Организация Объединенных Наций A/AC.291/9/Add.2

Генеральная Ассамблея

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

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

Подборка представленных государствами-членами предложений и материалов, касающихся положений о криминализации, общих положений и положений о процессуальных мерах и правоприменении, для включения во всеобъемлющую международную конвенцию о противодействии использованию информационно-коммуникационных технологий в преступных целях

Добавление

V.22-02337 (R) 010622 030622

Просьба отправить на вторичную переработку

Содержание

		Стр.
IV.	Процессуальные меры и правоприменение	3
	Ангола	3
	Австралия	3
	Бразилия	6
	Канада	12
	Колумбия	14
	Египет	15
	Сальвадор	16
	Европейский союз и его государства-члены	22
	Гана	26
	Иран (Исламская Республика)	35
	Япония	36
	Мексика	36
	Новая Зеландия	37
	Норвегия	38
	Российская Федерация, также от имени Беларуси, Бурунди, Китая, Никарагуа и Таджикистана	38
	Южная Африка	45
	Швейцария	54
	Соединенное Королевство Великобритании и Северной Ирландии	57
	Объединенная Республика Танзания	60
	Соединенные Штаты Америки	62
	Венесуэла (Боливарианская Республика)	69
	Вьетнам	70

IV. Процессуальные меры и правоприменение

Ангола

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

Процессуальные нормы и правоприменение

Средства доказывания: документальные доказательства (электронный документ, цифровой документ), экспертное заключение (компьютерная экспертиза).

Средства получения доказательств: поиск в интернете, оперативное обеспечение сохранности данных, оперативное раскрытие данных, судебное постановление о предоставлении доступа к данным, обыск компьютерных данных, выемка компьютерных данных, выемка электронной почты и запись сообщений аналогичного характера, перехват сообщений, скрытые действия (глубокая сеть и темная сеть).

Возвращение активов и лишение активов в пользу государства: арест и конфискация традиционных активов и криптоактивов.

Положения данной главы должны применяться при расследовании и уголовном преследовании лиц, причастных к совершению традиционных преступлений, а не только к киберпреступности.

Для разработки концепций, связанных с данной главой, можно воспользоваться региональными и международными правовыми документами, которые касаются вышеизложенных вопросов[1].

Австралия

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

Связь между криминализацией и процессуальными полномочиями

Австралия признает, что государства, возможно, пожелают обеспечить, чтобы Конвенция укрепила международное сотрудничество в борьбе с давно известными преступлениями, которые связаны или не связаны с киберпреступностью (такими, как причинение вреда или убийство), путем создания правовой базы для запросов и доступа к электронным доказательствам, находящимся в другой юрисдикции, в связи с совершением таких преступлений.

Процессуальные полномочия, следственные полномочия и основа для международного сотрудничества, которые предусмотрены в Конвенции в целях выявления, расследования и уголовного преследования в отношении киберпреступлений, должны применяться к преступлениям, перечисленным в Конвенции, но их применение не должно ограничиваться только этими преступлениями.

Процессуальные полномочия (подробно изложенные ниже), которые предусмотрены в Конвенции, должны применяться в отношении других уголовных преступлений, совершенных с использованием компьютерных систем или цифровых технологий, а также для сбора электронных доказательств,

[1] Примечания Секретариата: имеются в виду документы, указанные под различными подзаголовками: Конвенции Африканского союза о кибербезопасности и защите персональных данных, Конвенция Совета Европы о киберпреступности, Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Организации Объединенных Наций против коррупции.

необходимых для выявления, расследования и уголовного преследования в отношении преступлений, которые совершаются без использования компьютерной системы, если это отвечает установленным условиям и критериям для применения этих процессуальных полномочий.

Аналогичным образом, правовая основа для международного сотрудничества, предусмотренная в настоящей Конвенции, должна применяться не только в отношении уголовных преступлений, признанных таковыми в Конвенции, но и, в необходимых случаях, в отношении других уголовных преступлений, совершенных с использованием компьютера, а также при сборе электронных доказательств, необходимых для выявления, расследования и уголовного преследования в отношении обычного уголовного преступления.

Поэтому цель главы о криминализации состоит не в ограничении сферы применения других глав Конвенции, а в установлении общего стандарта для относительно нового вида преступности — киберпреступности — для всех государств.

Процессуальные меры по борьбе с киберпреступностью

Процессуальное право является важнейшим элементом расследования и уголовного преследования в отношении киберпреступлений. Конвенция должна установить четкую правовую основу для процессуальных мер, с тем чтобы правоохранительные органы могли получить доказательства, необходимые для противодействия киберпреступности, соблюдая при этом твердые гарантии и ограничения, которые подкрепляют принцип верховенства права, а также меры по защите прав человека и основных свобод. Статьи Конвенции, посвященные процессуальным мерам, должны также соответствовать существующим правовым нормам и не допускать фрагментации действующих международных механизмов.

Процессуальные меры должны применяться в отношении уголовных преступлений, предусмотренных в материально-правовых положениях Конвенции, и, отвечая требованиям внутреннего права государств, в отношении других уголовных преступлений, совершенных с использованием компьютерных систем или цифровых технологий, а также при сборе электронных доказательств, необходимых для выявления, расследования и уголовного преследования в отношении обычных преступлений, если это соответствует установленным условиям и критериям для использования таких процессуальных мер.

Австралия предлагает включить в новую Конвенцию следующие процессуальные меры:

- постановления об обеспечении сохранности электронных данных (включая хранящиеся данные о содержании сообщений, информацию об абонентах и данные о трафике);
- постановления о предоставлении электронных данных;
- обыск и выемка электронных данных;
- сбор электронных данных в режиме реального времени (включая данные о трафике и онлайн-перехват данных о содержании сообщений);
- постановления о срочном и оперативном обеспечении сохранности и предоставлении данных.

Процессуальные меры должны учитывать характер электронных данных, чтобы быстро и оперативно обеспечивать их сохранность, а правоохранительные и другие соответствующие органы должны иметь возможность оперативно и эффективно получить эти данные таким образом, чтобы преступные методы и практики в киберпространстве не мешали усилиям этих органов по сбору данных.

Условия, требования и гарантии при применении процессуальных мер

Процессуальные меры для выявления, расследования и уголовного преследования в отношении киберпреступлений могут быть связаны с обязательствами по защите прав человека и свобод, закрепленных в соответствующих международных документах по правам человека, включая Международный пакт о гражданских и политических правах. К таким правам относятся:

Право на справедливое судебное разбирательство (Международный пакт о гражданских и политических правах, статья 14)

Статья 14 Международного пакта о гражданских и политических правах закрепляет право на справедливое судебное разбирательство, включая процессуальные гарантии, принцип верховенства права и презумпцию невиновности. Комитет по правам человека заявил, что «статья 14 Пакта направлена на обеспечение надлежащего отправления правосудия и с этой целью гарантирует ряд конкретных прав».

Право, предусмотренное в статье 14, не является абсолютным; оно может подвергаться допустимым ограничениям, при условии что эти ограничения установлены законом и являются обоснованными, необходимыми и соразмерными для достижения законной цели.

Право не подвергаться вмешательству в личную жизнь (Международный пакт о гражданских и политических правах, статья 17)

Статья 17 Пакта закрепляет право не подвергаться вмешательству в личную жизнь и предусматривает, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции».

Суть этого права более подробно изложена в замечании общего порядка № 16 Комитета по правам человека. В нем указано, что «это право должно быть подкреплено гарантиями от любого такого вмешательства и таких посягательств, независимо от того, совершаются ли они государственными органами, физическими или юридическими лицами». В пункте 3 замечания общего порядка № 16 отмечается, что «термин "незаконное" означает, что вмешательство вообще не может иметь места, за исключением случаев, предусмотренных законом. Вмешательство, разрешаемое государствами, может совершаться только на основании закона, который должен в свою очередь соответствовать положениям, целям и задачам Пакта».

Право на свободное выражение своего мнения (Международный пакт о гражданских и политических правах, пункт 2 статьи 19)

В статье 19 Пакта закреплено право на свободное выражение мнений. В пункте 2 статьи 19 признается право искать, получать и распространять всякого рода информацию и идеи с использованием любых способов, в том числе письменных или устных сообщений, средств массовой информации, вещания и коммерческой рекламы.

Право на свободное выражение мнений не является абсолютным. Согласно пункту 3 статьи 19 свободное выражение мнений может быть ограничено в соответствии с законом и в случаях, когда это необходимо для защиты прав или репутации других лиц или охраны национальной безопасности, общественного порядка и здоровья или нравственности населения. Ограничения должны быть предусмотрены законодательством, необходимы для достижения желаемой цели и соразмерны необходимости, на основании которой устанавливаются ограничения.

Цель Конвенции и предусмотренных в ней процессуальных мер состоит в снижении уровня угрозы, воздействия и ущерба от киберпреступности, что

может стать допустимым основанием для ограничения прав человека и свобод, если эти меры являются законными, разумными, необходимыми и соразмерными.

Крайне необходимо, чтобы процессуальные меры, изложенные в Конвенции, устанавливались, осуществлялись и применялись при соблюдении условий и гарантий, которые предусмотрены в Конвенции и других применимых документах по правам человека.

Такие условия и гарантии должны включать, сообразно каждой процессуальной мере:

- судебный или иной независимый контроль или надзор;
- основания, оправдывающие применение той или иной процессуальной меры;
- ограничения в отношении сферы действия и сроков применения процессуальной меры;
- учет воздействия процессуальных мер на права, обязанности и законные интересы третьих лиц.

Бразилия

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

Глава III
Процессуальные меры и правоприменение

Статья 18
Сфера применения процессуальных норм[2]

1. Каждая Сторона принимает такие законодательные и иные меры, какие необходимы для установления полномочий и процедур, предусмотренных положениями настоящей главы, в целях предупреждения, выявления, пресечения и расследования киберпреступлений и уголовного преследования и наказания за их совершение.

2. За исключением случаев, когда предусмотрено иное, каждая Сторона применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии с главой II Конвенции;

b) других уголовных преступлений, совершенных с помощью информационно-коммуникационных технологий;

c) сбора доказательств в электронной форме, касающихся совершения уголовных преступлений.

Статья 19
Условия и гарантии[3]

1. Каждая Сторона обеспечивает, чтобы полномочия и процедуры, изложенные в настоящей главе, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными в нормах ее внутреннего права, которые обеспечивают надлежащую защиту прав человека и свобод, включая права, вытекающие из ее обязательств по Международному пакту о

[2] *Источник:* предложение Китая и Российской Федерации, с изменениями, внесенными Бразилией.
[3] *Источники:* Будапештская конвенция и предложение Китая и Российской Федерации.

гражданских и политических правах и по другим применимым международным документам правам человека, и которые устанавливают принцип соразмерности.

2. Такие условия и гарантии с учетом характера соответствующей процедуры и полномочия включают, в частности, судебный или иной независимый надзор, основания для применения и ограничение сферы и сроков действия такого полномочия или процедуры.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждая Сторона рассматривает вопрос о воздействии предусмотренных в настоящей главе полномочий и процедур на права, обязанности и законные интересы третьих лиц.

Статья 20
Оперативное обеспечение сохранности хранящихся компьютерных данных[4]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы ее компетентные органы имели возможность посредством дачи распоряжений или иным образом добиться оперативного обеспечения сохранности конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Сторона реализует положения пункта 1 выше посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которое отвечает за обеспечение их сохранности, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутренним законодательством.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19.

Статья 21
Оперативное обеспечение сохранности накопленной информации в электронной форме[5]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы ее компетентные органы имели возможность давать соответствующие распоряжения или указания или аналогичным образом оперативно обеспечивать сохранность конкретной информации в электронной форме, включая данные о трафике, в частности когда имеются основания полагать, что эти данные подвержены особому риску уничтожения, копирования или изменения, в том числе по причине истечения срока их хранения, установленного внутренним законодательством этой Стороны или правилами предоставления услуг провайдера.

2. Если Сторона реализует положения пункта 1 настоящей статьи посредством дачи распоряжения каким-либо лицам (в том числе юридическим) об обеспечении сохранности конкретной хранящейся информации, которая

[4] *Источник:* Будапештская конвенция.
[5] *Источник:* предложение Китая и Российской Федерации.

находится во владении или под контролем этих лиц, то эта Сторона принимает такие законодательные и иные правовые меры, какие могут потребоваться для того, чтобы обязать данное лицо хранить эту информацию и обеспечивать ее целостность в течение необходимого периода времени, но не более срока, установленного внутренним законодательством этой Стороны, 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 потребоваться для того, чтобы обязать лицо, которому поручено обеспечивать сохранность информации, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутренним законодательством.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19 настоящей Конвенции.

Статья 22
Оперативное обеспечение сохранности и частичное раскрытие данных о трафике[6]

Каждая Сторона принимает в отношении данных о трафике, сохранность которых должна быть обеспечена, такие законодательные и иные меры, какие могут потребоваться для того, чтобы:

a) гарантировать оперативное обеспечение сохранности данных о трафике независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения; и

b) гарантировать оперативное раскрытие компетентному органу этой Стороны или лицу, назначенному этим органом, достаточного объема данных о трафике, которые позволят Стороне идентифицировать поставщиков услуг и путь, по которому передавалось сообщение.

Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19.

Статья 23
Распоряжение о предоставлении информации[7]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочия на дачу распоряжения:

a) лицу на ее территории о предоставлении определенных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на компьютерном носителе данных; и

b) поставщику услуг, предлагающему свои услуги на территории этой Стороны, о предоставлении сведений о его абонентах, которые находятся во владении или под контролем этого поставщика услуг.

2. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19.

---

[6] *Источники:* Будапештская конвенция и предложение Китая и Российской Федерации.

[7] *Источники:* Будапештская конвенция и предложение Китая и Российской Федерации, с изменениями, внесенными Бразилией.

Статья 24
Обыск и выемка информации, хранящейся или обрабатываемой в электронной форме[8]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на получение доступа к находящимся на территории этой Стороны или под ее юрисдикцией:

a) устройствам информационно-коммуникационных технологий и хранящейся в них информации; и

b) носителям информации, на которых может храниться искомая электронная информация.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда ее компетентные органы, проводящие обыск в соответствии с положениями пункта 1 (a) настоящей статьи, имеют основания полагать, что искомая информация хранится на другом устройстве информационно-коммуникационных технологий на территории этой Стороны, такие органы имели возможность оперативно провести обыск в целях получения доступа к этому другому устройству информационно-коммуникационных технологий или содержащимся в нем данным.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на выемку электронной информации на ее территории или под ее юрисдикцией или на аналогичную защиту такой информации. Эти меры включают, в частности, предоставление следующих полномочий:

a) производить выемку устройств информационно-коммуникационных технологий, используемых для хранения информации, либо иным образом обеспечивать их защиту;

b) делать и сохранять копии такой информации в электронно-цифровой форме;

c) обеспечивать целостность соответствующей хранящейся информации;

d) изымать информацию, хранящуюся или обрабатываемую в электронной форме.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на дачу распоряжения в порядке, установленном ее внутренним законодательством, любому лицу, обладающему специальными знаниями в области функционирования соответствующей информационной системы, информационно-телекоммуникационной сети или их частей или применяемых мер защиты хранящейся в них информации, для предоставления необходимых сведений и/или оказания содействия в осуществлении мер, предусмотренных пунктами 1–3 настоящей статьи.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19 настоящей Конвенции.

---

[8] *Источник:* предложение Китая и Российской Федерации. Положение, аналогичное статье 19 Будапештской конвенции, с изменениями, внесенными Китаем и Российской Федерацией.

Статья 25
Сбор в режиме реального времени данных о трафике[9]

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

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

b) обязывать 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 трафике в связи с конкретными сообщениями на территории этой Стороны, передаваемыми посредством компьютерной системы.

2. Если Сторона в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то она может принять такие законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике в связи с конкретными сообщениями, передаваемыми на ее территории, путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19.

Статья 26
Перехват данных о содержании[10]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных преступлений, подлежащих квалификации в ее внутреннем законодательстве, с тем чтобы предоставить своим компетентным органам следующие полномочия:

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

b) обязывать 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 содержании конкретных сообщений на территории этой Стороны, передаваемых посредством компьютерной системы.

2. Если Сторона в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то она может принять такие законодательные и иные меры, какие могут потребоваться для

[9] *Источник:* Будапештская конвенция.
[10] *Источник:* Будапештская конвенция.

обеспечения сбора или записи в режиме реального времени данных о содержании конкретных сообщений на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 18 и 19.

Статья 27
Юрисдикция[11]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления юрисдикции в отношении любого преступления, предусмотренного в соответствии с положениями статей 2–11 настоящей Конвенции, когда такое преступление совершено:

a) на ее территории; или

b) на борту судна под флагом этой Стороны; или

c) на борту воздушного судна, зарегистрированного в соответствии с законодательством этой Стороны; или

одним из ее граждан, если это преступление является уголовно наказуемым в месте его совершения или если это преступление совершено за пределами территориальной юрисдикции любого государства.

2. Каждая Сторона может сохранить за собой право не применять или применять только в конкретных случаях или условиях нормы относительно юрисдикции, изложенные в пункте 1 (b)–(d) настоящей статьи или в любой его части.

3. Каждая Сторона принимает такие меры, какие могут потребоваться для установления юрисдикции в отношении дел, в которых предполагаемый правонарушитель находится на ее территории и которого по получении просьбы о выдаче она не выдает другой Стороне исключительно на основании его гражданства.

4. Настоящая Конвенция не исключает осуществления какой-либо Стороной уголовной юрисдикции в соответствии с ее внутренним законодательством.

5. Если Сторона, осуществляющая свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любые другие Стороны осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием, компетентные органы этих Сторон проводят, в надлежащих случаях, консультации друг с другом в целях координации своих действий[12].

---

[11] *Источник:* Будапештская конвенция, с изменениями, внесенными Бразилией.

[12] *Источник:* предложение Китая и Российской Федерации.

Канада

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

Процессуальные полномочия

Сфера действия процессуальных полномочий

1. Уточнить, что полномочия и процедуры, предусмотренные в настоящей статье, предназначены для целей конкретных уголовных расследований или судебных разбирательств.

2. За исключением случаев, когда специально предусмотрено иное, каждое Государство-участник применяет полномочия и процедуры, указанные в пункте 1, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

b) других уголовных преступлений, совершенных с помощью компьютерной системы; и

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

Оперативное обеспечение сохранности хранящихся компьютерных данных

1. Каждое Государство-участник принимает законодательные и иные меры, необходимые для того, чтобы его компетентные органы имели возможность давать распоряжения об оперативном обеспечении или иным образом добиваться оперативного обеспечения сохранности конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Государство-участник реализует положения пункта 1 посредством дачи распоряжения лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то Государство-участник принимает законодательные и иные меры, необходимые для того, чтобы обязать это лицо обеспечить сохранность и целостность таких данных в течение необходимого срока, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться их раскрытия. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает законодательные и иные меры, необходимые для того, чтобы обязать, если это обосновано и разрешено, хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность проведения таких процедур в течение срока, предусмотренного в его внутреннем законодательстве.

Оперативное обеспечение сохранности и частичное раскрытие данных о трафике

В отношении данных о трафике, подлежащих сохранению в соответствии с предыдущей статьей:

a) гарантировать оперативное обеспечение сохранности данных о трафике независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения; и

b) гарантировать оперативное раскрытие компетентному органу Государства-участника или лицу, назначенному этим органом, достаточного объема

данных о трафике, которые позволят Государству-участнику идентифицировать поставщиков услуг и путь, по которому передавалось сообщение.

Распоряжение о предоставлении информации

Каждое Государство-участник принимает необходимые меры для наделения своих внутренних компетентных органов полномочием на дачу распоряжения лицу на его территории относительно предоставления конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на носителе компьютерных данных.

Обыск и выемка хранящихся компьютерных данных

1. Каждое Государство-участник принимает необходимые меры для наделения своих внутренних компетентных органов полномочиями на проведение обыска или получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) к носителю компьютерных данных, на котором могут храниться компьютерные данные на его территории.

2. Каждое Государство-участник принимает необходимые меры для того, чтобы его внутренние компетентные органы могли оперативно распространить обыск или аналогичный доступ на другую систему, если они имеют основания полагать, что искомые данные хранятся в такой другой компьютерной системе или ее части на его территории и что такие данные в законном порядке могут быть получены из первой системы или с ее помощью.

3. Каждое Государство-участник принимает необходимые меры для предоставления своим внутренним компетентным органам полномочия на выемку или аналогичную защиту компьютерных данных, к которым получен доступ в соответствии с пунктом 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных; и

d) обеспечение недоступности этих компьютерных данных в компьютерной системе, к которой получен доступ, или их извлечение из нее.

4. Каждое Государство-участник принимает необходимые меры для предоставления своим внутренним компетентным органам полномочий на дачу распоряжения любому лицу, которое обладает знаниями о функционировании компьютерной системы или мерах, применяемых для защиты компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации для обеспечения возможности принятия мер, указанных в пунктах 1 и 2.

Юрисдикция

1. Каждое Государство-участник принимает необходимые меры для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда:

a) преступление совершено на территории этого Государства-участника;

b) преступление совершено на борту судна под флагом этого Государства-участника или воздушного судна, которое зарегистрировано в соответствии

с законодательством этого Государства-участника, на момент совершения преступления; или

c) преступление совершено гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории.

2. Позволить Государству-участнику 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 это лицо лишь на том основании, что оно является одним из граждан этого Государства-участника.

3. Позволить Государству-участнику 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 это лицо.

4. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любое другое Государство-участник осуществляет расследование, уголовное преследование или судебное разбирательство в отношении того же деяния, компетентные органы этих Государств-участников проводят, в надлежащих случаях, консультации друг с другом в целях координации своих действий.

5. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной и административной юрисдикции, установленной Государством-участником в соответствии с его внутренним законодательством.

Колумбия

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

Процессуальные меры и правоприменение

Принимая во внимание положения о полномочиях и процедурах, которыми Колумбия связана по Конвенции Организации Объединенных Наций против транснациональной организованной преступности, Конвенции Организации Объединенных Наций против коррупции и Будапештской конвенции о киберпреступности, в отношении процессуальных мер и правоприменения предлагается следующее:

Меры	*Положение действующего международно-правового документа*
Полномочия и процедуры	Статья 14 Будапештской конвенции
Условия и гарантии	Статья 15 Будапештской конвенции
Оперативное обеспечение сохранности хранящихся компьютерных данных	Статья 16 Будапештской конвенции
Оперативное обеспечение сохранности и частичное раскрытие данных о трафике	Статья 17 Будапештской конвенции
Распоряжение о предоставлении информации	Статья 18 Будапештской конвенции
Обыск и выемка хранящихся компьютерных данных	Статья 19 Будапештской конвенции
Сбор в режиме реального времени данных о трафике	Статья 20 Будапештской конвенции
Перехват данных о содержании	Статья 21 Будапештской конвенции

Меры	*Положение действующего международно-правового документа*
Юрисдикция	Статья 22 Будапештской конвенции, статья 15 Конвенции об организованной преступности и статья 42 Конвенции против коррупции
Приостановление операций (замораживание), арест и конфискация	Статья 31 Конвенции против коррупции

Египет

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

Глава III
Уголовное производство и правоприменение

Предлагается включить в эту главу следующие три основные статьи.

Статья 31
Сфера действия процессуальных положений

1. Каждое Государство-участник принимает такие законодательные меры, какие необходимы для установления полномочий и процедур в целях предупреждения, выявления, раскрытия и расследования преступлений и иных противоправных деяний и осуществления судебного разбирательства в связи с ними.

2. Каждое Государство-участник применяет вышеуказанные полномочия и процедуры в отношении:

a) уголовных преступлений и иных противоправных деяний, предусмотренных в настоящей Конвенции;

b) других уголовных преступлений и иных противоправных деяний, совершенных с помощью информационно-коммуникационных технологий;

c) сбора электронных доказательств.

Статья 32
Уголовно-процессуальные действия

Уголовно-процессуальные действия включают следующее:

1. Оперативное обеспечение сохранности данных, хранящихся в информационно-коммуникационных устройствах, включая данные отслеживания пользователей, которые хранятся в устройствах информационных технологий, особенно при наличии оснований предполагать, что такая информация может быть утрачена или изменена, посредством дачи распоряжения, обязывающего соответствующее лицо обеспечить целостность таких данных, которые находятся в его владении или под его контролем, с тем чтобы компетентные органы могли провести обыск и расследование, при соблюдении конфиденциальности в отношении любых действий, предпринятых в связи с этим.

2. Оперативное обеспечение сохранности и частичное раскрытие информации, полученной в результате отслеживания пользователей, независимо от того, сколько поставщиков услуг участвовали в передаче такой информации, и гарантия оперативного раскрытия компетентными органами достаточного объема данных о трафике, который позволит Государству-участнику выявить поставщиков услуг и путь передачи сообщения.

3. Дача распоряжений о предоставлении информации, находящейся во владении какого-либо лица на территории Государства-участника и хранящейся в

информационной системе или на носителе информации либо находящейся во владении или под контролем поставщика услуг, предоставляющего услуги на территории Государства-участника.

4. Проверка информации или доступ к информации, хранящейся в информационной системе или на носителе информации, или доступ к такой информации.

5. Выемка, копирование и сохранение хранящейся информации в целях проведения процедур поиска информации и получения доступа к ней.

6. Сбор в режиме реального времени информации об отслеживании пользователей и дача распоряжения, обязывающего поставщиков услуг в пределах юрисдикции Государства-участника собирать и записывать такую информацию и обеспечивать ее конфиденциальность.

7. Перехват информации о содержании, позволяющий компетентным органам с помощью технических средств собирать и записывать в режиме реального времени информацию, передаваемую посредством информационно-коммуникационных технологий.

8. Каждое Государство-участник принимает необходимые законодательные и иные меры, позволяющие его компетентным органам останавливать передачу и трансляцию любого контента, который способствует совершению преступлений, признанных таковыми в настоящей Конвенции.

Статья 33
Допустимые цифровые доказательства

Цифровые доказательства, полученные или извлеченные из устройств, оборудования, электронных носителей информации, информационных систем, компьютерных программ или любых информационно-коммуникационных систем, имеют доказательную ценность вещественных судебных доказательств в уголовных делах при условии, что такие цифровые доказательства отвечают техническим требованиям, установленным в законодательстве Государств-участников.

Сальвадор

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

Процессуальные меры и правоприменение

Сфера действия процессуальных мер

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящей статьи, в целях проведения конкретного уголовного расследования или судебного разбирательства.

Если не предусмотрено иное, каждое Государство-участник применяет полномочия и процедуры, указанные в предыдущем пункте настоящей статьи, в отношении:

a) преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции;

b) других уголовных преступлений, совершенных с помощью компьютерной системы;

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

Условия и гарантии

Каждое Государство-участник обеспечивает, чтобы полномочия и процедуры, предусмотренные в настоящем разделе, устанавливались, осуществлялись и применялись при соблюдении условий и гарантий, предусмотренных в его внутреннем законодательстве, которое обеспечивает надлежащую защиту прав и свобод человека.

Такие условия и гарантии, необходимые с учетом характера соответствующей процедуры или полномочия, включают, в частности, судебный или иной независимый надзор, основания для применения и ограничение сферы и сроков действия такого полномочия или процедуры.

В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждое Государство-участник рассматривает вопрос о воздействии полномочий и процедур, предусмотренных в настоящей статье, на права, обязанности и законные интересы третьих лиц.

Полномочия на запрос информации о преступлениях

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться для наделения его компетентных органов полномочиями давать распоряжение или иным образом обязать физическое или юридическое лицо на его территории относительно предоставления конкретных компьютерных данных, находящихся во владении или под контролем этого лица и хранящихся в компьютерной системе или на компьютерном носителе информации.

Обеспечение сохранности данных, хранящихся в компьютерных системах

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы его компетентные органы могли посредством распоряжений или аналогичным образом добиваться оперативного обеспечения сохранности конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

Если Государство-участник реализует положения предыдущего пункта посредством дачи распоряжения лицу относительно обеспечения сохранности конкретных компьютерных данных, находящихся во владении или под контролем этого лица, это Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо обеспечить сохранность и целостность таких компьютерных данных в течение необходимого срока, но не более 90 дней, с тем чтобы компетентные органы могли добиться их раскрытия. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

Обыск и выемка данных, хранящихся в компьютерной системе

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на проведение обыска или получение аналогичного доступа в отношении:

a) компьютерной системы или ее части и хранящихся в ней компьютерных данных; и

b) носителя компьютерных данных, на котором могут храниться компьютерные данные на его территории.

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда его органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на его территории, и такие данные в законном порядке доступны из первой системы или с ее помощью, эти органы могли оперативно распространить обыск или аналогичный доступ на такую другую систему.

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на выемку или аналогичную защиту компьютерных данных, доступ к которым получен в соответствии с предыдущими пунктами. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных;

d) обеспечение недоступности этих компьютерных данных в компьютерной системе или их извлечение из нее.

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочия на дачу распоряжения любому лицу, которое обладает знаниями о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации, с тем чтобы обеспечить принятие мер, указанных в предыдущих пунктах.

Сбор в режиме реального времени данных о трафике

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

b) обязывать поставщика услуг, чтобы он в рамках имеющихся у него технических возможностей собирал и записывал с помощью применения технических средств на территории данного Государства-участника или сотрудничал с компетентными органами и помогал им собирать и записывать данные о трафике в режиме реального времени, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью компьютерной системы.

Если Государство-участник в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то оно может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике, связанных с конкретными сообщениями на его территории, путем применения технических средств на этой территории.

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

Перехват данных о содержании

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных преступлений, подлежащих квалификации в соответствии с нормами его внутреннего законодательства, для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

b) обязывать поставщика услуг, чтобы он в рамках имеющихся у него технических возможностей собирал и записывал с помощью применения технических средств на территории этого Государства-участника или сотрудничал с компетентными органами и помогал им собирать и записывать данные о содержании в режиме реального времени, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью компьютерной системы.

Если Государство-участник в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то оно может принять такие законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике, связанных с указанными сообщениями на его территории, путем применения технических средств на этой территории.

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

Конфискация и арест

Государства-участники принимают, в максимально возможной степени в рамках своих внутренних правовых систем, такие меры, какие могут потребоваться для обеспечения конфискации:

a) доходов от преступлений, охватываемых настоящей Конвенцией, или имущества, стоимость которого соответствует стоимости таких доходов;

b) имущества, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении преступлений, охватываемых настоящей Конвенцией.

Государства-участники принимают такие меры, какие могут потребоваться для обеспечения выявления, отслеживания, замораживания или ареста любого из перечисленного в предыдущем пункте, с целью последующей конфискации.

Если доходы от преступлений были превращены или преобразованы, полностью или частично, в другое имущество, то меры, указанные в настоящей статье, применяются в отношении такого имущества.

Если доходы от преступлений были приобщены к имуществу, приобретенному из законных источников, то конфискации, без ущерба для любых полномочий, касающихся замораживания или ареста, подлежит та часть имущества, которая соответствует оцененной стоимости приобщенных доходов.

К прибыли или другим выгодам, которые получены от доходов от преступлений, от имущества, в которое были превращены или преобразованы доходы от преступлений, или от имущества, к которому были приобщены доходы от преступлений, также применяются меры, указанные в настоящей статье, таким же образом и в той же степени, как и в отношении доходов от преступлений.

Каждое Государство-участник уполномочивает свои суды или другие компетентные органы издавать постановления о представлении или аресте банковских, финансовых или коммерческих документов. Государства-участники не

уклоняются от принятия мер в соответствии с положениями настоящего пункта, ссылаясь на необходимость сохранения банковской тайны.

Государства-участники могут рассмотреть возможность установления требования о том, чтобы лицо, совершившее преступление, доказало законное происхождение предполагаемых доходов от преступления или другого имущества, подлежащего конфискации, в той мере, в какой такое требование соответствует основополагающим принципам их внутреннего законодательства и характеру судебного и иного разбирательства.

Положения настоящей статьи не толкуются как наносящие ущерб правам добросовестных третьих сторон.

Ничто, содержащееся в настоящей статье, не затрагивает принципа, согласно которому меры, о которых в ней говорится, определяются и осуществляются в соответствии с положениями внутреннего законодательства Государства-участника и при условии их соблюдения.

Распоряжение конфискованными доходами от преступлений или имуществом

Доходами от преступлений или имуществом, конфискованными Государством-участником на основании настоящей Конвенции, распоряжается это Государство-участник в соответствии со своим внутренним законодательством и административными процедурами.

Действуя по просьбе, направленной другим Государством-участником в соответствии с настоящей Конвенцией, Государства-участники в той мере, в какой это допускается внутренним законодательством, и, в случае получения соответствующей просьбы, в первоочередном порядке рассматривают вопрос о возвращении конфискованных доходов от преступлений или имущества запрашивающему Государству-участнику, с тем чтобы оно могло предоставить компенсацию потерпевшим от преступления или возвратить такие доходы от преступлений или имущество их законным собственникам.

Действуя по просьбе, направленной другим Государством-участником в соответствии с положениями настоящей Конвенции, Государство-участник может особо рассмотреть возможность заключения соглашений или договоренностей:

a) о перечислении суммы, соответствующей стоимости доходов от преступлений или имущества, или средств, полученных в результате реализации таких доходов или имущества или их части, на счет, предназначенный для этой цели в соответствии с положениями настоящей Конвенции, или по указанию межправительственных органов, специализирующихся на борьбе против организованной преступности;

b) передаче другим Государствам-участникам на регулярной или разовой основе части доходов от преступлений, или имущества, или средств, полученных в результате реализации таких доходов или имущества, в соответствии со своим внутренним законодательством или административными процедурами.

Сведения о судимости

Каждое Государство-участник может принимать такие законодательные или другие меры, какие могут потребоваться для учета, на таких условиях и в таких целях, какие оно сочтет надлежащими, любого ранее вынесенного в другом государстве обвинительного приговора в отношении лица, подозреваемого в совершении расследуемого преступления, для использования такой информации в ходе уголовного производства в связи с преступлением, признанным таковым в соответствии с настоящей Конвенцией.

Защита свидетелей

Каждое Государство-участник принимает, в пределах своих возможностей, надлежащие меры, направленные на обеспечение эффективной защиты от

вероятной мести или запугивания в отношении участвующих в уголовном производстве свидетелей, которые дают показания в связи с преступлениями, охватываемыми настоящей Конвенцией, и, в надлежащих случаях, в отношении их родственников и других близких им лиц.

Меры, предусмотренные в предыдущем пункте настоящей статьи, без ущерба для прав подсудимого, в том числе для права на надлежащее судебное разбирательство, могут, в частности, включать:

a) установление процедур для физической защиты таких лиц, например в той мере, в какой это необходимо и практически осуществимо, для их переселения в другое место, а также принятие таких положений, какие разрешают, в надлежащих случаях, не разглашать информацию, касающуюся личности и местонахождения таких лиц, или устанавливают ограничения на такое разглашение информации;

b) принятие правил доказывания, позволяющих давать свидетельские показания таким образом, который обеспечивает безопасность таких лиц, например разрешение давать показания с помощью средств связи, таких как видеосвязь или другие надлежащие средства;

c) Государства-участники рассматривают возможность заключения с другими государствами соглашений или договоренностей относительно переселения лиц, указанных в первом пункте настоящей статьи;

d) положения настоящей статьи применяются также в отношении потерпевших в той мере, в какой они являются свидетелями.

Помощь потерпевшим и их защита

Каждое Государство-участник принимает, в пределах своих возможностей, надлежащие меры для предоставления помощи и защиты потерпевшим от преступлений, охватываемых настоящей Конвенцией, особенно в случаях угрозы местью или запугивания.

Каждое Государство-участник устанавливает надлежащие процедуры для обеспечения доступа к компенсации и возмещению ущерба потерпевшим от преступлений, охватываемых настоящей Конвенцией.

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.

Меры, направленные на расширение сотрудничества с правоохранительными органами

Каждое Государство-участник принимает надлежащие меры для того, чтобы поощрять лиц, которые участвуют или участвовали в организованных преступных группах:

a) к предоставлению информации, полезной для компетентных органов, в целях расследования и доказывания в связи с такими вопросами, как:

i) идентификационные данные, характер, членский состав, структура, местонахождение или деятельность организованных преступных групп;

ii) связи, в том числе международные связи, с другими организованными преступными группами;

iii) преступления, которые совершили или могут совершить организованные преступные группы;

b) предоставлению фактической, конкретной помощи компетентным органам, которая может способствовать лишению организованных преступных групп их ресурсов или доходов от преступлений.

Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть возможность смягчения, в надлежащих случаях, наказания обвиняемого лица, которое существенным образом сотрудничает в расследовании или уголовном преследовании в связи с каким-либо преступлением, охватываемым настоящей Конвенцией.

Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть, в соответствии с основополагающими принципами своего внутреннего законодательства, возможность предоставления иммунитета от уголовного преследования лицу, которое существенным образом сотрудничает в расследовании или уголовном преследовании в связи с преступлением, охватываемым настоящей Конвенцией.

Защита таких лиц осуществляется в порядке, предусмотренном в соответствующей статье настоящей Конвенции.

В случае когда лицо, которое упоминается в первом пункте настоящей статьи и находится в одном Государстве-участнике, может существенным образом сотрудничать с компетентными органами другого Государства-участника, заинтересованные Государства-участники могут рассмотреть возможность заключения соглашений или договоренностей, в соответствии со своим внутренним законодательством, относительно возможного предоставления другим Государством-участником режима, указанного во втором и третьем пунктах настоящей статьи.

Европейский союз и его государства-члены

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

Глава III
Уголовное производство и правоприменение

Статья 13
Сфера действия процессуальных мер

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящей главы, в целях проведения конкретных уголовных расследований или судебных разбирательств.

2. Каждое Государство-участник применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии со статьями 5–10 настоящей Конвенции; и

b) сбора доказательств в электронной форме, подтверждающих совершение уголовного преступления, которое признано таковым в соответствии со статьями 5–10 настоящей Конвенции.

Статья 14
Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы полномочия и процедуры, указанные в настоящей главе, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными положениями его внутреннего законодательства, которые обеспечивают надлежащую и полную защиту прав человека и основных свобод в соответствии с

международным нормами по правам человека, включая права, вытекающие из обязательств, принятых этим Государством-участником в соответствии со Всеобщей декларацией прав человека, Международным пактом о гражданских и политических правах, Конвенцией против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания, Конвенцией о правах ребенка, Факультативным протоколом к Конвенции о правах ребенка, касающимся торговли детьми, детской проституции и детской порнографии, а также другими документами по правам человека, и в которых закреплены принципы соразмерности, законности и необходимости и требование о защите неприкосновенности частной жизни и персональных данных.

2. Такие условия и гарантии с учетом характера соответствующего полномочия или процедуры включают, в частности, судебный или иной независимый надзор, основания для применения и ограничения сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждое Государство-участник рассматривает вопрос о воздействии предусмотренных настоящей главой полномочий и процедур на права, обязанности и законные интересы третьих лиц.

Статья 15
Оперативное обеспечение сохранности хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться для того, чтобы его компетентные органы могли посредством распоряжений или схожим образом оперативно обеспечивать сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности в случаях, когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Государство-участник реализует положения пункта 1 выше посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, установленного его внутренним законодательством.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Статья 16
Распоряжение о предоставлении информации

1. Каждое Государство-участник принимает меры, которые могут быть необходимы для того, чтобы предоставить своим компетентным органам полномочия отдавать распоряжения:

a) лицу на территории этого Государства-участника о предоставлении конкретных находящихся во владении или под контролем этого лица компьютерных данных, которые хранятся в компьютерной системе или на компьютерном носителе данных; и

b) поставщику услуг, предлагающему свои услуги на территории этого Государства-участника, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Статья 17
Обыск и выемка хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться для предоставления его компетентным органам полномочий на проведение обыска и получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на его территории.

2. Каждое Государство-участник принимает меры, которые могут потребоваться для обеспечения того, чтобы, в случае когда его органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на его территории, и такие данные в законном порядке могут быть получены из первой системы или с ее помощью, компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на эту другую систему.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на выемку или аналогичную защиту компьютерных данных, полученных в соответствии с пунктом 1 или 2. Эти меры должны включать предоставление полномочий:

a) производить выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) изготавливать и сохранять копии этих компьютерных данных;

c) обеспечивать целостность относящихся к делу хранимых компьютерных данных;

d) обеспечивать недоступность этих компьютерных данных, находящихся в компьютерной системе, или извлекать их из нее.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий привлекать любое лицо, обладающее знаниями о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, для предоставления, в разумных пределах, необходимых сведений, с тем чтобы обеспечить принятие мер, указанных в пунктах 1 и 2.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Статья 18
Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться для установления юрисдикции в отношении любого преступления, признанного таковым в соответствии с положениями статей 5–10 настоящей Конвенции, когда такое преступление совершено:

a) на территории этого Государства-участника;

b) на борту судна под флагом этого Государства-участника или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника, на момент совершения преступления; или

c) одним из его граждан, если это преступление признается наказуемым в соответствии с уголовным законодательством места его совершения или если это преступление совершено за пределами территориальной юрисдикции какого-либо государства.

2. Каждое Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, если преступление совершено:

a) против гражданина этого Государства-участника;

b) гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории.

3. Каждое Государство-участник может также принять такие меры, какие могут потребоваться для установления его юрисдикции в отношении преступлений, охватываемых настоящей Конвенцией, если предполагаемый правонарушитель присутствует на его территории и по получении просьбы о выдаче это Государство-участник не выдает этого правонарушителя исключительно на основании его гражданства.

4. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любое другое Государство-участник осуществляет расследование, уголовное преследование или судебное разбирательство в отношении того же деяния, компетентные органы этих Государств-участников проводят, в надлежащих случаях, консультации друг с другом в целях координации своих действий.

5. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной юрисдикции, установленной Государством-участником в соответствии с его внутренним законодательством.

Статья 19
Помощь потерпевшим и их защита

1. Каждое Государство-участник принимает, в пределах своих возможностей, надлежащие меры для предоставления помощи и защиты потерпевшим от преступлений, признанных таковыми в соответствии со статьями 5–10 настоящей Конвенции.

2. Каждое Государство-участник устанавливает надлежащие процедуры для обеспечения доступа к компенсации и возмещению ущерба потерпевшим от преступлений, признанных таковыми в соответствии со статьями 5–10 настоящей Конвенции.

3. 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.

Гана

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

Глава III
Процессуальные меры и правоприменение[13]

Статья 23
Сфера действия процессуальных положений

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящей статьи, в целях проведения конкретного уголовного расследования или судебного разбирательства.

2. Если специально не оговорено иное, каждая Сторона применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии со статьями 5–20 настоящей Конвенции;

b) других уголовных преступлений, совершенных с помощью компьютерной системы; и

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

3. Каждая Сторона может сделать оговорку о сохранении за собой права применять меры, предусмотренные статьей 29 настоящей Конвенции, только в отношении преступлений или категорий преступлений, указанных в этой оговорке, при условии, что круг таких преступлений или категорий преступлений не является более ограниченным, чем круг преступлений, к которым она применяет меры, предусмотренные статьей 30 настоящей Конвенции. Каждая Сторона рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статье 29 настоящей Конвенции.

4. Если Сторона ввиду ограничений, которые предусмотрены ее внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 29 и 30, в отношении информации, передаваемой по компьютерной системе поставщика услуг, которая:

a) используется для обслуживания замкнутой группы пользователей; и

b) не использует сетей связи общего пользования, а также не соединена ни с какими другими компьютерными системами, как общего пользования, так и частными, эта Сторона может сохранить за собой право не применять указанных мер к такой передаче информации. Каждая Сторона рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статьях 29 и 30 настоящей Конвенции.

5. Если Сторона в силу ограничений, установленных в ее законодательстве, действовавшем на момент принятия настоящей Конвенции, не может применять меры, указанные в статье 31, эта Сторона может сохранить за собой право не применять эти меры. Каждая Сторона рассматривает возможность ограничения

[13] Текст для данного раздела позаимствован в основном из Будапештской конвенции, Конвенции Африканского союза о кибербезопасности и защите персональных данных, Закона об электронных сделках 2008 года (Закон 772) и Закона о кибербезопасности 2020 года (Закон 1038). Эти документы формируют законодательную базу Ганы для борьбы с киберпреступностью.

сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статье 31 настоящей Конвенции.

Статья 24
Условия и гарантии

1. Каждая Сторона обеспечивает, чтобы полномочия и процедуры, предусмотренные в настоящей главе, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, закрепленными в положениях ее внутреннего законодательства, которые обеспечивают надлежащую и полную защиту прав человека и основных свобод, включая права, вытекающие из обязательств, принятых ею в соответствии с Международным биллем о правах человека[14], в том числе в соответствии со Всеобщей декларацией прав человека и Международным пактом о гражданских и политических правах, а также с другими применимыми международно-правовыми документами по правам человека, и которые устанавливают принципы соразмерности и необходимости и требование относительно осуществления судебного надзора.

2. Такие условия и гарантии с учетом характера соответствующего полномочия или процедуры включают, в частности, судебный или иной независимый надзор, основания для применения и ограничение сферы и сроков действия такого полномочия или процедуры.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждая Сторона рассматривает вопрос о воздействии предусмотренных настоящим разделом полномочий и процедур на права, обязанности и законные интересы третьих лиц.

Статья 25
Оперативное обеспечение сохранности хранящихся компьютерных данных[15]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы ее компетентные органы имели возможность посредством распоряжений или иным образом оперативно обеспечивать сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Сторона реализует положения пункта 1 выше посредством распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутренним законодательством.

---

[14] Управление Верховного комиссара Организации Объединенных Наций по правам человека, «Международное право в области прав человека» (https://www.ohchr.org/ru/instruments-and-mechanisms/international-human-rights-law).

[15] На основе Будапештской конвенции, Конвенции Африканского союза о кибербезопасности и защите персональных данных, Закона Ганы об электронных сделках 2008 года (Закон 772) и Закона Ганы о кибербезопасности 2020 года (Закон 1038).

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 19 и 20.

Статья 26
Оперативное обеспечение сохранности и частичное раскрытие данных о трафике[16]

1. Каждая Сторона принимает в отношении данных о трафике, сохранность которых должна быть обеспечена, такие законодательные и иные меры, какие могут потребоваться для того, чтобы:

a) гарантировать оперативное обеспечение сохранности данных о трафике независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения; и

b) гарантировать оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этим органом, достаточного объема данных о трафике, которые позволят Стороне идентифицировать поставщиков услуг и путь, по которому передавалось сообщение.

2. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

Статья 27
Распоряжение о предоставлении информации

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для предоставления ее компетентным органам следующих полномочий:

a) дать распоряжение лицу на его территории о предоставлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на компьютерном носителе данных; и

b) дать распоряжение поставщику, предлагающему свои услуги на территории этой Стороны, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы постановление о предоставлении компьютерных данных или сведений об абонентах было получено соответствующим компетентным органом под надзором независимого контролирующего органа, такого как судебный орган. Такие меры обеспечивают требование, согласно которому компетентный орган должен представить независимому надзорному органу разумные основания, подтверждающие, что компьютерные данные или сведения об абоненте, в отношении которого ведется расследование, обоснованно необходимы для целей конкретного уголовного расследования.

3. Для целей пункта 2 компетентный орган:

a) объясняет независимому надзорному органу, почему компетентный орган считает, что запрашиваемые компьютерные данные или сведения об абонентах имеются:

i) у лица, которое имеет контроль над компьютерными данными или компьютерной системой или владеет ей; или

ii) соответствующего поставщика услуг;

[16] На основе Будапештской конвенции.

b) определяет и конкретно объясняет вид запрашиваемых компьютерных данных или сведений об абонентах,

c) указывает, какие меры следует принять для получения сведений об абонентах или компьютерных данных,

i) соблюдая конфиденциальность сведений о других пользователях, клиентах и третьих лицах; и

ii) не раскрывая сведений об абонентах или компьютерных данных любого субъекта, не имеющего отношения к расследованию.

4. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться для обеспечения того, чтобы независимый надзорный орган мог вынести постановление о предоставлении информации в соответствии с пунктом 2, если он убежден, что:

a) запрашиваемая информация является соответствующей, соразмерной и необходимой для целей конкретного уголовного расследования или судебного преследования;

b) должны быть приняты меры для обеспечения того, чтобы постановление исполнялось при соблюдении конфиденциальности других пользователей, клиентов и третьих лиц и без раскрытия информации и данных любого субъекта, не имеющего отношения к расследованию; и

c) расследование может не принести результатов или серьезно пострадать без разрешения на предоставление информации.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

6. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержании информации, с помощью которых можно установить:

a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;

c) любые другие сведения о месте установки оборудования связи, имеющиеся в соглашении или договоре на обслуживание.

Статья 28
Обыск и выемка хранящихся компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на проведение обыска или получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на ее территории.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда ее компетентные органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на территории этой Стороны, и такие данные в законном порядке могут

быть получены из первой системы или с ее помощью, эти компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на эту другую систему.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на выемку или аналогичную защиту компьютерных данных в соответствии с пунктом 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных;

d) обеспечение недоступности этих компьютерных данных в компьютерной системе, к которой получен доступ, или их извлечение из нее.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочия на дачу распоряжения любому лицу, которое обладает знаниями о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации, с тем чтобы обеспечить принятие мер, указанных в пунктах 1 и 2.

5. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий, позволяющим им иметь в сопровождении уполномоченное лицо или при содействии этого лица обеспечить возможность принятия мер, указанных в пунктах 1, 2 и 3.

6. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на изъятие любого компьютера, электронной записи, программы, информации, документа или предмета при исполнении ордера в соответствии с ее внутренним законодательством, если у компетентного органа имеются разумные основания полагать, что совершено любое из преступлений, признанных таковыми в соответствии со статьями 1–16 настоящей Конвенции, или готовится его совершение.

7. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

Статья 29
Сбор в режиме реального времени данных о трафике

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

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

b) обязывать 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 и записывать данные о трафике в режиме реального времени, которые связаны с конкретными сообщениями на ее территории, передаваемыми с помощью компьютерной системы.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы полномочие, предусмотренное настоящей статьей, было получено соответствующим компетентным органом только под контролем независимого надзорного органа, такого как судебный орган. Такие меры обеспечивают требование, согласно которому компетентный орган должен представить независимому надзорному органу разумные основания, подтверждающие, что компьютерные данные или сведения об абоненте, в отношении которого ведется расследование, обоснованно необходимы для целей конкретного уголовного расследования.

3. Для целей пункта 2 компетентный орган:

a) объясняет независимому надзорному органу, почему компетентный орган считает, что запрашиваемые компьютерные данные или информация об абонентах имеются:

i) у лица, которое имеет контроль над компьютерными данными или компьютерной системой или владеет ей; или

ii) поставщика услуг;

b) определяет и конкретно объясняет вид запрашиваемых данных о трафике;

c) определяет и конкретно объясняет преступления, в связи с которыми запрашиваются полномочия, предусмотренные настоящей статьей;

d) указывает, какие меры следует принять для получения сведений об абонентах или компьютерных данных,

i) соблюдая конфиденциальность сведений о других пользователях, клиентах и третьих лицах; и

ii) не раскрывая сведений об абонентах или компьютерных данных любого субъекта, не имеющего отношения к расследованию.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы независимый надзорный орган мог предоставить право собирать данные о трафике в режиме реального времени, если независимый надзорный орган убедится, что:

a) степень перехвата является соответствующей, соразмерной и необходимой для целей конкретного уголовного расследования или судебного преследования;

b) должны быть приняты меры для обеспечения того, чтобы постановление исполнялось при соблюдении конфиденциальности других пользователей, клиентов и третьих лиц и без раскрытия информации и данных любого субъекта, не имеющего отношения к расследованию; и

c) расследование может быть сорвано или серьезно затруднено, если не разрешить сбор данных о трафике в режиме реального времени.

5. Если Сторона в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то она может принять законодательные и иные меры, которые могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике, связанных с конкретными сообщениями, которые передаются на ее территории, с использованием технических средств на этой территории.

6. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

7. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

Статья 30
Перехват данных о содержании

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных правонарушений, подлежащих квалификации в соответствии с нормами ее внутреннего законодательства, для предоставления ее компетентным органам следующих полномочий:

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

b) обязывать поставщиков услуг в пределах имеющихся у них технических возможностей:

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

ii) сотрудничать с компетентными органами и помогать им собирать и записывать данные о содержании в режиме реального времени, которые связаны с конкретными сообщениями на ее территории, передаваемыми с помощью компьютерной системы.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы полномочие, предусмотренное настоящей статьей, было получено соответствующим компетентным органом только под контролем независимого надзорного органа, такого как судебный орган. Такие меры обеспечивают требование, согласно которому компетентный орган должен представить независимому надзорному органу разумные основания для разрешения перехвата данных о содержании сообщений, связанных с лицом или помещением, в отношении которого ведется расследование для достижения одной из следующих целей:

a) обеспечение интересов национальной безопасности;

b) предотвращение или раскрытие серьезного преступления;

c) обеспечение интересов экономического благополучия граждан в той мере, в какой эти интересы также соответствуют интересам национальной безопасности; или

d) выполнение просьбы об оказании взаимной правовой помощи.

3. Для целей пункта 2 компетентный орган:

a) объясняет независимому надзорному органу, почему компетентный орган считает, что запрашиваемые данные о содержании имеются:

i) у лица, которое имеет контроль над компьютерной системой или владеет ей;

ii) поставщика услуг;

b) определяет и объясняет вид данных о содержании, которые, как подозревается, находятся в компьютерной системе или во владении либо под контролем поставщика услуг;

c) определяет и конкретно объясняет преступления, в связи с которыми запрашивается полномочие, предусмотренное настоящей статьей;

d) указывает, какие меры следует принять для получения данных о содержании,

i) соблюдая конфиденциальность сведений о других пользователях, клиентах и третьих лицах; и

ii) не раскрывая данных о трафике любого субъекта, не имеющего отношения к расследованию.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы независимый надзорный орган мог предоставить полномочие на перехват данных о содержании, если независимый надзорный орган убедится, что:

a) степень перехвата является соответствующей, соразмерной и необходимой для целей конкретного уголовного расследования или уголовного преследования;

b) принимаются меры для обеспечения того, чтобы полномочие на перехват данных о содержании осуществлялось при соблюдении конфиденциальности других пользователей, клиентов и третьих лиц и без раскрытия информации и данных любого субъекта, не имеющего отношения к расследованию; и

c) расследование может не принести результатов или серьезно пострадать без разрешения на перехват данных.

5. Если Сторона в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то она может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о содержании конкретного сообщения на своей территории путем применения технических средств на этой территории.

6. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

7. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

Статья 31
Сохранение данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы поставщик услуг на ее территории сохранял:

a) информацию об абонентах в течение как минимум шести лет;

b) данные о трафике в течение 12 месяцев.

2. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 23 и 24.

3. Если Сторона в силу ограничений, которые установлены в ее законодательстве, действовавшем на момент принятия настоящей Конвенции, не может применять меры, указанные в настоящей статье, эта Сторона может сохранить за собой право не применять эти меры. Каждая Сторона рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в настоящей статье.

Статья 32
Конфискация и арест

1. Каждая Сторона принимает, в максимально возможной степени в рамках своей внутренней правовой системы, такие меры, какие могут потребоваться для обеспечения конфискации:

a) доходов от преступлений, охватываемых настоящей Конвенцией, или имущества, стоимость которого соответствует стоимости таких доходов;

b) имущества, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении преступлений, охватываемых настоящей Конвенцией.

2. Каждая Сторона принимает такие меры, какие могут потребоваться для обеспечения выявления, отслеживания, замораживания или ареста любого из перечисленного в пункте 1 настоящей статьи, с целью последующей конфискации.

3. Если доходы от преступлений были превращены или преобразованы, полностью или частично, в другое имущество, то меры, указанные в настоящей статье, применяются в отношении такого имущества.

4. Если такие доходы от преступлений были приобщены к имуществу, приобретенному из законных источников, то конфискации, без ущерба для любых полномочий, касающихся замораживания или ареста, подлежит та часть имущества, которая соответствует оцененной стоимости приобщенных доходов.

5. К прибыли или другим выгодам, которые получены от доходов от преступлений, от имущества, в которое были превращены или преобразованы доходы от преступлений, или от имущества, к которому были приобщены доходы от преступлений, также применяются меры, указанные в настоящей статье, таким же образом и в той же степени, как и в отношении доходов от преступлений.

6. Для целей настоящей статьи каждая Сторона уполномочивает свои суды или другие компетентные органы выносить постановления о представлении или аресте банковских, финансовых или коммерческих документов. Стороны не уклоняются от принятия мер в соответствии с положениями настоящего пункта, ссылаясь на необходимость сохранения банковской тайны.

7. Каждая Сторона может рассмотреть возможность установления требования о том, чтобы лицо, совершившее преступление, доказало законное происхождение предполагаемых доходов от преступления или другого имущества, подлежащего конфискации, в той мере, в какой такое требование соответствует основополагающим принципам ее внутреннего законодательства и характеру судебного и иного разбирательства.

8. Положения настоящей статьи не толкуются как наносящие ущерб правам добросовестных третьих лиц.

9. Никакое положение настоящей статьи не затрагивает принципа, согласно которому предусмотренные в ней меры определяются и осуществляются в соответствии с положениями внутреннего законодательства Стороны и при условии их соблюдения.

Статья 33
Юрисдикция

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями статей 5–20 настоящей Конвенции, когда такое правонарушение совершено:

a) на ее территории; или

b) борту судна под флагом этой Стороны; или

c) борту воздушного судна, зарегистрированного в соответствии с законодательством этой Стороны; или

d) одним из ее граждан, если это преступление является наказуемым согласно уголовному праву в месте его совершения или если это преступление совершено за пределами территориальной юрисдикции какого-либо государства.

2. Каждая Сторона может сохранить за собой право не применять или применять только в конкретных случаях или условиях нормы о юрисдикции, изложенные в пункте 1 (b)–(d) настоящей статьи или в любой их части.

3. Для целей статьи о выдаче, содержащейся в настоящей Конвенции, каждая Сторона принимает такие меры, какие могут потребоваться для установления

юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, в случаях, когда предполагаемый правонарушитель находится на ее территории и она по получении просьбы о выдаче не выдает его другой Стороне исключительно на основании его гражданства.

4. Настоящая Конвенция не исключает осуществления какой-либо Стороной уголовной юрисдикции в соответствии с ее внутренним законодательством.

5. Когда несколько Сторон заявляют о своей юрисдикции в отношении предполагаемого преступления, признанного таковым в соответствии с настоящей Конвенцией, заинтересованные Стороны, в надлежащих случаях, проводят консультации в целях определения наиболее подходящей юрисдикции для уголовного преследования.

Иран (Исламская Республика)

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

3. Правоприменение и процессуальные меры

Преступники постоянно и все чаще злоупотребляют услугами, предоставляемыми частным сектором, включая поставщиков услуг и платформы социальных сетей. Эта серьезная проблема требует выработки конкретных мер противодействия. С учетом фундаментального и решающего значения сотрудничества этих субъектов с правоохранительными органами в расследовании и уголовном преследовании в отношении таких преступлений и в пресечении таких злоупотреблений, в Конвенции следует конкретно описать обязательства и предусмотреть соответствующие положения о сотрудничестве частного сектора, поставщиков услуг и других аналогичных субъектов с правоохранительными органами, в частности секторов и поставщиков, имеющих глобальный или значительный охват на международном уровне.

Действенные и своевременные меры по установлению эффективного сотрудничества между этими субъектами и правоохранительными и судебными органами должны стать неотъемлемой частью Конвенции. С этой целью в специальных разделах Конвенции следует рассмотреть вопросы сотрудничества между национальными компетентными органами и такими субъектами, как поставщики услуг и частный сектор, и определить конкретные меры, включая оперативное обеспечение сохранности и раскрытие электронных данных правоохранительным органам.

Поскольку электронные доказательства представляют собой важнейший элемент расследования и уголовного преследования преступлений, совершенных с использованием информационно-коммуникационных технологий, в Конвенции необходимо установить, в частности, стандартные процедуры для получения, хранения и раскрытия подлинных электронных доказательств. Стандартные процедуры позволяют унифицировать и согласовывать меры противодействия таким преступлениям на национальном уровне, что также может обеспечить более эффективное сотрудничество между правоохранительными и судебными органами на международном уровне в вопросах сохранения и предоставления электронных доказательств.

Изъятие и возвращение активов и доходов от преступлений играют важную роль в лишении преступников стимулов для совершения преступлений и снижении уровня рецидивизма, а также в предоставлении компенсации потерпевшим. Поэтому оперативный арест, изъятие и возвращение доходов от преступлений должны стать одним из ключевых элементов Конвенции. Соответствующие положения Конвенции, касающиеся правоприменения и процессуальных мер, должны предоставлять национальным компетентным органам полномочия, обеспечивающие беспрепятственное и оперативное изъятие активов и доходов

от преступлений, а также предусматривать самые широкие меры помощи и сотрудничества в этой области.

Борьба с использованием информационно-коммуникационных технологий в преступных целях требует, чтобы правоохранительные органы имели и использовали современные технологии в ходе расследования и уголовного преследования в отношении преступлений для соразмерного противодействия таким преступлениям. Таким образом, следует поощрять и поддерживать использование современных технологий правоохранительными и судебными органами, включая процессуальные меры по предупреждению и пресечению преступлений, совершаемых с помощью информационно-коммуникационных технологий. Это также требует предоставления правоохранительным и судебным органам необходимого оборудования и технологий посредством оказания политически нейтральной и надежной технической поддержки.

Япония

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

3. Процессуальные меры и правоприменение

3.1. В отношении процессуальных мер для расследования киберпреступлений можно рассмотреть возможность оперативного обеспечения сохранности, обыска и выемки хранящихся компьютерных данных, вынесения распоряжений о предоставлении информации и сбора данных о трафике в режиме реального времени.

3.2. Мы могли бы рассмотреть возможность применения этих процессуальных положений в ходе расследования и уголовного производства в связи с уголовными преступлениями, признанными таковыми в данной Конвенции, и другими уголовными преступлениями, совершаемыми с помощью компьютерной системы, а также при сборе электронных доказательств совершения уголовного преступления.

3.3. При предоставлении вышеуказанных полномочий компетентным органам каждого государства-участника необходимо ввести положения, предусматривающие, что каждое государство-участник должно обеспечить надлежащую защиту прав, возникающих в соответствии с его обязательствами по договорам о правах человека и другим международно-правовым документам, а также других прав и свобод человека и что следует соблюдать внутреннее законодательство, устанавливающее принцип соразмерности. Данная Конвенция должна подтвердить эту концепцию в главе о процессуальных мерах и правоприменении.

Мексика

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

Процессуальные меры и правоприменение

С учетом важности цифровых доказательств для целей расследования, уголовного преследования и правоприменения ожидается, что государства — участники Конвенции согласуют общие и минимально одобренные процессуальные меры для получения, обработки и сохранения цифровых доказательств. Можно добавить следующее положение: «Государства могут рассмотреть и использовать все положения, содержащиеся в существующих международных документах, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности, для целей расследования и/или сбора доказательств и сохранения электронных доказательств».

В отношении частных субъектов, предоставляющих услуги в области информационно-коммуникационных технологий, Мексика рекомендует включить следующие положения:

> «Государства-участники обязуются ввести для частных субъектов, предоставляющих услуги в области информационно-коммуникационных технологий, которые учреждены на их соответствующей территории или действуют под их национальной юрисдикцией, обязанность принимать и осуществлять политику и процедуры должной предусмотрительности во избежание причинения ущерба третьим лицам.
>
> Государства-участники также обязуются принимать надлежащие меры для обеспечения того, чтобы частные субъекты, учрежденные на их территории или действующие под их национальной юрисдикцией, не нарушали законы других государств-участников».
>
> Было бы также уместно включить общую рекомендацию в отношении обязанности частных субъектов, предоставляющих услуги в области информационно-коммуникационных технологий, осуществлять эффективное сотрудничество с национальными правоохранительными и судебными органами в области расследования и уголовного преследования киберпреступлений, соблюдая при этом применимые положения о неприкосновенности частной жизни.

Новая Зеландия

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

Положения о процессуальных мерах и правоприменении

10. Новая Зеландия поддерживает включение в данную Конвенцию положений, обеспечивающих оперативное сохранение цифровых доказательств и доступ к ним, при условии включения в нее всеобъемлющих гарантий в целях защиты прав человека и основных свобод, уважения верховенства права и соблюдения принципа соразмерности. Например, положения, касающиеся:

- обыска и выемки конкретных хранящихся компьютерных данных;
- сбора конкретных компьютерных данных в режиме реального времени;
- перехвата конкретных компьютерных данных;
- обеспечения сохранности конкретных компьютерных данных;
- распоряжений о предоставлении конкретных компьютерных данных, находящихся во владении или под контролем лица и хранящихся в компьютерной системе или на носителе компьютерных данных.

11. Новая Зеландия также поддержит включение положений, предусматривающих меры, которые не допускают извлечения преступниками выгоды от совершенных ими преступлений, такие как арест и конфискация доходов от преступлений, а также положений, способствующих укреплению сотрудничества с правоохранительными органами.

Норвегия

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

Процессуальные меры и правоприменение

9. Специальному комитету следует использовать опыт осуществления действующих международных договоров, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Организации Объединенных Наций против коррупции. В то же время, с учетом того что в новой Конвенции будут рассмотрены проблемы современной киберпреступности, она должна содержать требование, чтобы государства-участники включили положения своего внутреннего законодательства, которые специально регулируют вопрос о применении электронных доказательств. Кроме того, Специальный комитет должен помнить о том, что время и эффективность имеют первостепенное значение при расследовании или уголовном преследовании в отношении киберпреступлений. Конвенция должна позволять осуществлять сотрудничество в области сбора и получения электронных доказательств в отношении преступлений любых видов, а не только киберпреступлений.

10. Во избежание излишнего дублирования усилий она должна предусматривать эффективное использование и укрепление существующих и налаженных каналов связи и сетей.

11. Необходимо отметить ключевую роль частного сектора.

12. Следует рассмотреть вопросы оказания помощи и защиты потерпевшим, а также защиты свидетелей.

13. Необходимо, чтобы положения о процессуальных мерах согласовывались с гарантиями надлежащей правовой процедуры и защиты прав человека и основных свобод.

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

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

Раздел 2

Уголовное производство и правоприменение

Статья 31
Сфера применения процессуальных норм

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений и иных противоправных деяний и осуществления судебного разбирательства в связи с ними.

2. За исключением случаев, когда положениями статьи 33 настоящей Конвенции предусматривается иное, каждое Государство-участник применяет полномочия и процедуры, упомянутые в пункте 1 настоящей статьи, в отношении:

a) преступлений и иных противоправных деяний, предусмотренных статьями 6–29 настоящей Конвенции;

b) других преступлений и иных противоправных деяний, совершенных с использованием информационно-коммуникационных технологий;

c) сбора доказательств, в том числе электронных, совершения преступлений и иных противоправных деяний.

3. a) Каждое Государство-участник может сделать оговорку о сохранении за собой права применять меры, предусмотренные статьей 38 настоящей Конвенции, только в отношении преступлений или категорий преступлений, указанных в этой оговорке, при условии, что круг таких преступлений или категорий преступлений не более ограничен, чем круг преступлений, к которым она применяет меры, предусмотренные статьей 33 настоящей Конвенции. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки с целью максимально широкого применения мер, предусмотренных положением статьи 38 настоящей Конвенции;

b) в том случае, когда Государство-участник ввиду ограничений, предусмотренных внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 33 и 38 настоящей Конвенции, к информации, передаваемой по информационной системе поставщика услуг, которая:

i) используется для обслуживания отдельной группы пользователей; и

ii) не использует информационно-телекоммуникационную сеть, а также не соединена ни с какими другими информационными системами,

это Государство-участник может сохранить за собой право не применять указанные меры к такой передаче информации.

Статья 32
Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящим разделом, 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 от 16 декабря 1966 года и по другим применимым международным договорам по правам человека.

2. Такие условия и гарантии с учетом характера полномочий и процедур 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 публичным интересам, в частности осуществлению правосудия, Государство-участник рассматривает влияние предусмотренных данным разделом полномочий и процедур на права, законные интересы и ответственность третьих лиц.

Статья 33
Сбор информации, передаваемой с использованием информационно-коммуникационных технологий

1. Каждое Государство-участник принимает такие законодательные и иные меры в целях противодействия преступлениям, предусмотренным настоящей Конвенцией и признанным таковыми в соответствии с его внутренним законодательством, какие могут быть необходимы для того, чтобы наделить его компетентные органы полномочиями:

a) собирать или записывать с применением технических средств информацию, передаваемую с использованием информационно-коммуникационных технологий, на территории этого Государства-участника; и

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

i) собирать или записывать с использованием технических средств на территории этого Государства-участника информацию в электронной форме, включающую данные о содержании сообщений и передаваемую с использованием информационно-коммуникационных технологий; или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им в сборе или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений и передаваемой с использованием информационно-коммуникационных технологий, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов его системы внутреннего права не может принять меры, предусмотренные в пункте 1 (a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений и передаваемой с использованием информационно-коммуникационных технологий 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 факта осуществления любых полномочий и действий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 34
Оперативное обеспечение сохранности накопленной информации в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы его компетентные органы имели возможность отдавать соответствующие распоряжения или указания или аналогичным образом оперативно обеспечивать сохранность конкретной электронно-цифровой информации, включая технические параметры трафика, в частности в случаях, когда имеются основания полагать, что эти данные особенно подвержены риску уничтожения, блокирования, копирования или модификации, в том числе в результате истечения срока давности их хранения, установленного внутренним законодательством или правилами предоставления услуг провайдера.

2. Если Государство-участник реализует положения пункта 1 настоящей статьи посредством дачи распоряжения какому-либо лицу (в том числе юридическому) об обеспечении сохранности конкретной хранимой информации, находящейся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные правовые меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эту информацию и обеспечивать ее целостность в течение необходимого периода времени, но не превышающего такого 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 также 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 31 и 32 настоящей Конвенции.

Статья 35
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 34 настоящей Конвенции, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

a) гарантировать, чтобы такое оперативное обеспечение сохранности технических параметров трафика было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу данной информации; и

b) гарантировать оперативное раскрытие компетентным органам этого Государства-участника достаточного количества технических параметров трафика, которое позволит соответствующему Государству-участнику идентифицировать поставщиков услуг и путь, которым передавалась указанная информация.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 36
Распоряжение о предоставлении информации

1. В целях, предусмотренных пунктом 1 статьи 31 настоящей Конвенции, каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы предоставить своим компетентным органам полномочия отдавать распоряжения:

a) лицу на территории этого Государства-участника о предоставлении конкретной электронно-цифровой информации, находящейся во владении или под контролем этого лица;

b) поставщику услуг, предлагающему свои услуги на территории этого Государства-участника, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

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:

a) вид используемой информационно-коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность пользователя, его почтовый или иные адреса, 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;

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

Статья 37
Обыск и выемка информации, хранимой или обрабатываемой в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на обыск в целях получения доступа к находящимся на территории этого Государства-участника или под его юрисдикцией:

a) устройствам ИКТ и хранящейся на них информации; и

b) носителям информации, на которых может храниться искомая электронно-цифровая информация.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы, в случае когда его компетентные органы в ходе обыска, производимого в соответствии с положениями пункта 1 (a) настоящей статьи, выясняют, что искомая информация хранится на другом устройстве информационно-коммуникационной технологии на территории этого Государства-участника, такие органы имели возможность оперативно произвести обыск в целях получения доступа к этому другому устройству информационно-коммуникационной технологии или содержащимся в нем данным.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий производить выемку на территории либо под юрисдикцией Государства-участника информации в электронной форме или иным аналогичным образом обеспечивать ее сохранность. Эти меры должны включать, в частности, предоставление следующих полномочий:

a) производить выемку устройств информационно-коммуникационной технологии, используемых для хранения информации, либо иным образом обеспечивать их сохранность;

b) изготавливать и сохранять копии соответствующей информации в электронно-цифровой форме;

c) обеспечивать целостность относящейся к делу хранимой информации;

d) изымать информацию, хранящуюся или обрабатываемую в электронно-цифровой форме на устройстве информационно-коммуникационной технологии.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий привлекать в порядке, установленном его внутренним законодательством, любое лицо, обладающее специальными знаниями о функционировании соответствующей информационной системы, информационно-телекоммуникационной сети или их частей или применяемых мерах защиты информации, для предоставления необходимых сведений и/или оказания содействия в осуществлении действий, предусмотренных пунктами 1–3 настоящей статьи.

5. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 38
Сбор в режиме реального времени технических параметров трафика

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий:

a) собирать или записывать с применением технических средств технические параметры трафика, передаваемого с использованием информационно-коммуникационных технологий, на территории этого Государства-участника; и

b) обязывать поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этого Государства-участника технические параметры трафика; или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им собирать или записывать в режиме реального времени технические параметры трафика, связанные с конкретной информацией, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов своей системы внутреннего законодательства не может принять меры, предусмотренные в пункте 1 (a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени технических параметров трафика 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 факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 39
Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, когда они совершены:

a) на территории этого Государства-участника; или

b) борту судна, которое несло флаг этого Государства-участника в момент совершения деяния, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника в такой момент.

2. При условии соблюдения статьи 3 настоящей Конвенции Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления и иного противоправного деяния, когда:

a) деяние совершено против гражданина этого Государства-участника, лица без гражданства, постоянно проживающего на его территории, юридического лица, учрежденного или имеющего постоянное представительство на его территории, государственного или правительственного объекта, включая помещения дипломатического представительства и консульского учреждения этого Государства-участника; или

b) деяние совершено гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории; или

c) деяние совершено против этого Государства-участника; или

d) деяние совершено полностью или частично за пределами территории Государства-участника, но его последствия составляют на его территории преступление или приводят к совершению преступления.

3. Для целей статьи 47 настоящей Конвенции каждое Государство-участник принимает такие меры, какие могут потребоваться, 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 на том основании, что это лицо является его гражданином либо лицом, которому этим Государством-участником предоставлен статус беженца.

4. Каждое Государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления и которое не выдает его, обязано, в случаях, предусмотренных в пунктах 1 и 2 настоящей статьи, без каких бы то ни было исключений и независимо от того, совершено ли оно на территории этого Государства-участника, без излишних задержек передать дело своим компетентным органам для целей преследования путем проведения разбирательства в соответствии с законодательством этого государства.

5. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, 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.

6. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной и административной юрисдикции, установленной Государством-участником в соответствии с его внутренним законодательством.

Глава III
Меры по противодействию преступлениям и иным противоправным деяниям в информационном пространстве

[…]

Статья 45
Меры по защите свидетелей

Каждое Государство-участник рассматривает возможность принятия таких законодательных мер, которые могут быть необходимы для обеспечения эффективной защиты:

a) лиц, которые добросовестно и на разумных основаниях предоставляют информацию, касающуюся противоправных деяний, предусмотренных статьями 6–28 настоящей Конвенции, или иным образом сотрудничают со следственными или судебными органами;

b) свидетелей, дающих показания в отношении противоправных деяний, предусмотренных статьями 6–28 настоящей Конвенции, а также потерпевших;

c) при необходимости членов семей лиц, указанных в подпунктах (a) и (b) настоящей статьи.

Южная Африка

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

Глава III
Процессуальные меры и правоприменение

Статья 18
Процессуальные положения

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящей статьи, в целях проведения конкретного уголовного расследования или судебного разбирательства.

2. Если в статье 32 специально не оговорено иное, каждое Государство-участник применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, связанных с использованием информационно-коммуникационных технологий и признанных таковыми в соответствии со статьями [...]–[...] настоящей Конвенции;

b) других уголовных преступлений, совершенных с помощью информационно-коммуникационных технологий; и

c) сбора доказательств в электронной форме в отношении уголовного преступления, совершенного с использованием информационно-коммуникационных технологий.

3. Каждое Государство-участник может сохранить за собой право применять меры, указанные в статье 31, только в отношении преступлений или категорий преступлений, связанных с использованием информационно-коммуникационных технологий, указанных в оговорке, при условии, что круг таких преступлений или категорий преступлений не является более ограниченным, чем круг преступлений, к которым оно применяет меры, указанные в статье 32. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статье 31 настоящей Конвенции.

4. Если Государство-участник ввиду ограничений, предусмотренных его внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 31 и 32, в отношении информации, передаваемой с использованием информационно-коммуникационной системы поставщика услуг, которая:

a) используется для обслуживания отдельной группы пользователей; и

b) не использует сетей связи общего пользования, а также не соединена ни с какими другими информационно-коммуникационными системами, как общего пользования, так и частными, это Государство-участник может сохранить за собой право не применять этих мер к такой передаче информации. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статьях 31 и 32 настоящей Конвенции.

Статья 19
Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы полномочия и процедуры, указанные в настоящей статье, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными нормами его внутреннего законодательства, которые обеспечивают надлежащую защиту прав и свобод человека, включая права и основные свободы,

вытекающие из обязательств этого Государства-участника по соглашениям, международным договорам и применимым международным документам в области прав человека, и которые закрепляют принцип соразмерности в соответствии с суверенитетом Государства-участника.

2. Такие условия и гарантии с учетом характера соответствующих полномочий и процедур включают, в частности, судебный или иной независимый надзор, основания для применения таких полномочий и процедур и ограничение их сферы и сроков действия.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждое Государство-участник рассматривает вопрос о воздействии предусмотренных настоящей главой полномочий и процедур на права, обязанности и законные интересы третьих лиц.

Статья 20
Оперативное обеспечение сохранности хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы его компетентные органы могли посредством дачи распоряжений или иным образом оперативно обеспечивать сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в информационно-коммуникационной системе, в частности когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения.

2. Если Государство-участник реализует положения пункта 1 выше посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего семи дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 27 и 28.

Статья 21
Обыск и выемка хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на проведение обыска или получение аналогичного доступа:

a) к информационно-коммуникационным технологиям, компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на его территории.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда его компетентные органы проводят обыск или получают аналогичный доступ к любым информационно-коммуникационным системам или компонентам, являющимся частью таких систем, конкретной компьютерной системе или ее части

в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в других информационно-коммуникационных системах или компонентах, являющихся частью таких систем, компьютерной системе или ее части на его территории, и такие данные законно доступны из первой системы или с ее помощью, эти компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на такую другую систему.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для наделения его компетентных органов полномочиями, когда это необходимо, с помощью или в присутствии уполномоченных должностных лиц иностранного/другого Государства-участника производить выемку или аналогичным образом обеспечивать защиту компьютерных данных, доступ к которым был получен в соответствии с пунктами 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту информационно-коммуникационных технологий или компонентов, составляющих их часть, компьютерной системы или ее части или компьютерного носителя данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных;

d) обеспечение недоступности или извлечение этих компьютерных данных в компьютерной системе или информационно-коммуникационных технологиях, к которым был получен доступ.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочия на дачу распоряжения любому лицу, обладающему знаниями о функционировании информационно-коммуникационных технологий или компонентов, являющихся их частью, компьютерной системы или мер, применяемых для защиты содержащихся в ней компьютерных данных, предоставлять в разумных пределах необходимую информацию, чтобы обеспечить возможность принятия мер, указанных в пунктах 1 и 2.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 27 и 28.

Статья 22
Сбор в режиме реального времени данных о трафике

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

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

i) собирать или записывать с применением технических средств на территории этого Государства-участника; или

ii) сотрудничать с компетентными органами и помогать им собирать и записывать данные о трафике в режиме реального времени, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью информационно-коммуникационной технологии или компьютерной системы.

Статья 23
Перехват данных о содержании

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных преступлений, признанных таковыми в соответствии с нормами его внутреннего законодательства, для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

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

i) собирать или записывать с применением технических средств на территории этого Государства-участника; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать данные о содержании в режиме реального времени, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью информационно-коммуникационных технологий или компьютерной системы.

2. Если Государство-участник в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то оно может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о содержании конкретных сообщений на его территории путем применения технических средств на этой территории.

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

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями статей 27 и 28.

Статья 24
Замораживание, арест и конфискация

1. Несмотря на любые положения настоящей статьи, она не толкуется как наносящая ущерб правам добросовестных третьих лиц, и ничто, содержащееся в настоящей статье, не затрагивает принципа, согласно которому указанные в ней меры определяются и осуществляются в соответствии с положениями внутреннего законодательства Государства-участника и при условии их соблюдения.

2. Положения настоящей статьи не толкуются таким образом, при котором ущемляются права добросовестных третьих лиц.

3. Ничто, содержащееся в настоящей статье, не затрагивает принципа, согласно которому указанные в ней меры определяются и осуществляются в соответствии с положениями внутреннего законодательства Государства-участника и при условии их соблюдения.

4. Каждое Государство-участник принимает, в максимально возможной степени в рамках своей внутренней правовой системы, такие меры, какие могут потребоваться для обеспечения конфискации:

a) доходов от преступлений, которые получены в результате преступлений, совершенных с использованием информационно-коммуникационных технологий и признанных таковыми в соответствии с настоящей Конвенцией, или имущества, стоимость которого соответствует стоимости таких доходов и выгоде затронутого Государства-участника;

b) имущества, оборудования и других средств, использовавшихся или предназначавшихся для использования при совершении преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

4. Каждое Государство-участник принимает такие меры, какие могут потребоваться для обеспечения выявления, отслеживания, замораживания или ареста любого из перечисленного в пункте 1 настоящей статьи, с целью последующей конфискации.

5. Каждое Государство-участник принимает, в соответствии со своим внутренним законодательством, такие законодательные и другие меры, какие могут потребоваться для того, чтобы регулировать действия компетентных органов по управлению замороженным, арестованным или конфискованным имуществом, указанным в пунктах 1 и 2 настоящей статьи.

6. Если такие доходы от преступлений были превращены или преобразованы, полностью или частично, в другое имущество, то меры, указанные в настоящей статье, применяются в отношении такого имущества.

7. Если такие доходы от преступлений были приобщены к имуществу, приобретенному из законных источников, то конфискации, без ущерба для любых полномочий, касающихся замораживания или ареста, подлежит та часть имущества, которая соответствует оцененной стоимости приобщенных доходов.

8. К прибыли или другим выгодам, которые получены от таких доходов от преступлений, от имущества, в которое были превращены или преобразованы такие доходы от преступлений, или от имущества, к которому были приобщены такие доходы от преступлений, также применяются меры, указанные в настоящей статье, таким же образом и в той же степени, как и в отношении доходов от преступлений.

9. Для целей настоящей статьи и статьи [...] [о международном сотрудничестве] настоящей Конвенции каждое Государство-участник уполномочивает свои суды или другие компетентные органы выносить постановления о представлении или аресте банковских, финансовых или коммерческих документов. Государство-участник не уклоняется от принятия мер в соответствии с положениями настоящего пункта, ссылаясь на необходимость сохранения банковской тайны.

10. Государства-участники могут рассмотреть возможность установления требования о том, чтобы лицо, совершившее преступление, доказало законное происхождение таких предполагаемых доходов от преступления или другого имущества, подлежащего конфискации, в той мере, в какой такое требование соответствует основополагающим принципам их внутреннего законодательства и характеру судебного и иного разбирательства.

Статья 25
Распоряжение конфискованными доходами от преступлений или имуществом

1. Доходами от преступлений или имуществом, конфискованными Государством-участником на основании пункта 3 статьи 33 настоящей Конвенции, распоряжается это Государство-участник в соответствии со своим внутренним законодательством и административными процедурами.

2. Действуя по просьбе, направленной другим Государством-участником в соответствии со статьей 39 настоящей Конвенции, Государства-участники в той мере, в какой это допускается их внутренним законодательством, и в случае получения соответствующей просьбы, в первоочередном порядке рассматривают вопрос о возвращении конфискованных доходов от преступлений или имущества запрашивающему Государству-участнику, с тем чтобы оно могло предоставить компенсацию потерпевшим от преступления или возвратить такие доходы от преступлений или имущество их законным собственникам.

3. Действуя по просьбе, направленной другим Государством-участником в соответствии со статьей 41 настоящей Конвенции, Государство-участник может

особо рассмотреть возможность заключения соглашений или договоренностей относительно:

a) перечисления суммы, соответствующей стоимости доходов от преступлений или имущества, или средств, полученных в результате реализации таких доходов или имущества или их части, на счет, предназначенный для этой цели в соответствии со статьей [...] настоящей Конвенции, или межправительственным органам, специализирующимся на борьбе против организованной преступности;

b) передачи другим Государствам-участникам на регулярной или разовой основе части доходов от преступлений, или имущества, или средств, полученных в результате реализации таких доходов или имущества, в соответствии со своим внутренним законодательством или административными процедурами.

Статья 26
Сведения о судимости

Каждое Государство-участник может принимать такие законодательные или иные меры, какие могут потребоваться для учета, на таких условиях и в таких целях, какие оно сочтет надлежащими, любого ранее вынесенного в другом государстве обвинительного приговора в отношении лица, предположительно совершившего преступление, для использования такой информации в ходе уголовного производства в связи с преступлением, совершенным с использованием информационно-коммуникационных технологий и признанным таковым в соответствии с настоящей Конвенцией.

Статья 27
Меры по укреплению сотрудничества с правоохранительными органами

1. Каждое Государство-участник принимает надлежащие меры для того, чтобы поощрять лиц, которые участвуют или участвовали в организованных преступных группах:

a) к предоставлению информации, необходимой компетентным органам, в целях расследования и доказывания в связи с такими вопросами, как:

i) идентификационные данные, характер, членский состав, структура, местонахождение или деятельность организованных преступных групп;

ii) связи, в том числе международные связи, с другими организованными преступными группами;

iii) преступления, которые совершили или могут совершить организованные преступные группы;

b) предоставлению фактической, конкретной помощи компетентным органам, которая может способствовать лишению организованных преступных групп их ресурсов или доходов от преступлений.

2. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть возможность смягчения, в надлежащих случаях, наказания обвиняемого лица, которое добросовестно и существенным образом сотрудничает в расследовании или уголовном преследовании в связи с каким-либо преступлением, охватываемым настоящей Конвенцией.

3. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть, в соответствии с основополагающими принципами своего внутреннего законодательства, возможность предоставления иммунитета от уголовного преследования лицу, которое добросовестно и существенным образом сотрудничает в расследовании или уголовном преследовании в связи с преступлением, охватываемым настоящей Конвенцией.

4. Защита таких лиц осуществляется в порядке, предусмотренном в статье 34 настоящей Конвенции.

5. В тех случаях, когда лицо, которое упоминается в пункте 1 настоящей статьи и находится в одном Государстве-участнике, может добросовестно и существенным образом сотрудничать с компетентными органами другого Государства-участника, заинтересованные Государства-участники могут рассмотреть возможность заключения соглашений или договоренностей, в соответствии со своим внутренним законодательством, относительно возможного предоставления другим Государством-участником режима, указанного в пунктах 2 и 3 настоящей статьи.

Статья 28
Сотрудничество между правоохранительными органами

1. Государства-участники тесно сотрудничают друг с другом, действуя сообразно своим внутренним правовым и административным системам, в целях повышения эффективности правоприменительных мер для борьбы с преступлениями, совершенными с использованием информационно-коммуникационных технологий и охватываемыми настоящей Конвенцией. Каждое Государство-участник, в частности, принимает эффективные меры, направленные:

a) на укрепление или, если это необходимо, установление каналов связи между их компетентными органами, учреждениями и поставщиками интернет-услуг, с тем чтобы обеспечить надежный и быстрый обмен информацией о всех аспектах преступлений, связанных с использованием информационно-коммуникационных технологий и охватываемых настоящей Конвенцией, включая, если заинтересованные Государства-участники сочтут это надлежащим, связи с другими видами преступной деятельности;

b) сотрудничество с другими Государствами-участниками в проведении расследований в связи с преступлениями, совершенными с использованием информационно-коммуникационных технологий и охватываемыми настоящей Конвенцией, в целях выявления:

i) личности, местонахождения и деятельности лиц, подозреваемых в причастности к таким преступлениям, или местонахождения других причастных лиц;

ii) перемещения доходов от преступлений или имущества, полученного в результате совершения таких преступлений;

iii) перемещения имущества, орудий, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении таких преступлений;

c) предоставление, в надлежащих случаях, необходимых предметов или необходимого количества веществ для целей анализа или расследования;

d) содействие эффективной координации между их компетентными органами, учреждениями и поставщиками интернет-услуг и поощрение обмена сотрудниками и другими экспертами, включая, при условии заключения заинтересованными Государствами-участниками двусторонних соглашений или договоренностей, направление сотрудников по связям;

e) обмен с другими Государствами-участниками информацией о конкретных средствах и методах, применяемых организованными преступными группами, включая, в надлежащих случаях, маршруты и средства транспорта, а также использование поддельных удостоверений личности, измененных или поддельных документов или других средств сокрытия их деятельности посредством использования информационно-коммуникационных технологий;

f) обмен информацией и координацию административных и других мер, принимаемых в надлежащих случаях в целях заблаговременного выявления преступлений, связанных с использованием информационно-коммуникационных технологий и охватываемых настоящей Конвенцией.

2. Для целей введения в действие настоящей Конвенции Государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей о непосредственном сотрудничестве между их правоохранительными органами, а в случае когда такие соглашения или договоренности уже имеются, их совершенствования. В отсутствие таких соглашений или договоренностей между заинтересованными Государствами-участниками Государства-участники могут рассматривать настоящую Конвенцию в качестве основы для сотрудничества между правоохранительными органами в отношении преступлений, охватываемых настоящей Конвенцией. В надлежащих случаях Государства-участники в полной мере используют соглашения или договоренности, в том числе механизмы международных или региональных организаций, для расширения сотрудничества между своими правоохранительными органами.

3. Государства-участники стремятся сотрудничать, в пределах своих возможностей, в целях противодействия транснациональным организованным преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Статья 29
Совместные расследования

Государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей, в силу которых в связи с делами, являющимися предметом расследования, уголовного преследования или судебного разбирательства в одном или нескольких государствах, заинтересованные компетентные органы могут создавать органы по проведению совместных расследований. В отсутствие таких соглашений или договоренностей совместные расследования могут проводиться по соглашению в каждом отдельном случае. Государства-участники обеспечивают полное уважение суверенитета Государства-участника, на территории которого должно быть проведено такое расследование.

Статья 30
Специальные методы расследования

1. В целях эффективного противодействия использованию информационно-коммуникационных технологий в преступных целях каждое Государство-участник в той мере, в какой это допускается основными принципами его внутренней правовой системы, и в соответствии с условиями, предусмотренными его внутренним законодательством, принимает такие меры, какие могут потребоваться, в пределах имеющихся у него средств, с тем чтобы разрешить применение на его территории специальных методов расследования, таких как электронное или иные формы наблюдения и негласные операции, и обеспечить допустимость в суде полученных с их помощью доказательств без ущерба для угрозы кибербезопасности и конфиденциальности разведывательных данных каждого Государства-участника.

2. В целях расследования преступлений, связанных с использованием информационно-коммуникационных технологий и охватываемых настоящей Конвенцией, Государствам-участникам рекомендуется заключать при необходимости соответствующие двусторонние или многосторонние соглашения или договоренности для использования таких специальных методов расследования в рамках сотрудничества на международном уровне. Такие соглашения или договоренности заключаются и осуществляются при полном соблюдении принципа суверенного равенства государств и уважения основных прав человека и свобод и выполняются в строгом соответствии с установленными в них условиями.

3. В отсутствие соглашения или договоренности, указанных в пункте 2 настоящей статьи, решения об использовании таких специальных методов расследования на международном уровне принимаются в каждом отдельном случае и

могут при необходимости учитывать финансовые договоренности и взаимопонимание в отношении осуществления юрисдикции заинтересованными Государствами-участниками.

Статья 31
Возвращение активов и распоряжение ими

1. Имуществом, конфискованным Государством-участником на основании статьи 33 или 34 настоящей Конвенции, распоряжается, включая возвращение такого имущества его предыдущим законным собственникам согласно пункту 3 настоящей статьи, это Государство-участник в соответствии с положениями настоящей Конвенции и своим внутренним законодательством.

2. Каждое Государство-участник принимает, в соответствии с основополагающими принципами своего внутреннего законодательства, такие законодательные и иные меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам возвращать конфискованное имущество, действуя по просьбе, направленной другим Государством-участником, в соответствии с настоящей Конвенцией, с учетом прав добросовестных третьих лиц.

3. В соответствии пунктами 1 и 2 настоящей статьи запрашиваемое Государство-участник:

a) в случае противодействия использованию информационно-коммуникационных технологий, как указано в настоящей Конвенции, если конфискация была произведена в соответствии со статьей [...] и на основании окончательного судебного решения, вынесенного в запрашивающем Государстве-участнике, притом что запрашиваемое Государство-участник может отказаться от требования относительно такого судебного решения, — возвращает конфискованное имущество запрашивающему Государству-участнику;

b) в случае доходов от любого другого преступления, связанного с использованием информационно-коммуникационных технологий и охватываемого настоящей Конвенцией, если конфискация была произведена в соответствии со статьей [...] настоящей Конвенции и на основании окончательного судебного решения, вынесенного в запрашивающем Государстве-участнике, притом что запрашиваемое Государство-участник может отказаться от требования относительно такого судебного решения, — возвращает конфискованное имущество запрашивающему Государству-участнику, если запрашивающее Государство-участник обоснованно доказывает запрашиваемому Государству-участнику свое существовавшее ранее право собственности на такое конфискованное имущество или если запрашиваемое Государство-участник признает ущерб, причиненный запрашивающему Государству-участнику, в качестве основания для возвращения конфискованного имущества;

c) во всех других случаях — в первоочередном порядке рассматривает вопрос о возвращении конфискованного имущества запрашивающему Государству-участнику, возвращении такого имущества его предыдущим законным собственникам или выплате компенсации потерпевшим от преступления.

4. В надлежащих случаях, если только Государства-участники не примут иного решения, запрашиваемое Государство-участник может вычесть разумные расходы, понесенные в ходе расследования или судебного разбирательства, которые привели к возвращению конфискованного имущества или распоряжению им согласно настоящей статье.

5. В надлежащих случаях Государства-участники могут в соответствии со своим внутренним законодательством также особо рассмотреть возможность заключения в каждом отдельном случае соглашений или взаимоприемлемых договоренностей относительно окончательного распоряжения конфискованным имуществом.

Швейцария

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

2.3. Положения о процессуальных мерах и правоприменении

Раздел 1

Общие положения

Сфера действия процессуальных положений

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях проведения конкретного уголовного расследования или судебного разбирательства.

2. Каждая Сторона применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции относительно криминализации;

b) других уголовных преступлений, совершенных с помощью компьютерной системы; и

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

3. a) Каждая Сторона может сохранить за собой право применять меры по сбору данных о трафике в режиме реального времени только к преступлениям или категориям преступлений, указанным в такой оговорке, при условии, что круг таких преступлений или категорий преступлений не является более ограниченным, чем круг преступлений, к которым она применяет меры по перехвату данных о содержании сообщений. Каждая Сторона рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер в отношении сбора данных о трафике в режиме реального времени.

b) В случае когда Сторона ввиду ограничений, которые установлены в ее внутреннем законодательстве, действующем на момент принятия настоящей Конвенции, не имеет возможности применить меры в отношении сбора данных о трафике в режиме реального времени и перехвата данных о содержании сообщений, передаваемых с помощью компьютерной системы поставщика услуг, которая:

i) используется для обслуживания замкнутой группы пользователей; и

ii) не использует сети связи общего пользования и не соединена с другой компьютерной системой, как общего доступа, так и частной,

эта Сторона может сохранить за собой право не применять указанные меры к такой передаче информации. Каждая Сторона рассматривает возможность ограничения такой оговорки для обеспечения возможности наиболее широкого применения мер по сбору данных о трафике в режиме реального времени и по перехвату данных о содержании сообщений.

Условия и гарантии

1. Каждая Сторона обеспечивает, чтобы полномочия и процедуры предусмотренные настоящей статьей, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутреннего права, которые обеспечивают надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств по Международному пакту о гражданских и политических правах и по другим применимым международным

и региональным документам в области прав человека, и которые устанавливают принцип соразмерности.

2. Такие условия и гарантии с учетом характера соответствующих процедур и полномочий включают, в частности, судебный или иной независимый надзор, основания для применения и ограничение сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждая Сторона рассматривает вопрос о воздействии предусмотренных настоящим разделом полномочий и процедур на права, обязанности и законные интересы третьих лиц.

Оперативное обеспечение сохранности хранящихся компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы ее компетентные органы имели возможность посредством дачи распоряжений или иным образом оперативно обеспечивать сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Сторона реализует положения пункта 1 выше посредством распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутренним законодательством.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями о сфере действия процессуальных положений и об условиях и гарантиях, которые содержатся в настоящей Конвенции.

Распоряжение о предоставлении информации

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

a) лицу на ее территории о предоставлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на компьютерном носителе данных; и

b) поставщику услуг, предлагающему свои услуги на территории этой Стороны, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах, которые касаются этих услуг.

2. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями о сфере действия процессуальных положений и об условиях и гарантиях, которые содержатся в настоящей Конвенции.

3. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах, пользующихся его услугами, в форме компьютерных данных или любой другой форме,

кроме данных о трафике или содержании информации, с помощью которой можно установить:

a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;

c) любые другие сведения о месте установки оборудования связи, имеющиеся в соглашении или договоре на обслуживание.

Обыск и выемка хранящихся компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на проведение обыска и или получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на ее территории.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда ее органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на ее территории, и такие данные в законном порядке могут быть получены из первой системы или с ее помощью, компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на эту другую систему.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на выемку или аналогичную защиту компьютерных данных в соответствии с пунктом 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных;

d) обеспечение недоступности этих компьютерных данных в компьютерной системе или их извлечение из нее.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочия на дачу распоряжения любому лица, которому известно о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации, с тем чтобы обеспечить принятие мер, указанных в пунктах 1 и 2.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с положениями о сфере действия процессуальных положений и об условиях и гарантиях, которые содержатся в настоящей Конвенции.

Раздел 2

Юрисдикция

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления юрисдикции в отношении любого преступления, предусмотренного в соответствии с положениями о криминализации, содержащимися в настоящей Конвенции, когда такое преступление совершено:

a) на ее территории; или

b) борту судна под флагом этой Стороны или воздушного судна, зарегистрированного в соответствии с законодательством этой Стороны; или

c) одним из ее граждан, если преступление является уголовно наказуемым по закону государства, в котором оно было совершено, или если преступление совершено за пределами территориальной юрисдикции любого государства.

2. Каждая Сторона может сохранить за собой право не применять или применять только в конкретных случаях или условиях положения о юрисдикции, изложенные в пункте 1 (b)–(d) настоящей статьи или в любой их части.

3. Каждая Сторона принимает такие меры, какие могут потребоваться для установления юрисдикции в отношении преступлений, признанных таковыми в соответствии с положениями о криминализации, содержащимися в настоящей Конвенции, в случаях, когда предполагаемый правонарушитель находится на ее территории и она по получении просьбы о выдаче не выдает его другой Стороне исключительно на основании его гражданства, при условии, что по законодательству обеих заинтересованных Сторон эти преступления подлежат наказанию в виде лишения свободы на максимальный срок не менее одного года или более строгому наказанию.

4. Сторона может также установить свою юрисдикцию в отношении любого преступления, признанного таковым в соответствии с положениями о криминализации, содержащимися в настоящей Конвенции, когда такое преступление совершено:

a) против гражданина этой Стороны;

b) против этой Стороны.

5. Настоящая Конвенция не исключает осуществления Стороной уголовной юрисдикции в соответствии с ее внутренним законодательством.

6. Если несколько Сторон заявляют о своей юрисдикции в отношении предполагаемого преступления, признанного таковым в соответствии с настоящей Конвенцией, заинтересованные Стороны, когда это необходимо, проводят консультации в целях определения наиболее подходящей юрисдикции для уголовного преследования.

Соединенное Королевство Великобритании и Северной Ирландии

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

Глава
Процессуальные меры и правоприменение

Статья 16
Условия и гарантии

1. Каждая Сторона обеспечивает, чтобы полномочия и процедуры, предусмотренные настоящим разделом, устанавливались, осуществлялись и

применялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутреннего права, которые обеспечивают надлежащую защиту прав человека и свобод, включая права, вытекающие из ее обязательств по Международному пакту о гражданских и политических правах и по другим применимым международно-правовым документам в области прав человека, и которые устанавливают принцип соразмерности.

2. Такие условия и гарантии с учетом характера соответствующих процедур или полномочий включают, в частности, судебный или иной независимый надзор, основания для применения и ограничение сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности надлежащему отправлению правосудия, каждая Сторона рассматривает вопрос о воздействии предусмотренных настоящим разделом полномочий и процедур на права, обязательства и законные интересы третьих лиц.

Статья 17
Сфера действия процессуальных положений, включая более широкое использование процессуального права в отношении всех преступлений

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях проведения конкретного уголовного расследования или судебного разбирательства.

2. Если специально не оговорено иное, каждая Сторона применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

b) других уголовных преступлений, совершенных с помощью компьютерной системы; и

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

Статья 18
Оперативное обеспечение сохранности данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы ее компетентные органы имели возможность посредством дачи распоряжений или иным образом оперативно обеспечивать сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Сторона реализует положения пункта 1 выше посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом.

4. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с гарантиями защиты прав человека.

Статья 19
Распоряжение о предоставлении информации

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

a) дать распоряжение лицу на ее территории о предоставлении определенных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на компьютерном носителе данных; и

b) дать распоряжение поставщику услуг, предлагающему свои услуги на территории этой Стороны, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах;

c) полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с гарантиями защиты прав человека.

2. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержании сообщений, с помощью которой можно установить:

a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;

c) любые другие сведения о месте установки оборудования связи, имеющиеся в соглашении или договоре на обслуживание.

Статья 20
Обыск и выемка хранящихся компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на проведение обыска или получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на ее территории.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы, в случае когда ее органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на ее территории, и такие данные в законном порядке могут быть получены из первой системы или с ее помощью, компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на эту другую систему.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочий на выемку или аналогичную защиту компьютерных данных в соответствии с пунктом 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих компьютерных данных;

d) обеспечение недоступности этих компьютерных данных в компьютерной системе или их извлечение из нее.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным органам полномочия на дачу распоряжения любому лицу, которому известно о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации, с тем чтобы обеспечить принятие мер, указанных в пунктах 1 и 2.

5. Полномочия и процедуры, указанные в настоящей статье, устанавливаются в соответствии с гарантиями защиты прав человека.

Объединенная Республика Танзания

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

5. Процессуальные меры

Законы о противодействии киберпреступности устанавливают стандарты допустимого поведения для пользователей информационно-коммуникационных технологий, устанавливают социально-правовые санкции за киберпреступления и защищают пользователей информационно-коммуникационных технологий в целом, а также смягчают и/или предотвращают причинение ущерба людям, данным, системам, услугам и инфраструктуре. Объединенная Республика Танзания предлагает включить в раздел Конвенции, посвященный процессуальным мерам, следующие положения.

Оперативное обеспечение сохранности и раскрытие электронных данных

Конвенция должна содержать положение, согласно которому государства-участники должны включить в свое внутреннее законодательство меры, необходимые для предоставления их компетентным органам полномочия давать распоряжения об оперативном обеспечении сохранности определенных электронных данных, включая данные о трафике, которые хранятся в компьютерной системе, или иным образом добиваться такого обеспечения сохранности. В частности, в случаях, когда имеются основания полагать, что электронные данные подвержены особому риску утраты или изменения.

Если посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся электронных данных, которые находятся во владении или под контролем этого лица, сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо обеспечить сохранность этих электронных данных и их целостность в течение необходимого срока, который необходим компетентным органам для раскрытия этих данных, эта сторона может предусмотреть возможность продления срока действия такого распоряжения.

Конвенция должна содержать положения о принятии государствами-участниками таких законодательных и иных мер, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность

выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

Распоряжение о предоставлении информации

В Конвенции должно быть предусмотрено положение о законодательных и иных мерах, которые могут потребоваться для наделения компетентных органов полномочием на дачу лицу на территории государства-участника распоряжения о предоставлении определенных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на компьютерном носителе данных.

Обыск и выемка хранящихся компьютерных данных

Необходимо, чтобы Конвенция устанавливала обязательства государств-участников по принятию ими законодательных и иных мер, которые могут потребоваться для наделения их компетентных органов полномочием на проведение обыска, получение доступа и выемку компьютерной системы или ее части, хранящихся в ней компьютерных данных и компьютерных данных, которые могут храниться на их территории.

Защита информаторов и свидетелей

Конвенция должна предусматривать обязательство государств-участников по обеспечению защиты информаторов, свидетелей и потерпевших от киберпреступлений, как того могут потребовать обстоятельства дела.

Кроме того, предлагается включить в Конвенцию требование о принятии государствами-участниками надлежащих мер, в пределах их возможностей, которые направлены на обеспечение эффективной защиты от вероятной мести или запугивания в отношении участвующих в уголовном производстве информаторов и свидетелей, дающих показания в связи с преступлениями, охватываемыми Конвенцией, и, в надлежащих случаях, в отношении их родственников и других близких им лиц в соответствии с их внутренним законодательством. Эти меры не должны ущемлять права обвиняемого, включая право на надлежащую правовую процедуру.

6. Правоприменение

Надлежащее противодействие киберпреступности и связанным с ней преступлениям требует применения различных процедур, состоящих из мер предупреждения, выявления и пресечения. Таким образом, эти процедуры, предписанные правоохранительным органам, нуждаются в закреплении. Поэтому Объединенная Республика Танзания считает, что Конвенция должна содержать следующие положения в области правоприменения.

Подготовка кадров, техническая помощь и обмен опытом и знаниями

Для эффективного предупреждения и пресечения использования информационно-коммуникационных технологий в преступных целях необходимо оказывать техническую помощь развивающимся странам и укреплять обмен информацией. Техническая помощь и обмен опытом и знаниями должны быть сосредоточены на следующем:

a) предупреждение и выявление преступлений, охватываемых Конвенцией, и противодействие им;

b) методы, используемые лицами, которые подозреваются в причастности к преступлениям, охватываемым Конвенцией, и соответствующие меры противодействия;

c) наблюдение за перемещением предметов контрабанды;

d) выявление и мониторинг перемещения доходов от преступлений, имущества, оборудования или других средств совершения преступлений и методов, используемых для передачи, сокрытия или утаивания таких доходов, имущества, оборудования или других средств совершения преступлений, а также методов, применяемых в борьбе с киберпреступностью;

e) сбор доказательств;

f) оснащение правоохранительных органов современным оборудованием и техническими средствами, включая использование нового программного обеспечения и агентурных операций;

g) методы, применяемые в борьбе с киберпреступлениями, которые совершаются с использованием компьютеров, телекоммуникационных сетей и других видов современных технологий;

h) планирование и реализация программ исследований и обучения, направленных на обмен опытом в области защиты киберпространства.

Совместные расследования

Киберпреступления по своему характеру не имеют границ и могут затрагивать несколько стран. Конвенция должна предусматривать обязательство государств-участников по заключению договоренностей в отношении дел, которые являются предметом расследования, уголовного преследования или судебного разбирательства в одном или нескольких государствах. Соответствующие компетентные органы могут создавать органы по проведению совместных расследований. Заинтересованным государствам-участникам настоятельно рекомендуется обеспечивать полное уважение суверенитета того государства-участника, на территории которого будет проводиться такое расследование.

Финансовая поддержка

В Конвенции должно содержаться положение, обязывающее развитые государства и учреждения Организации Объединенных Наций оказывать финансовую поддержку развивающимся странам для реализации стратегий по выявлению, предупреждению и пресечению киберпреступности.

Соединенные Штаты Америки

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

Процессуальные меры и правоприменение

Процессуальные положения

Сфера действия процессуальных положений

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях проведения конкретного уголовного расследования или судебного разбирательства.

2. Если в настоящей статье специально не предусмотрено иное, каждое Государство-участник применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении:

a) уголовных преступлений, признанных таковыми в главе о криминализации, содержащейся в настоящей Конвенции;

b) других уголовных преступлений, совершенных с помощью компьютерной системы; и

c) сбора доказательств в электронной форме, касающихся совершения уголовного преступления.

Оперативное обеспечение сохранности хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы его компетентные органы могли посредством дачи распоряжений или иным образом оперативно обеспечить сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся в компьютерной системе, в частности когда имеются основания полагать, что эти компьютерные данные подвержены особому риску утраты или изменения.

2. Если Государство-участник реализует положения пункта 1 выше посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранящихся компьютерных данных, которые находятся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать хранителя компьютерных данных или другое лицо, которому поручено обеспечивать их сохранность, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

Распоряжение о предоставлении информации

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для наделения его компетентных органов полномочием давать распоряжения или иным образом обязать физическое или юридическое лицо на его территории относительно предоставления конкретных компьютерных данных, находящихся во владении или под контролем этого лица и хранящихся в компьютерной системе или на компьютерном носителе информации;

Обыск и выемка хранящихся компьютерных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на проведение обыска или получение аналогичного доступа:

a) к компьютерной системе или ее части и хранящимся в ней компьютерным данным; и

b) носителю компьютерных данных, на котором могут храниться компьютерные данные на его территории.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения того, чтобы в случае, когда его компетентные органы проводят обыск или получают аналогичный доступ к конкретной компьютерной системе или ее части в соответствии с пунктом 1 (a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на его территории, и такие данные в законном порядке доступны в первой системе или с ее помощью, эти компетентные органы имели возможность оперативно распространить обыск или аналогичный доступ на такую другую систему.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на проведение выемки или аналогичную защиту компьютерных данных, к которым получен доступ в соответствии с пунктом 1 или 2. Эти меры включают полномочие:

a) на выемку или аналогичную защиту компьютерной системы или ее части или носителя компьютерных данных;

b) копирование этих компьютерных данных и сохранение копий;

c) обеспечение целостности соответствующих хранящихся компьютерных данных;

d) обеспечение недоступности этих компьютерных данных в компьютерной системе или их извлечение из нее.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочия на дачу распоряжения любому лицу, которое обладает знаниями о функционировании компьютерной системы или мерах, применяемых для защиты содержащихся в ней компьютерных данных, относительно предоставления, в разумных пределах, необходимой информации, с тем чтобы обеспечить принятие мер, указанных в пунктах 1 и 2.

Сбор в режиме реального времени данных о трафике

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

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

i) собирать или записывать с применением технических средств на территории этого Государства-участника; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные о трафике, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью компьютерной системы.

2. Если Государство-участник в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то оно может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике, связанных с конкретными сообщениями, на его территории путем применения технических средств на этой территории.

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

Перехват данных о содержании

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных преступлений, признанных таковыми в соответствии с нормами его внутреннего законодательства, для предоставления его компетентным органам следующих полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника; и

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

i) собирать или записывать с применением технических средств на территории этого Государства-участника; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать данные о содержании в режиме реального времени, которые связаны с конкретными сообщениями на его территории, передаваемыми с помощью компьютерной системы.

2. Если Государство-участник в силу устоявшихся принципов своей внутренней правовой системы не может принять меры, предусмотренные пунктом 1 (a), то оно может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о содержании, связанных с конкретными сообщениями, на его территории путем применения технических средств на этой территории.

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

Юрисдикция[17]

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться для установления юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда такое преступление совершено:

a) на территории этого Государства-участника; или

b) борту судна под флагом этого Государства-участника или на борту воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника на момент совершения этого преступления.

2. При условии соблюдения статьи о суверенитете, содержащейся в настоящей Конвенции, 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 лицом без гражданства, которое обычно проживает на его территории; или

c) преступление является одним из преступлений, признанных таковыми в соответствии со статьей [об отмывании денежных средств] настоящей Конвенции, и совершено за пределами его территории в целях совершения какого-либо преступления, признанного таковым в соответствии со статьей [об отмывании денежных средств] настоящей Конвенции, на его территории; или

d) преступление совершено против этого Государства-участника.

3. Для целей статьи о выдаче настоящей Конвенции каждое Государство-участник принимает такие меры, какие могут потребоваться, 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 исключительно на основании того, что это лицо является его гражданином.

---

[17] Конвенция Организации Объединенных Наций против коррупции, статья 42, и Конвенция Организации Объединенных Наций против транснациональной организованной преступности, статья 15.

4. Каждое Государство-участник принимает также такие меры, какие могут потребоваться для установления его 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 это лицо.

5. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любое другое Государство-участник осуществляет расследование, уголовное преследование или судебное разбирательство в отношении того же деяния, 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 с его внутренним законодательством.

Конфискация и арест[18]

1. Государства-участники принимают, в максимально возможной степени в рамках своих внутренних правовых систем, такие меры, какие могут потребоваться для обеспечения возможности конфискации:

a) доходов от преступлений, охватываемых настоящей Конвенцией, или имущества, стоимость которого соответствует стоимости таких доходов;

b) имущества, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении преступлений, охватываемых настоящей Конвенцией.

2. Государства-участники принимают такие меры, какие могут потребоваться для обеспечения возможности выявления, отслеживания, ареста или выемки любого из перечисленного в пункте 1 настоящей статьи, с целью последующей конфискации.

3. Если доходы от преступлений были превращены или преобразованы, полностью или частично, в другое имущество, то меры, указанные в настоящей статье, применяются в отношении такого имущества.

4. Если такие доходы от преступлений были приобщены к имуществу, приобретенному из законных источников, то конфискации, без ущерба для любых полномочий, касающихся наложения ареста или выемки, подлежит та часть имущества, которая соответствует оцененной стоимости приобщенных доходов от преступлений.

5. К прибыли или другим выгодам, полученным от доходов от преступлений, от имущества, в которое были превращены или преобразованы доходы от преступлений, или от имущества, к которому были приобщены доходы от преступлений, также применяются меры, указанные в настоящей статье, таким же образом и в той же степени, как и в отношении доходов от преступлений.

6. Для целей настоящей статьи и статьи [о международном сотрудничестве в целях конфискации] настоящей Конвенции каждое Государство-участник уполномочивает свои суды или другие компетентные органы выносить постановления о представлении или аресте банковских, финансовых или коммерческих документов. Государство-участник не уклоняется от принятия мер в соответствии с положениями настоящего пункта, ссылаясь на необходимость сохранения банковской тайны.

7. Государства-участники могут рассмотреть возможность установления требования о том, чтобы лицо, совершившее преступление, доказало законное

[18] Конвенция об организованной преступности, статья 12.

происхождение предполагаемых доходов от преступления или другого имущества, подлежащего конфискации, в той мере, в какой такое требование соответствует принципам их внутреннего законодательства и характеру судебного и иного разбирательства.

8. Положения настоящей статьи не толкуются как наносящие ущерб правам добросовестных третьих лиц.

9. Ничто, содержащееся в настоящей статье, не затрагивает принципа, согласно которому меры, о которых в ней говорится, определяются и осуществляются в соответствии с положениями внутреннего законодательства Государства-участника и при условии их соблюдения.

Распоряжение конфискованными доходами от преступлений или имуществом[19]

1. Доходами от преступлений или имуществом, конфискованными Государством-участником на основании статьи о конфискации и аресте и [любой статьи о международном сотрудничестве в целях конфискации] настоящей Конвенции, распоряжается это Государство-участник в соответствии со своим внутренним законодательством и административными процедурами.

2. Действуя по просьбе, направленной другим Государством-участником в соответствии с [любой статьей о международном сотрудничестве в целях конфискации] настоящей Конвенции, Государства-участники в той мере, в какой это допускается внутренним законодательством, и в случае получения соответствующего запроса, в первоочередном порядке рассматривают вопрос о возвращении конфискованных доходов от преступлений или имущества запрашивающему Государству-участнику, с тем чтобы оно могло предоставить компенсацию потерпевшим от преступления или возвратить такие доходы от преступлений или имущество их законным собственникам.

3. Действуя по просьбе, направленной другим Государством-участником в соответствии со статьей о конфискации и аресте или со статьей [о международном сотрудничестве в целях конфискации] настоящей Конвенции, Государство-участник может, принимая во внимание вопрос о компенсации потерпевшим, особо рассмотреть возможность заключения соглашений или договоренностей:

a) о перечислении суммы, соответствующей стоимости доходов от преступлений или имущества, или средств, полученных в результате реализации таких доходов или имущества или их части, на счет, предназначенный для этой цели в соответствии со статьей [о предоставлении технической помощи] настоящей Конвенции, или межправительственным органам, специализирующимся на борьбе против организованной преступности;

b) передаче другим Государствам-участникам на регулярной или разовой основе части доходов от преступлений, или имущества, или средств, полученных в результате реализации таких доходов или имущества, в соответствии со своим внутренним законодательством или административными процедурами.

Сведения о судимости[20]

Каждое Государство-участник может принимать такие законодательные или иные меры, какие могут потребоваться для учета, на таких условиях и в таких целях, какие оно считает надлежащими, любого ранее вынесенного в другом Государстве обвинительного приговора в отношении лица, подозреваемого в совершении расследуемого преступления, для использования такой информации в ходе уголовного производства в связи с преступлением, охватываемым настоящей Конвенцией.

---

[19] Конвенция об организованной преступности, статья 14.

[20] Конвенция об организованной преступности, статья 22.

Защита свидетелей[21]

1. Каждое Государство-участник принимает, в пределах своих возможностей, надлежащие меры, направленные на обеспечение эффективной защиты от вероятной мести или запугивания в отношении участвующих в уголовном производстве свидетелей, которые дают показания в связи с преступлениями, охватываемыми настоящей Конвенцией, и, в надлежащих случаях, в отношении их родственников и других близких им лиц.

2. Меры, предусмотренные в пункте 1 настоящей статьи, без ущерба для прав обвиняемого, в том числе для права на надлежащее разбирательство, могут, в частности, включать:

a) установление процедур для физической защиты таких лиц, например — в той мере, в какой это необходимо и практически осуществимо, — для их переселения в другое место, и принятие таких положений, какие разрешают, в надлежащих случаях, не разглашать информацию, касающуюся личности и местонахождения таких лиц, или устанавливают ограничения на такое разглашение информации;

b) принятие правил доказывания, позволяющих давать свидетельские показания таким образом, который обеспечивает безопасность свидетеля, например разрешение давать свидетельские показания с помощью средств связи, таких как видеосвязь или другие надлежащие средства.

3. Государства-участники рассматривают вопрос о заключении с другими государствами соглашений или договоренностей относительно переселения лиц, указанных в пункте 1 настоящей статьи.

4. Положения настоящей статьи применяются также к потерпевшим постольку, поскольку они являются свидетелями.

Помощь потерпевшим и их защита[22]

1. Каждое Государство-участник принимает, в пределах своих возможностей, надлежащие меры для предоставления помощи и защиты потерпевшим от преступлений, охватываемых настоящей Конвенцией, особенно в случаях угрозы местью или запугивания.

2. Каждое Государство-участник устанавливает надлежащие процедуры для обеспечения доступа к компенсации и возмещению ущерба потерпевшим от преступлений, охватываемых настоящей Конвенцией.

3. 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.

Меры, направленные на расширение сотрудничества с правоохранительными органами[23]

1. Каждое Государство-участник принимает надлежащие меры для того, чтобы поощрять лиц, которые участвуют или участвовали в организованных преступных группах:

a) к предоставлению информации, полезной для компетентных органов, в целях расследования и доказывания в связи с такими вопросами, как:

---

[21] Конвенция об организованной преступности, статья 24, и Конвенция против коррупции, статья 32.

[22] Конвенция об организованной преступности, статья 25.

[23] Конвенция об организованной преступности, статья 26.

i) идентификационные данные, характер, членский состав, структура, местонахождение или деятельность лиц, которые причастны к преступлениям, охватываемым настоящей Конвенцией;

ii) связи, в том числе международные связи, с другими лицами, которые причастны к преступлениям, охватываемым настоящей Конвенцией;

iii) преступления, которые совершили или могут совершить лица, которые причастны к преступлениям, охватываемым настоящей Конвенцией;

b) предоставлению фактической, конкретной помощи компетентным органам, которая может способствовать лишению [лиц, которые причастны к преступлениям, охватываемым настоящей Конвенцией] их ресурсов или доходов от преступлений.

2. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть возможность смягчения, в надлежащих случаях, наказания обвиняемого лица, которое существенным образом сотрудничает в расследовании или уголовном преследовании в связи с каким-либо преступлением, охватываемым настоящей Конвенцией.

3. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть, в соответствии с основополагающими принципами своего внутреннего законодательства, возможность предоставления иммунитета от уголовного преследования лицу, которое существенным образом сотрудничает в расследовании или уголовном преследовании в связи с преступлением, охватываемым настоящей Конвенцией.

4. Защита таких лиц осуществляется в порядке, предусмотренном в статье о защите свидетелей настоящей Конвенции.

5. В тех случаях, когда лицо, которое упоминается в пункте 1 настоящей статьи и находится в одном Государстве-участнике, может существенным образом сотрудничать с компетентными органами другого Государства-участника, заинтересованные Государства-участники могут рассмотреть возможность заключения соглашений или договоренностей, в соответствии со своим внутренним законодательством, относительно возможного предоставления другим Государством-участником режима, указанного в пунктах 2 и 3 настоящей статьи.

Венесуэла (Боливарианская Республика)

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

6. Процессуальные меры и правоприменение

Что касается уголовно-процессуальных мер и правоприменения, в качестве общих положений предлагается установить в будущей конвенции порядок:

- установления механизмов сотрудничества в выявлении доказательств и обмене ими и проведении других этапов расследования;
- определения механизмов установления ответственности негосударственных субъектов и создания нормативно-правовой базы, разграничивающей сферу действия обязательств таких субъектов в процессах, связанных с обеспечением соблюдения национального и международного права;
- установления юрисдикции в отношении использования информационно-коммуникационных технологий для содействия сотрудничеству и без причинения ущерба суверенитету государств в контексте уголовных расследований.

Вьетнам

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

Глава III
Процессуальные меры и правоприменение

8. Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться для установления его юрисдикции в отношении преступлений, указанных в статьях [...], в следующих случаях:

a) когда преступления совершены на любой территории, находящейся под его юрисдикцией, или на борту морского или воздушного судна, зарегистрированного в данном Государстве;

b) когда предполагаемый правонарушитель является гражданином данного Государства;

c) когда потерпевший является гражданином данного Государства и данное Государство считает это целесообразным.

2. Настоящая Конвенция не исключает осуществления Государством уголовной юрисдикции в соответствии с его внутренним законодательством.

9. Полномочия компетентных органов

Государства-участники:

a) принимают меры по предупреждению, выявлению, расследованию, уголовному преследованию и судебному разбирательству в отношении уголовных преступлений, охватываемыми настоящей Конвенцией;

b) собирают доказательства, относящиеся к преступлениям, охватываемым настоящей Конвенцией, включая цифровые данные, не нарушая суверенитета других Государств-участников.