

**Генеральная Ассамблея**

Distr.: General
16 May 2022
Russian
Original: English

**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

Содержание

	<i>Стр.</i>
V. Дополнительные сообщения	2
Введение	2
Индия	2
Ямайка (от имени Карибского сообщества)	14
Малайзия	25
Сингапур	30
Уругвай	33



V. Дополнительные сообщения

Введение

В настоящем добавлении представлены сообщения государств-членов, подготовленные для второй сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и полученные после 14 апреля 2022 года; представленные сообщения не разделены на тематические главы.

Индия

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

Справочная информация

1. Киберпространство является комплексной средой, объединяющей физических лиц, программное обеспечение, аппаратное обеспечение и услуги в сети Интернет, и обладает своеобразными и уникальными характерными чертами, отличающими его от физического пространства. Киберпространство представляет собой виртуальное пространство, не имеющее границ и обеспечивающее анонимность. В последние годы социальные сети и экосистема подвижной связи вошли в число важных каналов связи общественного пользования. С недавних пор преступники и антинациональные элементы во всем мире стали использовать социальные сети в качестве одного из основных инструментов для совершения киберпреступлений. В условиях не имеющего границ киберпространства в сочетании с возможностью мгновенного установления связи и анонимностью потенциал для совершения киберпреступлений с использованием социальных сетей и сети Интернет как в стране, так и во всем мире высок, как никогда.
2. Киберпреступность также стала одной из серьезных проблем в связи с резким ростом использования во всем мире устройств информационно-коммуникационных технологий. С развитием технологий люди стали полагаться на информационно-коммуникационные технологии для удовлетворения всех своих потребностей. В отличие от обычной преступности, киберпреступность не имеет географических границ, а киберпреступники не попадают в поле зрения и даже сохраняют анонимность, и это наносит ущерб всем заинтересованным сторонам, включая обычных граждан. В следующем разделе рассматриваются типы киберпреступлений, совершаемых во всем мире.

Классификация преступлений, совершаемых с использованием информационно-коммуникационных технологий

3. Киберпреступность — это широкий термин, используемый для определения преступной деятельности, в которой компьютеры или компьютерные сети являются инструментом, целью или местом преступления, и охватывающий все виды правонарушений — от повреждения электронного оборудования до атак типа «отказ в обслуживании». В целом киберпреступления можно классифицировать как «киберпреступления, совершаемые с помощью компьютерных технологий»¹ и «киберпреступления, совершаемые в информационной среде»². Кроме того, киберпреступления можно классифицировать как

¹ Такие преступления, как кражи, домогательства, эксплуатация детей, мошенничество и аферы: они могут быть совершены без использования компьютера, однако в определенных обстоятельствах их можно совершить именно благодаря компьютеру.

² Хакерство, использование вирусов-вымогателей, распределенные атаки типа «отказ в обслуживании», использование вредоносного программного обеспечения, распространение вирусов и кибертерроризм.

«киберпреступления против физических лиц», «киберпреступления против собственности» и «киберпреступления против государственной власти». Однако, возможно, лучше использовать такое определение, как «преступления, совершаемые с использованием информационно-коммуникационных технологий», поскольку под это определение также подпадают новые и новейшие технологии.

Криминализация

4. Каждое государство-участник принимает такие предусмотренные последующими пунктами законодательные и иные меры, которые необходимы для признания определенного действия в качестве преступления или эквивалентного ему деяния в своем внутреннем законодательстве. (Приведенный ниже список является ориентировочным и может быть дополнен иными преступлениями, совершенными с использованием информационно-коммуникационных технологий).

4(a) Повреждение компьютера, компьютерной системы и т. д.

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий какого-либо лица, которое без разрешения владельца или какого-либо другого лица, в ведении которого находится компьютер, компьютерная система или компьютерная сеть:

- a) получает или обеспечивает доступ к такому компьютеру, компьютерной системе, компьютерной сети или компьютерному ресурсу;
- b) скачивает, копирует или извлекает какие-либо данные, компьютерную базу данных или информацию из такого компьютера, компьютерной системы или компьютерной сети, включая информацию или данные, хранящиеся на каком-либо съемном носителе;
- c) внедряет или инициирует внедрение какой-либо вредоносной компьютерной программы или компьютерного вируса в какой-либо компьютер, компьютерную систему или компьютерную сеть;
- d) повреждает или вызывает повреждение какого-либо компьютера, компьютерной системы или компьютерной сети, данных, компьютерной базы данных или каких-либо иных программ, находящихся в таком компьютере, компьютерной системе или компьютерной сети;
- e) нарушает функционирование или вызывает нарушение функционирования какого-либо компьютера, компьютерной системы или компьютерной сети;
- f) каким-либо способом отказывает или инициирует отказ в доступе какому-либо лицу, имеющему право доступа к какому-либо компьютеру, компьютерной системе или компьютерной сети;
- g) оказывает какую-либо помощь какому-либо лицу для упрощения доступа к компьютеру, компьютерной системе или компьютерной сети в нарушение положений настоящего акта или правил или положений, принятых в соответствии с ним;
- h) проводит оплату услуг, полученных каким-либо лицом, за счет другого лица путем вмешательства в работу какого-либо компьютера, компьютерной системы или компьютерной сети, либо манипуляций с ними;
- i) уничтожает, удаляет или изменяет какую-либо информацию, находящуюся в компьютерном ресурсе, или снижает ее ценность или полезность или каким-либо способом оказывает на нее вредное воздействие;
- j) похищает, скрывает, уничтожает или изменяет, либо принуждает какое-либо лицо похитить, скрыть, уничтожить или изменить какой-либо исходный код, используемый для компьютерного ресурса, в целях нанесения ущерба.

4(b) *Необеспечение защиты данных*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий корпоративной структуры, которая, владея какими-либо конфиденциальными личными данными или информацией, используя или обрабатывая их в компьютерном ресурсе, находящемся в ее владении, под ее контролем или управлением, проявляет небрежность в применении и поддержании обоснованных методов и процедур обеспечения безопасности и тем самым наносит неправомерный ущерб или предоставляет неправомерную выгоду какому-либо лицу.

4(c) *Манипуляции с исходными компьютерными документами*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания преступлением, подлежащим наказанию, согласно его внутреннему законодательству, действий какого-либо лица, которое сознательно или намеренно скрывает, уничтожает или изменяет, либо намеренно или сознательно принуждает иное лицо скрывать, уничтожать или изменять любой исходный компьютерный код, используемый для компьютера, компьютерной программы, компьютерной системы или компьютерной сети, при условии, что этот исходный компьютерный код подлежит хранению или поддержанию в соответствии с действующим законодательством.

4(d) *Рассылка оскорбительных сообщений по каналам связи и т. д.*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий какого-либо лица, которое использует компьютерный ресурс или устройство связи для:

- а) рассылки какой-либо информации крайне оскорбительного или угрожающего характера;
- б) постоянной рассылки с использованием такого компьютерного ресурса или устройства связи какой-либо заведомо ложной информации с целью вызвать раздражение и неудобство, создать угрозу и затруднения, нанести оскорбление и травму, осуществить преступное запугивание, вызвать вражду, ненависть или недоброжелательность;
- с) рассылки каких-либо электронных писем или электронных почтовых сообщений с целью вызвать раздражение или неудобство, обмануть или ввести в заблуждение адресата или получателя относительно источника этих сообщений.

4(e) *Получение украденного компьютерного ресурса или коммуникационного устройства неправомерным путем*

Если какое-либо лицо, получает неправомерным путем или хранит какой-либо украденный компьютерный ресурс или устройство связи, зная или имея основания полагать, что этот компьютерный ресурс или устройство связи были украдены.

4(f) *Кража личных данных (подмена личности)*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий какого-либо лица, которое обманным или неправомерным образом использует электронную подпись, пароль или любой другой уникальный идентификационный признак любого иного лица.

4(g) *Мошенничество путем выдачи себя за другое лицо при помощи компьютерных ресурсов (подмена личности)*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое использует какой-либо компьютерный ресурс или устройство связи для мошенничества путем подмены личности.

4(h) *Нарушение неприкосновенности частной жизни*

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое намеренно или сознательно осуществляет фиксацию, публикацию или распространение изображения интимных частей тела какого-либо лица без его согласия при обстоятельствах, нарушающих неприкосновенность частной жизни этого лица:

а) «Распространение» означает отправку визуального изображения в электронном виде с тем, чтобы оно было просмотрено одним или несколькими лицами.

б) «Фиксация» в отношении изображения означает видеозапись, фотографирование, киносъемку или запись любым способом.

с) «Интимная зона» означает обнаженные или закрытые нижним бельем гениталии, паховую область, ягодицы или женскую грудь.

д) «Публикация» означает воспроизведение изображения в печатной или электронной форме и предоставление всеобщего доступа к нему.

е) «При обстоятельствах, нарушающих неприкосновенность частной жизни» означает при обстоятельствах, когда лицо может иметь достаточные основания полагать, что:

i) он или она может переодеваться в уединении, не опасаясь, что кто-либо сделает изображение интимных частей его или ее тела; или

ii) какие-либо интимные части его или ее тела не будут видны, независимо от того, находится ли это лицо в общественном или частном месте.

4(i) *Кибертерроризм*

1. Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое:

а) действует с намерением поставить под угрозу единство, целостность, безопасность или суверенитет государства либо запугать население или любую группу населения:

i) отказывая в доступе или создавая условия для отказа в доступе какому-либо лицу, имеющему право доступа к компьютерному ресурсу; или

ii) предпринимая попытку проникновения или доступа к компьютерному ресурсу без разрешения или с превышением пределов санкционированного доступа; или

iii) внедряя любые вредоносные компьютерные программы или иницируя их внедрение;

и посредством таких действий причиняет или может причинить смерть или увечья физическим лицам, привести к нанесению ущерба или уничтожению имущества, либо нарушает цепь поставок или услуг, важных для жизни сообщества, либо отдает себе отчет в том, что его действия могут привести к повреждению

или нарушению такой цепи поставок или услуг, или оказать негативное воздействие на критическую информационную инфраструктуру;

b) сознательно или преднамеренно проникает в компьютерный ресурс или получает доступ к нему без разрешения или с превышением пределов санкционированного доступа и получает посредством таких действий доступ к информации, данным или компьютерной базе данных, доступ к которым ограничен по соображениям государственной безопасности или международных отношений, или к какой-либо информации, данным или компьютерной базе данных с ограниченным доступом при наличии оснований полагать, что информация, данные или компьютерная база данных, полученные таким образом, могут быть использованы для нанесения или вероятного нанесения ущерба интересам суверенитета и целостности государства, безопасности государства, дружественных отношений с иностранными государствами, общественного порядка, приличия или морали, или в связи с неуважением к суду, клеветой или подстрекательством к преступлению, или в интересах любого иностранного государства, группы лиц, либо иным образом, то это лицо совершает преступление кибертерроризма.

2. Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершения и покушения на совершение какого-либо преступления, соответствующего описанию в пунктах 1(a) и (b).

4(j) Публикация или распространение непристойных материалов в электронных сообщениях

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое публикует или распространяет или способствует публикации или распространению в электронной форме каких-либо материалов, являющихся развратными или вызывающих нездоровый сексуальный интерес, или могущих способствовать развращению и разложению лиц, которые могут, с учетом всех соответствующих обстоятельств, прочесть, увидеть или услышать содержащиеся или воплощенные в них сведения.

4(k) Публикация или распространение материалов, содержащих откровенное изображение действий сексуального характера и т. д., в электронной форме

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое публикует или распространяет или способствует публикации или распространению в электронной форме каких-либо материалов, содержащих откровенное изображение действий сексуального характера или сексуального поведения.

4(l) Публикация или распространение материалов, содержащих откровенное изображение действий сексуального характера с участием детей и т. д., в электронной форме

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, действий любого лица, которое:

a) публикует, распространяет или способствует публикации или распространению в электронной форме каких-либо материалов, изображающих вовлечение детей в действия сексуального характера или сексуальное поведение; или

b) создает тексты или цифровые изображения, собирает, ищет, просматривает, скачивает, рекламирует, продвигает, обменивает или распространяет в какой-либо электронной форме материалы, изображающие детей в непристойном, неприличном или в откровенно сексуальном виде; или

с) привлекает, заманивает или склоняет детей к отношениям в онлайн-среде с одним ребенком или несколькими детьми для совершения откровенных действий сексуального характера или действий, способных оскорбить добросовестного взрослого человека на компьютерном ресурсе; или

d) способствует надругательствам над детьми в сети Интернет; или

e) записывает в какой-либо электронной форме совершаемые им или иными лицами акты надругательства, связанные с откровенными действиями сексуального характера в отношении детей;

при том условии, что данный раздел не охватывает какие-либо книги, брошюры, статьи, письменные материалы, чертежи, живописные изображения или рисунки в электронной форме:

i) публикация которых оправдана как предназначенная для общественного блага на том основании, что такая книга, брошюра, статья, письменный материал, чертеж, живописное изображение или рисунок представляет интерес для науки, литературы, искусства либо образования или других областей общего характера; или

ii) которые сохраняются или используются в рамках добросовестного сохранения наследия или в религиозных целях.

Возраст «детей» определяется в соответствии с внутренним законодательством данного государства.

4(m) Раскрытие информации в нарушение законного договора

Если иное не предусмотрено настоящей Конвенцией, какое-либо лицо, включая посредника, которое, предоставляя услуги на условиях законного договора, получило доступ к каким-либо материалам, содержащим персональные данные другого лица, с намерением причинить неправомерный ущерб или извлечь неправомерную выгоду, либо, зная о возможности причинить такой ущерб или извлечь такую выгоду, раскрывает без согласия затронутого лица или в нарушение законного договора такие материалы любому иному лицу.

5. Другие противоправные деяния, совершаемые с использованием информационно-коммуникационных технологий

Без ущерба для (статьи о защите суверенитета), в целях сотрудничества, осуществляемого в соответствии с настоящей Конвенцией, Договаривающиеся Стороны достигают взаимного согласия относительно сущности любых иных противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий. (С учетом развития информационно-коммуникационных технологий в данную Конвенцию следует включить положение «Иные противоправные деяния»). Кроме того, с помощью настоящей Конвенции можно дополнительно расширить сферу криминализации следующих киберпреступлений, упомянутых в документе Управления Организации Объединенных Наций по наркотикам и преступности³:

- Незаконный доступ
- Незаконный перехват: осуществляемый техническими средствами противоправный перехват непубличных передач информации в электронной форме в компьютерную систему, из нее или внутри нее, включая незаконное создание электромагнитных помех
- Инструменты для неправомерного использования компьютеров
- Преступления, касающиеся персональных данных

³ Источник: United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, проект, представленный в феврале 2013 года, р. 22.

- Личный вред
- Расизм и ксенофобия
- Правонарушения, касающиеся поддержки терроризма
- Вирусы-вымогатели.

13. Используемые термины

а) «Устройство связи» означает сотовые телефоны, карманные персональные компьютеры или их сочетание, или какое-либо иное устройство, используемое для связи, отправки или передачи какого-либо текста, видеоматериала, аудиоматериала или изображения.

б) «Компьютер» означает какое-либо электронное, магнитное, оптическое или иное высокоскоростное устройство или систему обработки данных, выполняющие логические, арифметические функции и функции памяти путем манипуляций с электронными, магнитными или оптическими импульсами, и охватывает все средства ввода, вывода, обработки, хранения, компьютерного программного обеспечения или связи, которые соединены или связаны с компьютером в компьютерную систему или компьютерную сеть.

с) «Компьютерная сеть» означает соединение одного или нескольких компьютеров или компьютерных систем либо устройств связи посредством:

- i) использования спутниковых, микроволновых, наземных, проводных, беспроводных или иных средств связи; и
- ii) окончных устройств или комплекса, состоящего из двух или более взаимосвязанных компьютеров или устройств связи, независимо от того, поддерживается ли взаимосвязь постоянно.

д) «Компьютерный ресурс» означает компьютер, компьютерную систему, компьютерную сеть, данные, компьютерную базу данных или программное обеспечение.

е) «Компьютерная система» означает устройство или совокупность устройств, включая устройства поддержки ввода и вывода и исключая калькуляторы (которые не являются программируемыми устройствами и не могут использоваться совместно с внешними файлами), содержащие компьютерные программы, электронные инструкции, входные данные и выходные данные и выполняющие логические и арифметические функции, функции хранения и поиска данных, функции управления связью и иные функции.

ф) «Вредоносная компьютерная программа» означает любой набор компьютерных инструкций, предназначенных для того, чтобы:

- i) изменять, уничтожать, записывать, передавать данные или программы, находящиеся в компьютере, компьютерной системе или компьютерной сети; или
- ii) любыми средствами нарушать нормальную работу компьютера, компьютерной системы или компьютерной сети.

г) «Компьютерная база данных» означает представление информации, знаний, фактов, понятий или инструкций в виде текста, изображения, аудиоматериалов, видеоматериалов, которые подготавливаются или были подготовлены в формализованном виде или были произведены компьютером, компьютерной системой или компьютерной сетью и предназначены для использования в компьютере, компьютерной системе или компьютерной сети.

h) «Компьютерный вирус» означает любую компьютерную инструкцию, информацию, данные или программу, которая уничтожает, повреждает, ухудшает или отрицательно воздействует на работу компьютерного ресурса или присоединяется к другому компьютерному ресурсу и действует при выполнении

программы, данных или инструкций или при каком-либо ином событии в данном компьютерном ресурсе.

i) «Повреждение» означает уничтожение, изменение, удаление, добавление, модификацию или переустройство какого-либо компьютерного ресурса любым способом.

j) «Компьютерный исходный код» означает протокол программы, компьютерные команды, дизайн и компоновку и программный анализ компьютерного ресурса в какой-либо форме.

k) «Кибербезопасность» означает защиту информации, оборудования, устройств, компьютеров, компьютерных ресурсов, устройств связи и хранящейся в них информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения.

l) «Данные» означают представление информации, знаний, фактов, концепций или инструкций, которые подготавливаются или были подготовлены в формализованном виде и предназначены для обработки, обрабатываются или были обработаны в компьютерной системе, компьютерной сети или облаке, и могут существовать в любой форме (включая компьютерные распечатки, магнитные или оптические носители информации, перфокарты, перфоленты), либо хранятся в оперативной памяти компьютера.

m) «Информация» включает данные, сообщения, тексты, изображения, звуковые файлы, голосовые файлы, коды, компьютерные программы, программное обеспечение и базы данных или микрофильмы или созданные компьютером микрофиши.

n) «Корпоративная структура» означает любую компанию и охватывает фирмы, индивидуальные предприятия или иные объединения лиц, занимающихся коммерческой или профессиональной деятельностью.

o) «Обоснованные методы и процедуры обеспечения безопасности» означают методы и процедуры обеспечения безопасности, разработанные для защиты такой информации от несанкционированного доступа, повреждения, использования, модификации, раскрытия или нарушения, которые могут быть обозначены в соглашении между сторонами или в каком-либо действующем законе, а в отсутствие такого соглашения или какого-либо закона — обоснованные методы и процедуры обеспечения безопасности, которые могут быть определены государствами-участниками по итогам консультаций с надлежащими профессиональными органами или ассоциациями.

p) «Конфиденциальные личные данные или информация» означают личную информацию, которая может быть определена государствами-участниками по итогам консультаций с надлежащими профессиональными органами или ассоциациями.

q) «Электронное письмо» и «электронное почтовое сообщение» означают сообщение или информацию, созданные, переданные или полученные на компьютере, в компьютерной системе, на компьютерном ресурсе или устройстве связи, включая вложения в виде текста, изображения, аудиоматериала, видеоматериала или любой иной электронной записи, которая может быть передана вместе с сообщением.

r) «Посредник в социальных сетях» означает посредника, который преимущественно или исключительно обеспечивает онлайн-взаимодействие между двумя или более пользователями и позволяет им создавать, загружать, делиться, распространять, изменять или получать доступ к информации, используя его услуги.

s) «Электронная запись» означает данные, запись или созданные данные, изображение или звуки, сохраненные, полученные или отправленные в электронной форме или в виде микрофильма или микрофиши, созданных компьютером.

t) «Источник» означает лицо, которое отправляет, генерирует, хранит или передает какое-либо электронное сообщение или обеспечивает отправление, генерацию, хранение или передачу какого-либо электронного сообщения какому-либо иному лицу; при этом данное понятие не включает посредника.

u) «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 собственности на такие активы или какую-либо их часть, или интерес в них или в какой-либо их части.

v) «Доходы от преступления» означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения преступления и иного противоправного деяния, предусмотренного настоящей Конвенцией.

w) «Конфискация» включает в соответствующих случаях изъятие и означает окончательное лишение имущества по постановлению суда или другого компетентного органа.

x) «Основное правонарушение» означает любое правонарушение, в результате которого получены доходы, в отношении которых могут быть совершены указанные в настоящей Конвенции деяния, образующие состав преступления.

y) «Детская порнография» означает любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях.

14. Юрисдикция, ориентированная на данные

Юрисдикция, ориентированная на данные, означает, что страна, данные граждан которой подвергаются хранению/обработке/проверке/объединению в какой-либо иной стране мира, должна обладать более широкой юрисдикцией в отношении данных, независимо от того, где осуществляется физическое хранение/обработка/проверка/объединение данных. Юрисдикция, ориентированная на данные, обеспечивает приоритет права собственности на данные, конфиденциальности (признанного основополагающего права граждан всего мира) и прав человека.

(Краткое пояснение. В современных условиях классическая юрисдикция, основанная на Вестфальской модели, оказывается неэффективной в киберпространстве, особенно в отношении облачных ресурсов, что приводит к возникновению серьезных юрисдикционных проблем. В качестве типичного примера можно привести киберпреступление, совершенное с использованием вычислительных мощностей в облаке из одной страны и хранилищ, расположенных в другой стране, при этом поставщик облачных услуг зарегистрирован в третьей стране, а пользователь (жертва и злоумышленник), чьи данные хранятся у поставщика услуг, может быть жителем четвертой страны. Очевидно, что в такой ситуации крайне сложно определить юрисдикцию на основании классических территориальных моделей. В связи с вышеизложенным Индия предлагает утвердить в Конвенции юрисдикцию, ориентированную на данные, вместо юрисдикции на основе территориальных моделей. Право собственности на данные, связанное с неприкосновенностью частной жизни, является признанным основополагающим правом граждан всего мира. Это подтвердил Суд Европейского союза, признавший право физических лиц на забвение. Право на неприкосновенность частной жизни также связано с правами человека, на что

указывали многие страны в Специальном комитете, и юрисдикция, ориентированная на данные, поможет защитить право на неприкосновенность частной жизни, основные права и права человека.)

15. «Юрисдикция» может быть определена следующим образом

1. Каждое государство-участник принимает такие меры, какие могут быть необходимы в целях установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда:

а) преступление совершено на территории этого государства-участника или затрагивает территорию государства-участника; или

б) преступление совершено на борту судна, плавающего под флагом этого государства-участника, или воздушного судна, зарегистрированного согласно законам этого государства-участника на момент совершения преступления.

2. При условии соблюдения настоящей Конвенции государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, когда:

а) преступление совершено против гражданина и юридического лица этого государства-участника; или

б) преступление совершено гражданином и юридическим лицом этого государства-участника или лицом без гражданства, которое обычно проживает на его территории; или

с) преступление совершено за пределами его территории в целях совершения какого-либо преступления, признанного таковым в соответствии с Конвенцией, на его территории;

d) преступление совершено против этого государства-участника; или

е) преступление совершено в отношении компьютерных ресурсов, расположенных на его территории;

ф) преступление касается цифровых/электронных данных граждан государства-участника, независимо от того, где осуществляется физическое хранение/обработка/проверка/объединение этих данных.

3. Для целей настоящей Конвенции каждое государство-участник принимает такие меры, какие могут быть необходимы для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории, и оно не выдает такое лицо лишь на том основании, что оно является одним из его граждан.

4. Каждое государство-участник может также принять такие меры, какие могут быть необходимы в целях установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории, и оно не выдает его.

5. Если государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что какие-либо другие государства-участники осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием, компетентные органы этих государств-участников проводят в надлежащих случаях консультации друг с другом для координации своих действий. В целях проведения консультаций в соответствии с настоящей статьей Договаривающиеся Стороны принимают во внимание юрисдикцию, ориентированную на данные, то есть на данные, принадлежащие жертве

киберпреступления или противоправного деяния, совершенного с использованием информационно-коммуникационных технологий.

6. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной юрисдикции, установленной государством-участником в соответствии со своим внутренним законодательством.

17. Обыск и выемка информации, хранимой или обрабатываемой в электронной форме

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления ее компетентным органам полномочий на обыск или получение аналогичного доступа к:

- а) компьютерной системе или ее части, а также хранимой в ней информации в электронной форме; и
- б) находящемуся на ее территории носителю информации, на котором может храниться информация в электронной форме.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы в случае, когда ее органы власти проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (а) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на ее территории, и существует законная возможность получить доступ к таким данным в первоначальной системе или из нее, органы власти должны иметь возможность оперативно распространить обыск или аналогичный доступ на эту другую систему.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления ее компетентным органам полномочий производить выемку или иным аналогичным образом обеспечивать сохранность информации в электронной форме, доступ к которой был получен в соответствии с пунктом 1 или 2. Эти меры включают предоставление полномочий для:

- а) проведения изъятия или обеспечения аналогичной защиты компьютерной системы или ее части, или носителя информации в электронной форме;
- б) изготовления и сохранения копии этой информации в электронной форме;
- с) сохранения/поддержания целостности информации в электронной форме.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления ее компетентным органам полномочий привлекать любое лицо, обладающее специальными знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты информации в электронной форме, для предоставления, если это целесообразно, необходимых сведений, с тем чтобы обеспечить осуществление действий, предусмотренных пунктами 1 и 2.

18. Сбор технических параметров трафика в режиме реального времени

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления ее компетентным органам полномочий:

- а) собирать или записывать с применением технических средств на территории этой Стороны; и

b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:

- i) собирать или записывать с применением технических средств на территории этой Стороны; или
- ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени технические параметры трафика, связанные с определенными средствами связи на ее территории и передаваемые с помощью компьютерной системы.

2. Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные в пункте 1 (a), то вместо этого она может принять законодательные и иные меры, которые могут быть необходимы для обеспечения сбора или записи в режиме реального времени технических параметров трафика, связанных с определенными средствами связи и передаваемых на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой относящейся к этому информации.

19. Сбор контента и метаданных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для оперативного предоставления метаданных без необходимости заключения договоров о взаимной правовой помощи. Поставщик услуг, располагающий такими метаданными, предоставляет такую информацию по прямому запросу правоохранительных органов через уполномоченный центральный орган каждого государства.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для оперативного предоставления данных о контенте. В рамках настоящей Конвенции будет разработан механизм такого оперативного обмена данными.

20. Перехват данных о контенте

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы в отношении ряда серьезных правонарушений, признанных таковыми в соответствии с ее внутренним законодательством, с тем чтобы уполномочить свои компетентные органы:

a) собирать или записывать с применением технических средств на территории этой Стороны; и

b) обязать поставщика услуг в пределах, имеющихся у него технических возможностей:

- i) собирать или записывать с применением технических средств на территории этой Стороны; или
- ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные о контенте определенных сообщений, передаваемых на ее территории с помощью компьютерной системы.

2. Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные в пункте 1 (a), то вместо этого она может принять законодательные и иные меры, которые могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о контенте, связанных с определенными

сообщениями, передаваемыми на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой относящейся к этому информации.

21. Оперативное обеспечение сохранности накопленной информации в электронной форме

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы ее компетентные органы имели возможность отдавать распоряжения или схожим образом оперативно обеспечивать сохранность конкретной информации в электронной форме, включая технические параметры трафика и данные о контенте, сохраняемые посредством компьютерной системы, в частности в случаях, когда имеются основания полагать, что эта информация в электронной форме особо подвержена риску утраты или модификации.

2. Если Сторона реализует положения приведенного выше пункта 1 посредством отдания распоряжения какому-либо лицу об обеспечении сохранности конкретной информации, хранимой в электронной форме и находящейся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать данное лицо хранить и обеспечивать целостность этой информации в электронной форме в течение необходимого периода времени, не превышающего 180 суток, с тем чтобы компетентные органы могли добиться раскрытия этих данных. Сторона может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать хранителя или иное лицо, на которое возложена обязанность обеспечения сохранности информации в электронной форме, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

4. Каждая сторона создает центральный координационный орган, обеспечивающий выполнение такого запроса о сохранении данных другим государством.

Ямайка (от имени Карибского сообщества)

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

Глава 1. Общие положения

Статья. Общие положения

Целями настоящей Конвенции являются:

1. Содействие принятию и укреплению мер, направленных на более эффективное и действенное предупреждение преступлений и иных противоправных деяний, направленных против конфиденциальности, целостности и доступности систем информационно-коммуникационных технологий и информации в электронной форме, и на борьбу с ними;

2. Поощрение, обеспечение и поддержка международного сотрудничества и технической помощи в рамках предупреждения уголовных преступлений и иных противоправных деяний, направленных на подрыв конфиденциальности, целостности и доступности систем информационно-коммуникационных технологий и информации в электронной форме, и борьбы с ними;

3. Поощрение, обеспечение и поддержка международного сотрудничества и технической помощи в принятии мер по возвращению активов, приобретенных в результате уголовных преступлений и иных противоправных деяний, упомянутых в настоящей Конвенции.

Статья. Сфера применения

1. Настоящая Конвенция применяется в соответствии с ее положениями к предупреждению уголовных преступлений и преследованию за них, поощрению, обеспечению и поддержке международного сотрудничества в деле предупреждения и пресечения использования информационно-коммуникационных технологий для совершения уголовных преступлений, а также к замораживанию, аресту, конфискации и возвращению доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

2. Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не обязательно, чтобы в результате совершения уголовных преступлений, признанных таковыми в соответствии с ее положениями, был причинен ущерб или вред лицам, имуществу и государству.

Статья. Защита суверенитета

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

2. Ничто в настоящей Конвенции не наделяет государство-участника правом осуществлять на территории другого государства-участника или государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства-участника или государства в соответствии с его внутренним законодательством и в соответствии с нормами международного права и текущими обязательствами.

Глава 2. Криминализация

Статья. Незаконный/несанкционированный доступ к компьютерной системе или данным

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния доступ ко всей компьютерной системе или к любой ее части, когда он совершается умышленно и противоправным образом. Государство-участник может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением или несоблюдением мер безопасности, либо с умыслом на завладение информацией в электронной форме или с другим бесчестным умыслом, либо в отношении компьютерной системы, которая соединена с другой компьютерной системой. *(На основании Будапештской конвенции, статья 2 — Незаконный доступ)*

Статья. Незаконный/несанкционированный перехват

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, неправомерный или несанкционированный перехват компьютерной системы или данных, осуществляемый с применением технических средств для перехвата технических параметров трафика и данных, обрабатываемых с помощью информационных коммуникационных технологий и не предназначенных для общественного пользования, включая электромагнитные излучения от компьютерной системы, содержащей такую информацию в электронной форме.

2. Государство-участник может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья. Незаконное воздействие на данные

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправный или несанкционированный ввод, повреждение, удаление, порчу, изменение или блокировку информации в электронной форме.

2. Государство-участник может оставить за собой право требовать, чтобы деяния, описанные в пункте 1, считались преступными при наличии серьезного ущерба.

Статья. Незаконное воздействие на систему

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное или несанкционированное препятствование функционированию системы информационно-коммуникационных технологий путем ввода, передачи, повреждения, удаления, порчи, изменения или блокировки информации в электронной форме.

2. Каждое государство-участник может оставить за собой право ужесточить наказание, если деяния, обозначенные в пункте 1, затрагивают или повреждают критическую инфраструктуру.

Статья. Неправомерное использование устройств/вредоносного программного обеспечения/компьютерных программ

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправным образом:

a) производство, продажу, приобретение для использования, импорт, распространение или предоставление в пользование иным способом:

i) устройств, включая компьютерные программы, разработанные или адаптированные преимущественно для совершения каких-либо уголовных преступлений, признанных таковыми в соответствии со статьями (несанкционированный/незаконный доступ, несанкционированный/незаконный перехват/воздействие на данные/воздействие на систему);

ii) компьютерного пароля, кода доступа или аналогичных данных, позволяющих получить доступ ко всей или любой части информационной, коммуникационной и технологической системы с намерением использовать их для совершения каких-либо уголовных преступлений, признанных таковыми в соответствии со статьями (несанкционированный/незаконный доступ, несанкционированный/незаконный перехват/воздействие на данные/воздействие на систему); и

b) владение предметами, указанными в подпунктах (a)(i) или (ii) выше, с намерением использовать их для совершения каких-либо уголовных преступлений, признанных таковыми в соответствии со статьями (несанкционированный/незаконный доступ, несанкционированный/незаконный перехват/воздействие на данные/воздействие на систему). Государство-участник может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось обладание несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иные формы предоставления в пользование или владение, упомянутые в пункте 1 настоящей статьи, не преследуют цель совершения уголовных преступлений, признанных таковыми в соответствии со статьями (несанкционированный/незаконный доступ, несанкционированный/незаконный перехват/воздействие на данные/воздействие на систему) настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждое государство-участник может оставить за собой право не применять пункт 1 настоящей статьи при условии, что эта оговорка не будет касаться продажи, распространения или иных форм предоставления в пользование предметов, указанных в пункте 1 (a) ii) настоящей статьи.

Статья. Преступления, связанные с содержанием данных

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправным образом:

a) производство материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми с помощью системы информационно-коммуникационных технологий;

b) предложение или предоставление в пользование материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми с помощью системы информационно-коммуникационных технологий;

c) распространение или передачу материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми с помощью системы информационно-коммуникационных технологий;

d) приобретение материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми для себя или для другого лица с помощью компьютерной системы/системы информационно-коммуникационных технологий;

e) хранение материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми в компьютерной системе/системе информационно-коммуникационных технологий или на компьютерном носителе данных.

2. Для целей пункта 1 выше в понятие «материалы с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми» включаются материалы, которые визуально изображают:

a) участие ребенка в откровенных сексуальных действиях;

b) участие лица, кажущегося ребенком, в откровенных сексуальных действиях;

c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

3. Для целей пункта 2 выше термин «ребенок» относится к каждому человеческому существу до достижения им возраста восемнадцати (18) лет, если по закону, применимому к данному ребенку, он не достигает совершеннолетия ранее. *(Конвенция о правах ребенка, статья 1)*

Статья. Нарушение неприкосновенности частной жизни/распространение изображений сексуального характера без согласия изображенного лица

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправным образом:

а) умышленную публикацию, распространение, передачу, продажу, предоставление в пользование или рекламу интимных изображений лица, когда известно, что лицо, запечатленное на этом изображении, не давало своего согласия на эти действия;

б) публикацию, распространение, передачу, продажу, предоставление в пользование или рекламу интимных изображений лица, осуществляемые с намерением оскорбить лицо, запечатленное на этом изображении, или причинить ему вред.

Определение понятия «интимное изображение»

2. В настоящей статье «интимное изображение» означает видеофиксацию какого-либо лица, осуществленную любым способом, включая фотосъемку, киносъемку или видеозапись:

а) в которой данное лицо обнажено, обнажает свои половые органы, анальную область или грудь, или участвует в откровенных сексуальных действиях;

б) в отношении которой на момент фиксации существовали обстоятельства, дающие разумные основания рассчитывать на сохранение конфиденциальности; и

с) в отношении которой изображенное лицо сохраняет разумные основания рассчитывать на сохранение конфиденциальности на момент совершения преступления.

Статья. Интеллектуальная собственность

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать уголовным преступлением нарушение авторских и смежных прав, как они определены в законодательстве этого государства-участника, когда такие деяния совершаются умышленно с использованием информационно-коммуникационных технологий и в коммерческих масштабах.

Преступления, связанные с использованием компьютерных средств

Статья. Подлог с использованием компьютерных технологий

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправным образом, ввод, изменение, удаление или блокировку информации в электронной форме, влекущие за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными.

2. Государство-участник может требовать, чтобы условием наступления уголовной ответственности являлся умысел на мошенничество или аналогичный бесчестный умысел.

Статья. Мошенничество с использованием компьютерных технологий

1. Каждое государство-участник принимает такие законодательные и другие меры, какие могут быть необходимы для того, чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное или несанкционированное лишение другого лица его имущества путем:

а) любого введения, изменения, стирания или блокировки информации в электронной форме;

б) любого воздействия на функционирование компьютерной системы;

с мошенническим или бесчестным умыслом извлечения экономической выгоды для себя или для другого лица.

Статья. Незавершенные преступления

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния участие в любом качестве, например, в качестве сообщника, пособника, подстрекателя, соучастника или заговорщика, в совершении какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

2. Каждое государство-участник может принять такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния любое покушение на совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния приготовление к совершению какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

Статья. Ответственность юридических лиц

1. Каждое государство-участник принимает такие меры, какие могут быть необходимы, согласно его правовым принципам, для установления ответственности юридических лиц за участие в совершении уголовного преступления, признанного таковым в соответствии с настоящей Конвенцией и совершенного в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

а) полномочий представлять данное юридическое лицо;

б) права принимать решения от имени этого юридического лица;

с) права осуществлять надзор или контроль внутри этого юридического лица.

2. В дополнение к случаям, уже предусмотренным пунктом 1 настоящей статьи, каждое государство-участник принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение преступления или иного противоправного деяния, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании предоставленных ему явно выраженных или подразумеваемых полномочий.

3. В зависимости от внутреннего законодательства государства-участника ответственность юридических лиц может быть уголовной, гражданско-правовой или административной.

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

5. 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.

Статья. Санкции и меры

1. Каждое государство-участник предусматривает применение уголовных санкций за совершение какого-либо уголовного преступления, признанного таковым в соответствии с настоящей Конвенцией, соразмерных тяжести этого преступления и являющихся эффективными, пропорциональными и оказывающими сдерживающее воздействие, в том числе предусматривающими лишение свободы.

2. Каждое государство-участник обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии со статьей (Ответственность юридических лиц), эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций или мер, включая денежные санкции.

Глава 3. Процессуальное право и правоприменение

Статья. Сфера применения процессуальных норм

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для установления полномочий и процедур, предусмотренных в настоящей главе, в целях проведения уголовного расследования или осуществления судебного разбирательства.

2. За исключением случаев, когда положениями статьи (Перехват сообщений) предусматривается иное, каждое государство-участник применяет полномочия и процедуры, упомянутые в пункте 1 настоящей статьи, в отношении:

- а) уголовных преступлений, признанных таковыми в соответствии со статьями (положениями о криминализации) настоящей Конвенции;
- б) иных уголовных преступлений, совершенных с использованием информационных, коммуникационных и технологических систем; и
- с) сбора доказательств в электронной форме, свидетельствующих о совершении уголовного преступления.

3. Каждое государство-участник может сохранить за собой право применять меры, предусмотренные статьей (Сбор данных в режиме реального времени), только в отношении уголовных преступлений или категорий уголовных преступлений, указанных в этой оговорке, при условии, что круг таких преступлений не более ограничен, чем круг уголовных преступлений, к которым государство-участник применяет меры, предусмотренные статьей (Перехват данных о контенте).

4. В том случае, когда государство-участник ввиду ограничений, предусмотренных его законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьей (Сбор данных в режиме реального времени) и статьей (Перехват данных о контенте), к сообщениям, передаваемым по компьютерной системе поставщика услуг, которая:

- i) используется для обслуживания отдельной группы пользователей; и
- ii) не использует сети связи общего пользования и не соединена с другой компьютерной системой, как общего доступа, так и частной;

это государство-участник может сохранить за собой право не применять указанные меры к таким сообщениям.

5. Каждое государство-участник рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, предусмотренных статьями (Сбор данных в режиме реального времени и Перехват данных о контенте).

Статья. Условия и гарантии

1. Каждое государство-участник обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящей статьей, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами его внутреннего законодательства, обеспечивающими надлежащую защиту прав и свобод человека, включая права, вытекающие из обязательств, которые государство-участник взяло на себя по Международному пакту о гражданских и политических правах 1966 года и по другим применимым международным договорам по правам человека.

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 таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности, надлежащему отправлению правосудия, государство-участник рассматривает влияние указанных в данной статье полномочий и процедур на права, ответственность и законные интересы третьих лиц.

Статья. Оперативное обеспечение сохранности информации в электронной форме

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы его компетентные органы имели возможность отдавать соответствующие распоряжения или схожим образом оперативно обеспечивать получение, сбор и сохранность конкретной информации в электронной форме, включая технические параметры трафика, в частности, в случаях, когда имеются основания полагать, что эти данные особенно подвержены риску удаления, модификации или утраты.

2. Если государство-участник реализует указанные выше положения пункта 1 посредством дачи распоряжения какому-либо лицу, в том числе юридическому, об обеспечении сохранности конкретной информации, хранимой в электронной форме и находящейся во владении или под контролем этого лица, то это государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать это лицо хранить эту информацию в электронной форме и обеспечивать ее целостность в течение необходимого периода времени, однако не более срока, установленного внутренним законодательством этого государства-участника, с тем чтобы компетентные органы могли добиться раскрытия этих данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать лицо, на которое возложена обязанность по обеспечению сохранности информации, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей (Сфера применения процессуальных норм и Условия и гарантии).

Статья. Оперативное обеспечение сохранности и частичное раскрытие данных о технических параметрах трафика

1. Каждое государство-участник принимает в отношении технических параметров трафика, сохранность которых должна быть обеспечена в соответствии с положениями статьи (Оперативное обеспечение сохранности информации в электронной форме), такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

а) гарантировать, чтобы такое оперативное обеспечение сохранности технических параметров трафика было возможным независимо от того, вовлечены ли в передачу данных сообщений один или несколько поставщиков услуг; и

б) гарантировать оперативное раскрытие компетентным органам этого государства-участника или лицу, назначенному этими органами, достаточного количества технических параметров трафика, которое позволит соответствующему государству-участнику идентифицировать поставщиков услуг и путь, которым передавались указанные сообщения.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются на основании статей (Сфера применения процессуальных норм и Условия и гарантии).

Статья. Распоряжение о предоставлении информации

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий отдавать следующие распоряжения при наличии разумных оснований полагать, что было совершено или совершается уголовное преступление:

а) лицу, в том числе юридическому лицу, находящемуся на его территории, о предоставлении находящейся во владении или под контролем этого лица информации в электронной форме, хранимой в компьютерной системе или на носителе информации в электронной форме; и

б) поставщику услуг, предлагающему свои услуги на этой территории государства-участника, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах, которые имеют отношение к этим услугам.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей (Сфера применения процессуальных норм и Условия и гарантии).

3. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах, кроме технических параметров трафика или содержания информации, с помощью которых можно определить:

а) вид используемых информационно-коммуникационных услуг, принятые с этой целью меры технического обеспечения и период предоставления услуги;

б) личность пользователя, его почтовый или географический адрес, номера телефонов и других средств связи, включая IP-адреса, сведения о выставленных ему счетах и произведенных им платежах в рамках соглашения или договора на обслуживание;

с) сведения о месте установки информационно-коммуникационного оборудования, имеющего отношение к соглашению или договору на его обслуживание.

Статья. Обыск и выемка информации, хранимой или обрабатываемой в электронной форме

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам, при наличии разумных оснований полагать, что было совершено или совершается уголовное преступление, полномочий на проведение обыска или получение аналогичного доступа к:

- а) системе информационно-коммуникационных технологий или ее части и хранящейся в ней информации в электронной форме; и
- б) находящемуся на его территории носителю информации, на котором может храниться информация в электронной форме.

2. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы в случае, когда его органы власти проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (а) и имеют разумные основания полагать, что искомые данные хранятся в иной компьютерной системе или ее части на его территории, и такие данные либо доступ к ним можно законно получить из первоначальной системы, органы власти могли бы оперативно распространить право проведения обыска или получения аналогичного доступа на эту иную систему.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий производить выемку или иным аналогичным образом обеспечивать сохранность информации в электронной форме, доступ к которой был получен в соответствии с пунктом 1 или 2. Эти меры включают предоставление полномочий:

- а) производить выемку или иным аналогичным образом обеспечивать сохранность компьютерной системы или ее части, или носителя информации в электронной форме;
- б) изготавливать и сохранять копию этой информации в электронной форме;
- с) обеспечивать целостность относящейся к делу хранимой информации в электронной форме;
- д) закрывать доступ к информации в электронной форме, имеющейся в компьютерной системе, к которой был получен доступ, или изымать такую информацию из этой системы.

4. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий привлекать любое лицо, обладающее специальными знаниями о функционировании соответствующей компьютерной системы или о применяемых мерах защиты содержащейся в ней информации в электронной форме, для предоставления, если это целесообразно, необходимых сведений с тем, чтобы обеспечить принятие мер, предусмотренных пунктами 1, 2 и 3.

5. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются на основании статей (Сфера применения процессуальных норм и Условия и гарантии).

Статья. Сбор технических параметров трафика в режиме реального времени

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий, при наличии разумных оснований полагать, что было совершено или совершается уголовное преступление:

- a) собирать или записывать с применением технических средств на территории этой Стороны; и
- b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:
 - i) собирать или записывать с применением технических средств на территории этой Стороны; или
 - ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени технические параметры трафика, связанные с определенными средствами связи на ее территории и передаваемые с помощью компьютерной системы.

2. Если какое-либо государство-участник в силу своего внутреннего законодательства не может принять меры, предусмотренные в пункте 1 (a), то вместо этого оно может принять такие законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени технических параметров трафика, связанных с определенными средствами связи и передаваемых на его территории путем применения технических средств на этой территории.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются на основании статей (Сфера применения процессуальных норм и Условия и гарантии).

Статья. Перехват данных о контенте

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий предпринять следующие действия в отношении ряда серьезных уголовных преступлений, определенных внутренним законодательством этого государства, при наличии разумных оснований полагать, что было совершено или совершается уголовное преступление:

- a) осуществлять сбор, запись или хранение с применением технических средств на территории этой Стороны и
- b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:
 - i) осуществлять сбор, запись или хранение с применением технических средств на территории этой Стороны или
 - ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные о содержании определенных сообщений, передаваемых на ее территории с помощью компьютерной системы.

2. Если какое-либо государство-участник в силу своего внутреннего законодательства не может принять меры, предусмотренные в пункте 1 (a), то вместо этого оно может принять такие законодательные и иные меры, которые могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о содержании определенных сообщений, передаваемых на его территории, путем применения технических средств на этой территории.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются на основании статей (Сфера применения процессуальных норм и Условия и гарантии).

Малайзия

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

Глава I. Общие положения

Статья 1. Цель

Целями настоящей Конвенции являются:

- a) содействие принятию и укреплению мер, направленных на более эффективное и действенное предупреждение киберпреступности и борьбу с ней;
- b) поощрение и облегчение международного сотрудничества;
- c) содействие наращиванию потенциала и оказанию технической помощи для укрепления способности государств-членов противодействовать киберпреступности; и
- d) обеспечение надлежащего баланса между интересами правоприменения и соблюдением основных прав человека.

Статья 2. Употребление терминов

Применительно к настоящей Конвенции:

- a) «Ребенок» означает любое лицо в возрасте до 18 лет.
- b) «Компетентный орган» означает судебный, административный или другой правоохранительный орган, который в соответствии с внутренним законодательством уполномочен отдавать распоряжения, санкционировать или предпринимать действия по исполнению мер, предусмотренных настоящей Конвенцией, в отношении проведения уголовных расследований или уголовного преследования.
- c) «Компьютер» означает электронное, магнитное, оптическое, электрохимическое или иное устройство обработки данных или группу таких взаимосвязанных или связанных устройств, выполняющих функции логических и арифметических вычислений, запоминания и отображения, и включает любое средство хранения данных или средство связи, непосредственно связанное или работающее в сочетании с таким устройством или группой таких взаимосвязанных или связанных устройств, но не включает автоматическую пишущую машинку или наборное устройство, или портативный ручной калькулятор или другие подобные устройства, не являющиеся программируемыми устройствами или не содержащими никаких средств хранения данных.
- d) «Киберпреступления» означают преступления, признанные таковыми в соответствии с настоящей Конвенцией.
- e) «Данные» означают представление информации или понятий, которые подготавливаются или были подготовлены в форме, пригодной для использования в компьютере.
- f) «Функция» включает логические функции, функции контроля, арифметические функции, функции удаления, хранения и извлечения, а также функции связи или электросвязи с компьютером, из него или внутри него.

g) «Программа» означает данные, представляющие собой инструкции или операторы, которые при исполнении их в компьютере обеспечивают выполнение компьютером определенной функции.

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. В указанных в настоящей Конвенции случаях она может также применяться к сбору доказательств в электронной форме, свидетельствующих о совершении уголовного преступления.
3. Предоставление и оказание технической помощи и наращивание потенциала по вопросам, охватываемым 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 или функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством.

Глава II. Криминализация и правоприменение

Статья 5. Несанкционированный доступ

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, несанкционированный доступ любого лица в какой-либо форме к какой-либо программе или данным, находящимся в компьютере.

Статья 6. Несанкционированный перехват

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, несанкционированный перехват данных или сообщений каким-либо лицом любым способом.

Статья 7. Воздействие на данные

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в своем внутреннем законодательстве в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправное повреждение, удаление, порчу или изменение информации в электронной форме.
2. Государство-участник может оставить за собой право потребовать, чтобы под такими преступлениями подразумевались описанные в пункте 1 деяния, приведшие к серьезному ущербу.

Статья 8. Создание помех для компьютера, программы или данных

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, создание серьезных помех для компьютерной программы или данных путем вмешательства,

прерывания функционирования, блокировки, создания препятствий, воспрепятствования доступу или повреждения.

Статья 9. Неправомерное использование данных, программы или компьютера

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправным образом, производство, адаптацию, продажу, приобретение для использования, импорт, предложение, распространение, поставку или предоставление для использования иным способом любых данных, программ или компьютеров.

Статья 10. Преступления, связанные с детской порнографией

1. Признать в качестве уголовно наказуемых деяний следующие действия, когда они совершаются умышленно и противоправным образом:

а) изготовление, производство или руководство изготовлением любой детской порнографии в целях ее распространения с использованием компьютерной системы;

б) использование или побуждение к использованию ребенка в подготовке к изготовлению или производству, или в подготовке к руководству изготовлением или производством, или в изготовлении или производстве, или в руководстве изготовлением или производством детской порнографии в целях ее распространения с использованием компьютерной системы;

с) обмен, публикацию, печать, воспроизведение, продажу, предоставление в аренду, распространение, демонстрацию, рекламу, передачу, продвижение, импорт, экспорт, трансляцию, предложение или предоставление в пользование какой-либо детской порнографии с использованием компьютерной системы;

д) приобретение, сбор или поиск какой-либо детской порнографии с использованием компьютерной системы;

е) участие в любой предпринимательской деятельности, которая, насколько знает или имеет основания полагать данное лицо, связана с какой-либо детской порнографией с использованием компьютерной системы, или извлечение прибыли из такой деятельности;

ф) получение доступа к какой-либо детской порнографии, личное владение ею или осуществление контроля над ней с использованием компьютерной системы.

2. Для целей пункта 1 термин «детская порнография» соответствует определению в Факультативном протоколе к Конвенции о правах ребенка, касающемся торговли детьми, детской проституции и детской порнографии.

Статья 11. Покушение, пособничество и подстрекательство

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния подстрекательство к участию или 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 принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния любое покушение на совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

3. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния подготовку к совершению какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

Статья 12. Ответственность юридических лиц

1. Каждое государство-участник принимает такие меры, какие, с учетом его правовых принципов, могут быть необходимы для установления ответственности юридических лиц за участие в преступлениях, признанных таковыми в соответствии с 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.

Статья 13. Преследование, вынесение судебного решения и санкции

1. Каждое государство-участник за совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, предусматривает применение таких уголовных санкций, которые учитывают степень опасности этого преступления.

2. Каждое государство-участник стремится обеспечить использование любых предусмотренных в его внутреннем законодательстве дискреционных юридических полномочий, относящихся к уголовному преследованию лиц за преступления, охватываемые настоящей Конвенцией, для достижения максимальной эффективности правоохранительных мер в отношении этих преступлений и с должным учетом необходимости воспрепятствовать совершению таких преступлений.

3. Применительно к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, каждое государство-участник принимает надлежащие меры, в соответствии со своим внутренним законодательством и с должным учетом прав защиты, в целях обеспечения того, чтобы условия, устанавливаемые в связи с решениями об освобождении до суда или до принятия решения по кассационной жалобе или протесту, учитывали необходимость обеспечения присутствия обвиняемого в ходе последующего уголовного производства.

4. Каждое государство-участник обеспечивает, чтобы его суды или другие компетентные органы учитывали опасный характер преступлений, охватываемых настоящей Конвенцией, при рассмотрении вопроса о возможности досрочного или условного освобождения лиц, осужденных за такие преступления.

5. Ничто, содержащееся в настоящей Конвенции, не затрагивает принцип, согласно которому определение преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и применимых юридических возражений или других правовых принципов, определяющих правомерность деяний, входит в сферу внутреннего законодательства каждого государства-участника, а уголовное преследование и наказание за такие преступления осуществляются в соответствии с этим законодательством.

Глава III. Уголовное судопроизводство и правоприменение

Статья 14. Сфера применения процессуальных мер

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для установления полномочий и процедур, предусмотренных в настоящей главе, в целях проведения уголовного расследования или осуществления судебного разбирательства.

2. За исключением конкретных случаев, предусматривающих иное, каждое государство-участник применяет полномочия и процедуры, упомянутые в пункте 1 настоящей статьи, в отношении:

- a) уголовных преступлений, признанных таковыми в соответствии с определениями преступлений в настоящей Конвенции;
- b) иных уголовных преступлений, совершаемых с использованием компьютерной системы; и
- c) сбора доказательств в электронной форме, свидетельствующих о совершении уголовного преступления.

Статья 15. Распоряжение о предоставлении информации

Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для наделения его компетентных органов полномочиями предписывать пребывающему на его территории лицу представить определенную информацию в электронной форме, находящуюся во владении или под контролем этого лица и хранящуюся в компьютерной системе или на носителе информации в электронной форме.

Статья 16. Обыск и выемка информации, хранящейся в электронной форме

Каждое государство-участник принимает такие меры, какие могут быть необходимы для предоставления его компетентным органам полномочий на проведение обыска, выемки и удержания каких-либо доказательств, и компетентные органы имеют право использовать любую программу или данные, хранящиеся в любом компьютере, или получать доступ к любому компьютеру, осматривать или проверять работу любого компьютера и любого связанного с ним оборудования или материала, который, как компетентные органы имеют разумные основания предполагать, используется или использовался в связи с совершением какого-либо преступления, признанного таковым в настоящей Конвенции.

Статья 17. Юрисдикция

1. Каждое государство-участник принимает такие меры, какие могут быть необходимы, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда:

- a) преступление совершено на территории этого государства-участника; или
- b) преступление совершено на борту судна, плавающего под флагом этого государства-участника, или воздушного судна, зарегистрированного согласно законам этого государства-участника на момент совершения преступления.

2. При условии соблюдения статьи настоящей Конвенции о суверенитете государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, когда:

- a) преступление совершено против гражданина этого государства-участника; или
- b) преступление совершено гражданином этого государства-участника; или

с) преступление совершено против этого государства-участника.

3. Для целей статьи настоящей Конвенции, касающейся экстрадиции, каждое государство-участник принимает такие меры, какие могут быть необходимы, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории, и оно не выдает такое лицо лишь на том основании, что оно является одним из его граждан.

4. Каждое государство-участник может также принять такие меры, какие могут быть необходимы, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории, и оно не выдает его.

5. Если государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что какие-либо другие государства-участники осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием, компетентные органы этих государств-участников проводят в надлежащих случаях консультации друг с другом в целях координации своих действий.

6. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной юрисдикции, установленной государством-участником в соответствии со своим внутренним законодательством.

Статья 18. Права потерпевших

1. Каждое государство-участник устанавливает надлежащие процедуры для обеспечения доступа к компенсации потерпевшим от преступлений, охватываемых настоящей Конвенцией.

2. Каждое государство-участник, при условии соблюдения своего внутреннего законодательства, создает возможности для изложения и рассмотрения мнений и опасений потерпевших на соответствующих стадиях уголовного производства в отношении лиц, совершивших преступления, таким образом, чтобы это не наносило ущерба правам защиты.

Сингапур

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

Общие положения

Термины и определения

2. С самого начала следует дать четкие определения терминов, которые будут использоваться в Конвенции. В частности, есть два ключевых термина, предложенных для описания предмета Конвенции, а именно «киберпреступность» и «использование информационно-коммуникационных технологий в преступных целях». Получивший широкое признание термин «киберпреступность» включает «киберпреступления, совершаемые с помощью компьютерных технологий» и «киберпреступления, совершаемые в информационной среде». Второй термин — «использование информационных и коммуникационных технологий в преступных целях» — охватывает широкий спектр связанных с коммуникационными технологиями вопросов, выходящий за рамки «киберпреступности».

3. Сингапур считает, что в основу Конвенции должен быть положен термин «киберпреступность», поскольку это общепринятый термин, охватывающий существующие и возникающие угрозы киберпреступности, с которыми сталкиваются государства-члены. Это позволит направить Конвенцию на преступления, характерные для киберпространства или совершаемые благодаря киберпространству, и принять более прагматичный подход к борьбе с этими угрозами.

4. На первой сессии также обсуждался вопрос о том, какую формулировку следует использовать в Конвенции — «предотвращение и борьба» или «противодействие». Сингапур предпочитает формулировку «предотвращение и борьба», используемую в ранее принятых документах, включая Конвенцию Организации Объединенных Наций против транснациональной организованной преступности.

Конфиденциальность данных

5. Необходимо установить баланс между обеспечением конфиденциальности данных и необходимостью поддержания общественной безопасности, включая борьбу с киберпреступлениями в целях обеспечения безопасности в сети Интернет, и предоставить правоохранительным органам возможность быстро и эффективно принимать необходимые меры для борьбы с киберпреступностью.

Криминализация и правоприменение

6. Следует также включить в Конвенцию кибермошенничество (совершаемое с помощью компьютерных технологий или в информационной среде), поскольку этот вид мошенничества составляет несоразмерно высокую долю от всех остальных видов мошенничества в современном мире. Только в Сингапуре в 2021 году жертвы мошенничества потеряли не менее 633,3 млн долл. США, причем число случаев мошенничества увеличилось на 52,9 процента по сравнению с предыдущим годом и составило более половины всех преступлений. Мошеннические синдикаты располагают большими ресурсами и используют технологии для совершения мошенничества в обход государственных границ и для заматывания следов.

7. Редакционные предложения Сингапура представлены ниже. Мы считаем, что наши предложения создают реалистичные и разумные исходные позиции для направления настоящей Конвенции на борьбу с основными видами кибермошенничества.

Незаконный доступ

1. Каждое государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния противоправный доступ ко всей компьютерной системе или к любой ее части, когда он совершается умышленно.

2. Государство-участник может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с умыслом на завладение информацией в электронной форме или с другим бесчестным умыслом, например, на присвоение личности другого лица, или в отношении компьютерной системы, которая связана с другой компьютерной системой.

Кибермошенничество

Каждое государство-участник принимает такие законодательные и другие меры, какие могут быть необходимы для того, чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно и противоправным образом, лишение другого лица или организации имущества путем:

а) любого ввода, изменения, удаления или блокировки информации в электронной форме;

- b) любого воздействия на функционирование компьютерной системы;
- c) противоправного использования компьютерной системы для обмана или побуждения другого лица или организации к какому-либо действию или бездействию, которого это лицо или организация в противном случае не совершили или не допустили, с мошенническим или бесчестным намерением получить для себя или для другого лица:
 - i) экономическую выгоду; и/или
 - ii) информацию в электронной форме или персональные данные, которые в противном случае не стали бы доступны лицу, совершившему преступление.

Незаконный доступ к паролям и учетным данным

Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы признать в своем внутреннем законодательстве в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправное приобретение, присвоение, получение или распространение паролей или учетных данных, обеспечивающих противоправный доступ к компьютерной системе или к информации в электронной форме.

Процессуальные меры и правоприменение

Сохранение, сбор, получение электронных доказательств и данных и обмен ими

8. Мы хотели бы высказать три соображения в отношении сохранения, сбора, получения электронных доказательств и данных и обмена ими:

a) Поскольку все больше данных хранится в облаке и все больше операций осуществляется в цифровом формате, цифровые доказательства фигурируют в подавляющем большинстве уголовных расследований, особенно связанных с киберпреступлениями. Если не обеспечить своевременное сохранение, сбор и получение цифровых данных, то при проведении расследований и уголовного преследования возникнут затруднения.

b) Выполнение запросов на получение цифровых доказательств, поступающих по существующим каналам, например, по линии договоров о взаимной правовой помощи (ДВПП) — это длительный процесс. Если не обеспечить своевременное сохранение, сбор и получение цифровых доказательств, то высока вероятность того, что к тому времени, когда страны примут решение об удовлетворении запроса по линии ДВПП, эти доказательства уже будут утрачены. Таким образом, мы выступаем за принятие мер по выполнению законных запросов об оперативном обеспечении сохранности компьютерных данных.

c) Киберпреступность носит трансграничный характер. Благодаря техническим достижениям преступники получили возможность осуществлять свою деятельность дистанционно и в обход государственных границ. Положения о трансграничном обмене электронными доказательствами и данными позволят нашим правоохранительным органам получать реальные улики для проведения своих расследований, а также будут способствовать успешному задержанию и последующему судебному преследованию преступников и возвращению активов. Конвенция должна предоставить Сторонам возможность отклонять запросы, если исполнение запроса может нанести ущерб суверенитету, безопасности, общественному порядку или другим существенным интересам запрашиваемой Стороны.

9. Кроме того, мы отмечаем, что у государств-членов разные правовые системы и что они действуют в разных обстоятельствах, что в конечном счете может повлиять на их способность применять процедурные меры, особенно связанные со сбором и перехватом данных в режиме реального времени. Мы отмечаем, что принятие мер по сохранению, сбору и получению электронных доказательств и данных и обмену ими будет способствовать существенному

повышению эффективности процессов расследования большинства киберпреступлений, особенно по линии многостороннего договора, пользующегося широкой поддержкой государств. Поэтому нам следует избегать слишком жестких предписаний в отношении оперативной деятельности, обеспечивая применимость положений Конвенции для большинства государств, что позволит расширить возможности присоединения к Конвенции и ее ратификации. Это позволит нам эффективнее противодействовать киберпреступности на глобальном уровне.

Меры по возвращению активов

10. Сингапур заслушал замечания ряда государств-членов о необходимости создания механизма возврата активов. Мы с ними согласны. Группы киберпреступников проводят сложные транснациональные операции, которые сложно обнаружить или пресечь. Они располагают обширными ресурсами и умело используют технологии для заметания следов. При возвращении преступных доходов, уже выведенных за пределы страны, нередко возникают серьезные затруднения.

11. Таким образом, настоящая Конвенция позволяет осуществлять конкретные, своевременные, эффективные и согласованные глобальные меры по возвращению активов, поскольку способность какой-либо страны возратить преступные доходы, уже выведенные за пределы ее юрисдикции, будет зависеть от сотрудничества с зарубежными правоохранительными органами. Очень важно создать условия для совместной работы стран по возвращению активов, с тем чтобы преступные организации не извлекали выгоду из своих преступных доходов и не наращивали свои возможности, потенциал и изощренность операций.

Уругвай

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

1. В настоящей Конвенции учитываются существующие международные документы и усилия на национальном, региональном и международном уровнях по предупреждению и пресечению использования информационно-коммуникационных технологий в преступных целях в соответствии с резолюцией 74/247 Генеральной Ассамблеи.

В связи с этим следует также включить в настоящую Конвенцию положение о связи между Конвенцией и другими уже существующими документами, обращая внимание в том числе на такие вопросы, как приоритетное применение и неисключительный характер документов.

По мнению Уругвая, следует включить в данный текст в качестве общего положения призыв к согласованности действий в рамках системы Организации Объединенных Наций по предотвращению незаконного использования информационно-коммуникационных технологий и борьбе с ним.

2. Следует снабдить Конвенцию гибким механизмом для последующих действий и пересмотра соответствующих мер с учетом достигнутого прогресса и постоянных изменений в данной сфере.

Конвенция должна быть изложена нейтральным техническим языком без формулировок, относящихся к конкретной операционной системе или программному обеспечению, и должна обеспечить более широкий подход, поддающийся толкованию в быстро меняющихся условиях.

По мнению Уругвая, крайне важно включить в Конвенцию положения о формулировании заявлений о толковании, а также предусмотреть гибкую процедуру внесения поправок, облегчающую обновление Конвенции, и механизмы урегулирования споров.

Следует периодически проводить конференцию Сторон для изучения существенных изменений в данной сфере и отражения их в содержании настоящей Конвенции. Руководством к действию может служить пункт 1 статьи 69 Конвенции Организации Объединенных Наций против коррупции:

Конференция государств-участников прилагает все усилия для достижения консенсуса в отношении каждой поправки. Если все усилия по достижению консенсуса были исчерпаны и согласие не было достигнуто, то, в качестве крайней меры, для принятия поправки требуется большинство в две трети голосов государств-участников, присутствующих и участвующих в голосовании на заседании Конференции государств-участников.

3. Следует принимать во внимание возможности привлечения к участию частного сектора, гражданского общества и научных кругов и вклад этих субъектов.

4. В отношении международной юрисдикции Уругвай считает, что вопросы совпадающей юрисдикции двух или более государств следует рассматривать с учетом временного приоритета в расследовании и даты подачи жалобы.

Тем не менее, если государство-участник, осуществляющее свою юрисдикцию в отношении какого-либо преступления, признанного таковым в настоящей Конвенции и совершенного на его территории, на борту судна, плавающего под флагом этой Стороны, или воздушного судна, зарегистрированного согласно законам этой Стороны, получает уведомление или иным образом узнает о том, что любые другие государства-участники осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием, компетентные органы этих государств-участников проводят, в надлежащих случаях, консультации друг с другом в целях координации своих действий.

Сторона также принимает меры, определенные в настоящей Конвенции, если преступник находится на территории ее страны и не может быть выдан на основании его гражданства. Государство, на территории которого находится лицо, совершившее преступления, признанные таковыми в настоящей Конвенции, без дальнейшего промедления передает дело своим компетентным органам в целях судебного преследования в соответствии с законодательством этого государства.

5. Борьба с киберпреступностью — это актуальная и неотложная задача, которую следует решать, принимая во внимание вопросы защиты, уважения и осуществления прав человека и основных свобод.

Все положения настоящей Конвенции следует понимать и применять согласно соответствующим международным обязательствам в области прав человека. Поэтому в преамбулу Конвенции следует включить пункт, вновь подтверждающий Всеобщую декларацию прав человека, Международный пакт о гражданских и политических правах и другие соответствующие документы по правам человека.
