технически нейтральные формулировки. Например, было бы неуместно давать определения для постоянно меняющихся технологий, таких как «бот-сеть».

Поэтому формулировки положений, содержащих определения, должны быть как можно более общими, понятными и емкими, включая при этом ссылки на действующие международные документы, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности. Мы считаем, что эта точка зрения в равной степени применима и к обсуждению других частей данной конвенции, таких как положения о криминализации.

2.3 Сфера применения

2.3.1. Сфера применения настоящей конвенции должна быть четко обозначена и основываться на положениях Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Конвенции Организации Объединенных Наций против коррупции.

2.3.2. Вопросы кибербезопасности и регулирования сети Интернет в данной конвенции рассматриваться не должны. Например, следующие меры окажут отрицательное воздействие на законную экономическую деятельность, будут препятствовать развитию технологий и выйдут за рамки мандата Специального комитета:

- установление в рамках данной конвенции норм безопасности;
- возложение на юридических и физических лиц обязательств по соблюдению таких норм или наложение санкций за нарушение таких норм;
- привлечение к ответственности юридических лиц, их представителей или создателей программного обеспечения, которые непреднамеренно участвуют в киберпреступлениях, совершаемых другими субъектами, не сознавая этого.

Мексика

[Подлинный текст на английском языке]
[13 апреля 2022 года]

Общие положения

В целях предотвращения возможных упущений и несоответствия положениям других будущих юридически обязательных документов, а также в соответствии с прецедентными международными и региональными договорами Мексика поддерживает включение в качестве начальных положений общих ссылок вместо исчерпывающих и подробных.

Что касается суверенитета, то для его подтверждения Мексика рекомендует в качестве примера воспользоваться формулировкой Рамочной конвенции Организации Объединенных Наций об изменении климата и включить в преамбулу общую ссылку следующего содержания: «Вновь подтверждая принцип суверенитета государств в международном сотрудничестве в деле противодействия использованию информационно-коммуникационных технологий в преступных целях».

Мексика рекомендует также включить в преамбулу пункт, в котором вновь подтверждается Устав Организации Объединенных Наций, применимость норм международного права и положений Всеобщей декларации прав человека и других обязательств в области прав человека, следующего содержания: «Вновь подтверждая цели и принципы Устава Организации Объединенных Наций, нормы международного права, положения Всеобщей декларации прав человека и других соответствующих документов в области прав человека».

Кроме того, рекомендуется включить общее положение о важности принятия государствами соответствующих мер по защите людей и, в частности, уязвимых групп: «Решили принять меры по предотвращению, реагированию, смягчению последствий, расследованию и уголовному преследованию для эффективной защиты людей и, в частности, уязвимых групп от использования информационно-коммуникационных технологий в преступных целях».

Как уже отмечалось в этом предложении ранее, для правительства Мексики будет крайне важно учесть в конвенции меры по предотвращению, реагированию, смягчению последствий, расследованию и уголовному преследованию.

В процессе переговоров по конвенции будет важно признать актуальность предыдущих международных юридически обязательных документов, в частности Конвенции Организации Объединенных Наций против транснациональной организованной преступности, представив на обсуждение конкретный опыт, который может быть использован для повышения эффективности международного сотрудничества в борьбе с киберпреступностью. В качестве общего положения необходимо включить соответствующий призыв к обеспечению слаженности действий в рамках всей системы Организации Объединенных Наций.

Мексика рекомендует также явным образом отметить в преамбуле возможности и преимущества информационно-коммуникационных технологий, чтобы ясно показать, что они не обязательно используются преступниками и в незаконных целях: «Признавая, что информационные, телекоммуникационные и цифровые технологии предоставляют возможности для активизации развития, преодоления неравенства и поддержки единения общества, обеспечения благосостояния, справедливости и соблюдения прав человека, и признавая важность содействия всеобщему доступу к этим технологиям и защиты их преимуществ».

Кроме того, Мексика разделяет заинтересованность в том, чтобы избежать чрезмерного использования гарантий, которые могут иметь ограничительный эффект и противоречить духу международного сотрудничества, которым необходимо руководствоваться в этом процессе.

«Цель настоящей Конвенции заключается в содействии двустороннему и многостороннему сотрудничеству и правовой помощи, включая межотраслевое сотрудничество, для предупреждения, пресечения, расследования, смягчения последствий и уголовного преследования использования информационно-коммуникационных технологий в преступных целях».

Мексика считает необходимым добавить другие общие положения по следующим вопросам: определение процедур урегулирования конфликтов; создание механизма обзора осуществления; обеспечение участия и сотрудничества со стороны других соответствующих заинтересованных сторон в поддержке усилий государств-участников по предупреждению использования информационно-коммуникационных технологий в преступных целях и борьбы с ним; признание важности сети Интернет для общественности и актуальности для целей конвенции подхода, предполагающего сетевой нейтралитет.

Новая Зеландия

[Подлинный текст на английском языке]
[8 апреля 2022 года]

Общие положения

8. По нашему мнению, общие положения должны включать следующее.

- *Цель.* При разработке эффективного договора наиболее применим последовательный, реалистичный и адресный подход к определению наших целей. Новая Зеландия считает, что нашей целью должно быть создание гармонизированной, современной и эффективной глобальной основы для сотрудничества и координации усилий государств по борьбе с растущей угрозой, которую киберпреступность представляет для частных лиц, бизнеса и правительств. Сюда относится оказание всем государствам поддержки и технической помощи в развитии потенциала и возможностей для борьбы с этими угрозами.

- *Сфера применения.* Сфера применения должна также быть четко заданной и определенной. Предложение Председателя, содержащееся в документе зала заседаний A/AC.291/CRP.8/Rev.1, представляет собой хорошую основу для определения сферы применения конвенции.

- *Принятые определения*. Определения должны быть точными, однозначными, не терять актуальности в будущем и, по возможности, быть основанными на соответствующих действующих международных и региональных документах.

- В любой всеобъемлющий документ должно также включаться общее положение, в котором подчеркивается защита прав человека и основных свобод и уважение верховенства права с уделением особого внимания позиции женщин, детей, коренных народов и уязвимых групп.

9. Мы слышали также мнение ряда государств, что для них важно включить положение о государственном суверенитете. Хотели бы отметить, что в контексте настоящей конвенции любое такое положение должно применяться с учетом некоторых критически важных отличий киберпространства от физической сферы. В частности: a) киберпространство сопряжено с элементом виртуальности, не имеющим четкой территориальной привязки; и b) при осуществлении действий в информационном пространстве могут быть задействованы объекты киберинфраструктуры, действующие одновременно на нескольких территориях и в различных юрисдикциях.

Приложение II
Определения

«Компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных.

«Компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютеру команду выполнить такую функцию.

«Материал, содержащий сцены сексуальной эксплуатации детей» означает любые материалы, в том числе в форме изображений, видео или прямой трансляции, которые изображают ребенка, совершающего реальные или смоделированные откровенные сексуальные действия, или любое изображение ребенка в преимущественно сексуальных целях.

«Имущество» означает любые активы, в том числе цифровые, будь то материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них.

Норвегия

[Подлинный текст на английском языке]
[8 апреля 2022 года]

Общие положения

1. В конвенции должны быть предусмотрены положения о принципиальной позиции в отношении защиты прав человека и основных свобод, включая право на неприкосновенность частной жизни и защиту персональных данных. Мы должны гарантировать полную совместимость будущей конвенции Организации Объединенных Наций по киберпреступности с международно-правовыми обязательствами в этой области.

2. Эффективность документа достигается за счет обеспечения необходимых гарантий, включая пропорциональность, законность и необходимость правоприменения.

3. Главной целью должно быть международное сотрудничество в предупреждении киберпреступности и борьбе с ней.

Российская Федерация, также от имени Беларуси, Бурунди, Китая, Никарагуа и Таджикистана

[Подлинный текст на русском языке]
[7 апреля 2022 года]

Глава I. Общие положения

Статья 1. Цели

Целями настоящей Конвенции являются:

a) содействие принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере информационно-коммуникационных технологий и борьбу с ними;

b) предотвращение действий, направленных против конфиденциальности, целостности и доступности информационно-коммуникационных технологий, и предупреждение злоупотреблений в сфере использования

информационно-коммуникационных технологий, путем обеспечения наказуемости деяний, охватываемых настоящей Конвенцией и предоставления полномочий, достаточных для эффективной борьбы с такими преступлениями и иными противоправными деяниями, путем содействия выявлению и расследованию таких деяний и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей о международном сотрудничестве;

c) повышение эффективности и развитие международного сотрудничества, в том числе в контексте подготовки кадров и оказания технической помощи в предупреждении преступлений в сфере информационно-коммуникационных технологий и борьбе с ними.

Статья 2. Сфера применения

1. Настоящая Конвенция применяется в соответствии с ее положениями к предупреждению, выявлению, пресечению, расследованию и преследованию за преступления и иные противоправные деяния, признанные таковыми в соответствии со статьями 6–29 настоящей Конвенции, а также осуществлению мер по устранению последствий от совершения таких деяний, включая приостановление операций, связанных с активами, приобретёнными в результате совершения какого-либо из преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, арест, конфискацию и возвращение доходов от таких преступлений.

2. Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен имущественный вред.

Статья 3. Защита суверенитета

1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами государственного суверенитета, суверенного равенства государств и невмешательства во внутренние дела других государств.

2. Настоящая Конвенция не наделяет компетентные органы Государства-участника правом осуществлять на территории другого Государства-участника юрисдикцию и функции, которые относятся к исключительной компетенции органов этого другого государства, если иное не предусмотрено в настоящей Конвенции в соответствии с его внутренним законодательством.

Статья 4. Термины и определения

Для целей настоящей Конвенции:

a) «арест имущества» означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа;

b) «бот-сеть» означает два и более устройства информационно-коммуникационных технологий, на которые установлена вредоносная программа, управляемая централизовано и скрытно от пользователей;

c) «вредоносная программа» означает программу, объективным свойством которой является несанкционированные модификация, уничтожение, копирование, блокирование информации или нейтрализация средств защиты информации в цифровой форме;

d) «детская порнография» определяется в соответствии с пунктом «c» статьи 2 Факультативного протокола к Конвенции о правах ребенка, касающимся

торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 года;

e) «доходы» означает любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления и иного противоправного деяния, предусмотренного настоящей Конвенцией, а также прибыль или другие выгоды, которые получены от таких доходов, от имущества, в которое были превращены или преобразованы такие доходы, или от имущества, к которому были приобщены такие доходы;

f) «информационно-коммуникационные технологии» (информационно-коммуникационных технологий) означает процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления;

g) «информационно-телекоммуникационные сети» означает совокупность инженерного оборудования, предназначенного для управления технологическими процессами с применением средств вычислительной техники и телекоммуникаций;

h) «имущество» означает любые активы, материальные и нематериальные, движимые или недвижимые, выраженные в вещах или в правах, включая денежные средства, в том числе находящиеся на банковских счетах, цифровые финансовые активы, цифровую валюту, включая криптовалюту, а также юридические документы или акты, подтверждающие право на такие активы или на их часть;

i) «информация» означает любые сведения (сообщения, данные), независимо от формы их представления;

j) «конфискация» означает принудительное безвозмездное изъятие имущества на основании постановления суда или другого компетентного органа;

k) «компьютерная атака» означает целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы или информационно-телекоммуникационные сети в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

l) «цифровая информация» означает сведения (данные), независимо от формы и характеристик, содержащиеся и обрабатываемые в информационно-телекоммуникационных устройствах, системах и сетях;

m) «критическая информационная инфраструктура» означает совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой;

n) «объекты критической инфраструктуры» означает информационные системы и информационно-коммуникационные сети государственных органов, а также информационные системы и автоматизированные системы управления технологическими процессами, функционирующие в сфере оборонной промышленности, здравоохранения, образования, транспорта, связи, энергетики, кредитно-финансовой сфере, атомной и других важных сферах жизнедеятельности государства и общества;

o) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством использования информационно-коммуникационных технологий, или

ii) любую другую организацию, которая осуществляет обработку или хранение информации в электронной форме от имени организации, упомянутой в подпункте (i), или пользователей услуг такой организации;

p) «технические параметры трафика» означают любую информацию в электронной форме (за исключением содержания передаваемых данных), связанную с передачей данных с использованием информационно-коммуникационных технологий и указывающую, в частности, на источник передачи данных, пункт назначения, маршрут, время, дату, размер, продолжительность, тип соответствующего сетевого сервиса;

q) «устройство информационно-коммуникационных технологий» означает совокупность (комплекс) технических средств, использующуюся/предназначенную для автоматизированной обработки, хранения и передачи информации в электронной форме;

r) «электронное доказательство» означает любую доказательную информацию, хранимую или передаваемую в цифровой форме (на электронном носителе информации).

Понятие «существенный ущерб» определяется в соответствии с внутренним законодательством запрашиваемого Государства-участника.

Южная Африка

[Подлинный текст на английском языке]
[14 апреля 2022 года]

Глава I. Общие положения

Статья 1. Заявляемые цели

Конвенция должна иметь следующие цели:

a) содействие принятию и укрепление мер по предупреждению и пресечению использования информационно-коммуникационных технологий в преступных целях/для совершения киберпреступлений и обеспечение защиты пользователей информационно-коммуникационных технологий от таких преступлений;

b) содействие принятию и укрепление мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере информационно-коммуникационных технологий и борьбу с ними;

c) поощрение, облегчение и поддержка международного сотрудничества в предупреждении и пресечении использования информационно-коммуникационных технологий в преступных целях/для совершения киберпреступлений;

d) предоставление практических средств для активизации технической помощи среди государств-участников и наращивания потенциала национальных органов власти в области предупреждения и пресечения использования информационно-коммуникационных технологий в преступных целях/для совершения киберпреступлений, а также усиление мер по содействию обмену информацией, опытом и примерами положительной практики.

Статья 2. Термины

Для целей настоящей Конвенции:

a) «единица» означает:

i) данные;

ii) компьютерную программу;

iii) компьютерный носитель данных; или

iv) компьютерную систему;

которая:

a. имеет отношение к совершению преступления или подозреваемого преступления или связана с этим либо обоснованно считается имеющей отношение к совершению преступления или подозреваемого преступления или связанной с этим;

b. может служить доказательством совершения преступления или подозреваемого преступления; или

c. предназначена для использования или обоснованно считается предназначенной для использования при совершении преступления или предполагаемого преступления, представляющего собой одно из следующего:

i. преступление по смыслу настоящей Конвенции;

ii. любое другое преступление, совершенное посредством использования информационно-коммуникационных технологий; или

iii. преступление, совершенное в иностранном государстве, которое по существу аналогично преступлению, предусмотренному настоящей Конвенцией;

b) «материалы о сексуальных надругательствах над детьми» означает любое изображение, каким бы образом оно ни было создано, или любое описание или воспроизведение откровенных сексуальных действий, включая любую фотографию, фильм, видео, изображение, сделанное или произведенное электронными, механическими или другими средствами, если:

i) в производстве такого визуального отображения участвует несовершеннолетнее лицо;

ii) таким визуальным отображением является цифровое изображение, компьютерное изображение или созданное на компьютере изображение несовершеннолетнего лица, участвующего в откровенных сексуальных действиях, или изображения его половых органов, которые производятся или используются главным образом в сексуальных целях и эксплуатируются с ведома или без ведома ребенка; и

iii) такое визуальное отображение создается, адаптируется или изменяется так, чтобы казалось, что несовершеннолетнее лицо участвует в откровенных сексуальных действиях;

c) «компьютер» означает любое электронное программируемое устройство, используемое самостоятельно либо в составе компьютерной системы или любого другого устройства или оборудования, или любую его часть, используемое для выполнения заранее определенных арифметических, логических операций, операций маршрутизации, обработки или хранения в соответствии с заданными инструкциями, и включает любые данные, компьютерную программу или компьютерный носитель информации, которые связаны, соединены или используются с таким устройством;

d) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию;

e) «компьютерный носитель информации» означает любое устройство, с которого могут быть воспроизведены данные или компьютерная программа или на котором данные или компьютерная программа могут быть сохранены компьютерной системой, независимо от того, является ли устройство физически подсоединенным или подключенным к компьютерной системе;

f) «компьютерная программа» означает данные, представляющие собой инструкции или команды, при исполнении которых в компьютерной системе она выполняет определенную функцию;

g) «компьютерная система» означает:

i) один компьютер; или

ii) два или более подключенных друг к другу или связанных компьютера, что позволяет этим подключенным друг к другу или связанным компьютерам:

a. обмениваться друг с другом данными или любыми другими функциями; или

b. обмениваться данными или любыми другими функциями с другим компьютером или компьютерной системой;

h) «конфискация», которая включает в соответствующих случаях изъятие, означает окончательное лишение имущества по постановлению суда или другого компетентного органа;

i) «киберзависимые преступления» — это преступления, которые могут совершаться только с использованием компьютеров, компьютерных сетей и другого вида информационно-коммуникационных технологий;

j) «преступления, совершаемые посредством кибертехнологий» — это преступления, которые не зависят от компьютеров или сетей, но претерпели изменения в масштабах или форме благодаря использованию сети Интернет и коммуникационных технологий;

k) «сообщение данных» означает данные, которые созданы, отправлены, получены или сохранены с помощью электронных средств, причем любые выводимые данные имеют понятную форму;

l) «цифровая информация» означает любые сведения (данные), независимо от формы и характеристик, содержащиеся и обрабатываемые в информационно-коммуникационных устройствах, системах и сетях;

m) «электронное доказательство» означает любую доказательную информацию, хранимую или передаваемую в цифровой форме (на электронном носителе информации);

n) «арест активов» означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа;

o) «имущество» означает любые активы, будь то материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них;

p) «доходы от преступления» означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления;

q) «основное правонарушение» означает любое правонарушение, в результате которого получены доходы, в отношении которых могут быть совершены деяния, образующие состав преступления, указанные в статье 23 настоящей Конвенции и во внутреннем законодательстве Государства-участника/Государства-члена;

r) «арест активов» означает осуществление постоянного контроля над активами либо вступление в окончательное владение имуществом или осуществление постоянного контроля над ним по постановлению суда или другого компетентного органа;

s) «поставщик услуг» означает любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы, или любую другую

организацию, которая осуществляет обработку или хранение компьютерных данных от имени такой службы обмена информацией или пользователей такой службы;

t) «технические параметры трафика» означают данные, относящиеся к обмену информацией, указывающие на источник, пункт назначения, маршрут, формат, время, дату, размер, продолжительность передачи информации или тип соответствующей услуги.

Статья 3. Сфера применения

Настоящая Конвенция применяется, в соответствии с ее положениями, к предупреждению, расследованию и уголовному преследованию киберзависимых преступлений и/или конкретных преступлений, совершаемых посредством кибертехнологий и с использованием информационно-коммуникационных технологий в преступных целях, а также к замораживанию, аресту, конфискации и возвращению доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 4. Защита суверенитета

1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств.

2. Ничто в настоящей Конвенции не наделяет Государство-участника правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством.

Швейцария

[Подлинный текст на английском языке]
[8 апреля 2022 года]

2.1. Общие положения

Цель

Цели настоящей Конвенции:

a) содействие принятию и укрепление мер, направленных на эффективное и действенное [предупреждение/пресечение и противодействие] киберпреступности;

b) поощрение, облегчение и поддержка международного сотрудничества и технической помощи в предупреждении киберпреступности и борьбе с ней.

Уважение и защита прав человека и основных свобод

Государства-участники должны осуществлять свои обязательства согласно настоящей Конвенции в соответствии со своими обязательствами по международному праву прав человека.

Термины

«Компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных.

«Компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной

системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию.

«Поставщик услуг» означает:

a) любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы; и

b) любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей такой службы.

«Технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер, продолжительность обмена информацией или тип соответствующей услуги.

Сфера применения

Настоящая Конвенция, если в ней не указано иное, применяется к предупреждению, расследованию и уголовному преследованию в связи с преступлениями, признанными таковыми в соответствии с положениями настоящей Конвенции о криминализации.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[12 апреля 2022 года]

Глава. Общие положения

Статья 1. Цель

Цель настоящей Конвенции заключается в содействии международному сотрудничеству и технической помощи в деле предупреждения киберпреступности и борьбы с ней.

Статья 2. Определения

Для целей настоящей Конвенции:

a) «компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных;

b) «компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютерной системе команду выполнить какую-либо функцию;

c) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы; и

ii) любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей услуг такой службы;

d) «технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер, продолжительность обмена информацией или тип соответствующей услуги.

Статья 3. Сфера применения

1. Настоящая Конвенция, если в ней не указано иное, применяется к предупреждению, расследованию и уголовному преследованию в связи с преступлениями, признанными таковыми в настоящей Конвенции.

2. Настоящая Конвенция может также применяться, если в ней это указано, к сбору электронных доказательств совершения уголовного преступления.

Статья 4. Защита прав человека

Каждая Сторона обеспечивает соответствие обязательств, осуществляемых ею по настоящей Конвенции, международному праву прав человека.

Дополнительные замечания

Соединенное Королевство считает, что в главе, содержащей общие положения, целесообразно рассмотреть также вопрос о том, как данная конвенция соотносится с другими документами Организации Объединенных Наций в области уголовного правосудия и дополняет их, а также включить обязательство учитывать гендерные аспекты при осуществлении положений конвенции.

Объединенная Республика Танзания

[Подлинный текст на английском языке]
[8 апреля 2022 года]

3. Общие положения

Цель настоящей Конвенции должна заключаться в содействии сотрудничеству в противодействии использованию информационно-коммуникационных технологий в преступных целях. Киберпространство изменяется, и на сегодняшний день существует широкий спектр терминов, используемых в информационно-коммуникационных технологиях. Крайне важно, чтобы в Конвенции были определены термины, повсеместно принятые в информационно-коммуникационных технологиях, чтобы избежать двусмысленности или недопонимания.

3.1. Определение терминов

Объединенная Республика Танзания считает, что в Конвенции должны даваться технически нейтральные определения терминов, чтобы они отражали быстрые изменения, которые происходят в сфере технологий. Должны быть определены следующие термины:

a) доступ;

b) поставщик услуг доступа;

c) поставщик услуг кеширования;

d) ребенок;

e) детская порнография;

f) компьютерная система;

g) компьютерные данные;

h) конфискация;

i) контрабанда;

j) криптография;

k) кибертерроризм;

l) данные;

m) сообщение данных;

n) носитель данных;

o) электронные данные;

p) замораживание;

q) препятствие работе компьютерной системы;

r) интерактивная система сообщений;

s) перехват в отношении работы компьютера;

t) межсоединение;

u) источник;

v) расистские и ксенофобские материалы;

w) изъятие;

x) поставщик услуг в области информационно-коммуникационных технологий;

y) технические параметры трафика.

3.2. Юрисдикция

Конвенция должна предусматривать законодательные и иные меры, которые могут потребоваться каждому Государству-участнику для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, если:

a) преступление совершено на территории этого Государства-участника;

b) преступление совершено на борту судна, которое несло флаг этого Государства-участника, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника;

c) преступление направлено против компьютерной системы, устройства, данных или лица, находящегося на территории этого Государства-участника;

d) преступление совершено гражданином этого Государства-участника или против гражданина Государства-участника.

Соединенные Штаты Америки

[Подлинный текст на английском языке]
[8 апреля 2022 года]

Термины

«Ребенок» означает любое лицо в возрасте до 18 лет.

«Материалы о сексуальных надругательствах над детьми» означают любое изображение или прямую трансляцию: a) ребенка, совершающего реальные или смоделированные откровенные сексуальные действия; или b) взрослого, совершающего реальные или смоделированные откровенные сексуальные действия в

отношении ребенка, намеренно включенного в изображение или прямую трансляцию. Ребенок не обязательно должен осознавать, понимать или характеризовать такое откровенное сексуальное поведение[6].

«Компьютерные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, в том числе соответствующую программу, дающую компьютеру команду выполнить такую функцию.

«Компьютерная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит автоматическую обработку данных.

«Конфискация» означает окончательное лишение имущества по постановлению суда или другого компетентного органа[7].

«Киберпреступления» означают преступления, признанные таковыми в соответствии с Конвенцией.

«Арест» или «выемка» означают временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа[8].

«Основное правонарушение» означает любое правонарушение, в результате которого получены доходы, в отношении которых могут быть совершены деяния, указанные в статье о киберпреступлениях настоящей Конвенции, образующие состав преступления[9].

«Доходы от преступления» означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления[10].

«Имущество» означает любые активы, будь то материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них[11].

«Региональная организация экономической интеграции» означает организацию, созданную суверенными государствами какого-либо региона, которой ее государства-члены передали полномочия по вопросам, регулируемым настоящей Конвенцией, и которая должным образом уполномочена в соответствии с ее внутренними процедурами подписывать, ратифицировать, принимать, утверждать настоящую Конвенцию или присоединяться к ней; ссылки в настоящей Конвенции на «Государства-участники» относятся к таким организациям в пределах их компетенции[12].

«Поставщик услуг» означает: a) любую государственную или частную организацию, которая обеспечивает пользователям ее услуги возможность обмена информацией посредством компьютерной системы; b) любую другую организацию, которая обрабатывает или хранит компьютерные данные от имени такой службы обмена информацией или пользователей услуг такой службы.

«Откровенные сексуальные действия» включает, по крайней мере, следующие реальные или смоделированные действия: a) половой акт, в том числе

---

[6] Адаптированное определение из ст. 2, п. (c) Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии.

[7] Конвенция против организованной преступности, ст. 2, п. (g).

[8] Там же, ст. 2, п. (f).

[9] Там же, ст. 2, п. (h).

[10] Там же, ст. 2, п. (e).

[11] Там же, ст. 2, п. (d).

[12] Там же, ст. 2, п. (j).

генитально-генитальный, орально-генитальный, анально-генитальный или орально-анальный, между детьми или между взрослым и ребенком; b) скотоложство; c) мастурбацию; d) садистское или мазохистское насилие в сексуальном контексте; e) развратные действия, заключающиеся в демонстрации гениталий или лобковой области ребенка, как одетого, так и обнаженного.

«Технические параметры трафика» означают любые компьютерные данные, связанные с обменом информацией посредством компьютерной системы, генерируемые компьютерной системой, являющейся составной частью коммуникационной цепочки, указывающие на источник, пункт назначения, маршрут, время, дату, размер, продолжительность обмена информацией или тип соответствующей услуги.

Сфера применения

Настоящая Конвенция, если в ней не указано иное, применяется к предупреждению, расследованию и уголовному преследованию в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, а также к сбору и получению электронных доказательств и обмену ими.

Защита прав человека и основных свобод и верховенства права

1. Государства-участники выполняют свои обязательства по настоящей Конвенции при полном уважении прав человека и основных свобод и верховенства права.

2. Ничто в настоящей Конвенции не толкуется как затрагивающее другие права и обязательства государств и лиц в соответствии с международным правом, в том числе с Уставом Организации Объединенных Наций и международным правом прав человека.

3. Любое лицо, которое взято под стражу или в отношении которого приняты любые другие меры или осуществляется разбирательство в соответствии с настоящей Конвенцией, пользуется всеми правами и гарантиями в соответствии с законодательством государства, на территории которого это лицо находится, и соответствующими положениями международного права прав человека, включая Международный пакт о гражданских и политических правах.

Защита суверенитета[13]

1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств.

2. Ничто в настоящей Конвенции не наделяет Государство-участника правом осуществлять на территории другого государства юрисдикцию или функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством.

Венесуэла (Боливарианская Республика)

[Подлинный текст на испанском языке]
[13 апреля 2022 года]

4. Общие положения

Общие положения конвенции в этом контексте должны соответствовать основным принципам международного публичного права как неотъемлемой части будущего документа, закрепленным в Уставе Организации Объединенных

[13] Конвенция против организованной преступности и Конвенция против коррупции, ст. 4.

Наций, включая, среди прочего, признание суверенитета и территориальной юрисдикции в соответствии с национальным законодательством государств, в том числе применение принципа суверенитета к киберпространству, невмешательство во внутренние дела других государств и уважение их территориальной целостности, а также мирное урегулирование споров.

В конвенции должен обеспечиваться принцип взаимодополняемости с другими международными документами, как многосторонними, так и региональными, касающимися транснациональной преступности, такими как Конвенция Организации Объединенных Наций против коррупции и Конвенция Организации Объединенных Наций против транснациональной организованной преступности, а также должно обеспечиваться соблюдение обязанностей, предусмотренных международным правом прав человека, включая конвенции по правам человека.

В этой связи Боливарианская Республика Венесуэла подчеркивает, что, как и в случае других международно-правовых документов, данный документ не должен искусственно создавать конфликта между концепциями национального суверенитета и прав человека, которые по своей природе являются взаимодополняющими.

Эта глава должна содержать определения основных терминов и выражений, используемых в конвенции.

Вьетнам

[Подлинный текст на английском языке]
[12 апреля 2022 года]

Глава I. Общие положения

1. Цели

a) Содействие принятию и усиление мер по предупреждению использования информационно-коммуникационных технологий в преступных целях и борьбы с ним;

b) поощрение, облегчение и поддержка международного сотрудничества и технической помощи в предупреждении использования информационно-коммуникационных технологий в преступных целях и борьбе с ним, в том числе в принятии мер по возвращению активов, в соответствии с основополагающими принципами международного права и с соблюдением прав человека.

2. Сфера применения

Настоящая Конвенция применяется к предупреждению, расследованию и уголовному преследованию использования информационно-коммуникационных технологий в преступных целях.

3. Защита суверенитета

a) Государства-члены осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства, территориальной целостности государств, отказа от угрозы силой или ее применения и принципом невмешательства во внутренние дела других государств;

b) Ничто в настоящей Конвенции не наделяет Государство-член правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого Государства-члена в соответствии с его внутренним законодательством.

4. Определения

a) «Киберпространство» означает сеть объектов информационно-технологической инфраструктуры, которая включает телекоммуникационные сети, сеть Интернет, компьютерные сети, системы обмена информацией, системы обработки и контроля информации и базы данных;

b) «информационная система» означает сочетание аппаратных средств, программного обеспечения и баз данных, развернутых для обеспечения функций создания, передачи, сбора, обработки и хранения информации в киберпространстве;

c) «кибератака» означает использование киберпространства, информационных технологий или электронных устройств для саботажа или нарушения работы телекоммуникационной сети, сети Интернет, компьютерных сетей, систем обмена информацией, систем обработки информации и управления, баз данных или электронных устройств;

d) «кибертерроризм» означает акт терроризма или финансирования терроризма, который связан с использованием киберпространства, информационных технологий или электронных устройств;

e) «персональная информация» означает информацию, связанную с идентификацией физического лица;

f) «цифровые данные» включают сигналы, буквы, цифры, изображения, звуки и аналогичные элементы, которые создаются, хранятся, передаются или принимаются с помощью электронных средств;

g) «инфраструктура киберпространства» означает систему инфраструктурных объектов, которые обеспечивают функции создания, передачи, сбора, обработки и хранения информации и данных в киберпространстве.