Организация Объединенных Наций A/AC.291/9

Генеральная Ассамблея

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

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

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

Резюме

Настоящий документ подготовлен Председателем Специального комитета при поддержке секретариата в рамках подготовки ко второй сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В него вошли полученные от государств-членов предложения, касающиеся положений о криминализации (A/AC.291/9), общих положений (A/AC.291/9/Add.1) и положений о процессуальных мерах и правоохранительной деятельности (A/AC.291/9/Add.2).

V.22-02325 (R) 190522 270522

Содержание

I. Введение

1. В рамках подготовки ко второй сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и в соответствии с планом и порядком дальнейшей работы Специального комитета, утвержденными на его первой сессии, в частности их пунктами 3 и 4, государствам-членам было предложено представить секретариату для рассмотрения в ходе второй сессии проекты текстов глав или положений, касающихся положений о криминализации (A/AC.291/9), общих положений (A/AC.291/9/Add.1) и положений о процессуальных мерах и правоохранительной деятельности (A/AC.291/9/Add.2).

2. На этой основе Председатель Комитета при поддержке секретариата подготовил настоящий переговорный документ с подборкой полученных от Государств-членов предложений и материалов в отношении конкретных глав, которые будут рассмотрены в ходе второй сессии. Соответственно, содержащиеся в настоящем документе конкретные предложения по формулировкам или общие замечания касаются только глав о криминализации, общих положениях и процессуальных мерах и правоохранительной деятельности и скомпонованы по главам в том виде, в каком они были получены от государств-членов и переведены на шесть официальных языков Организации Объединенных Наций. Если не указано иное, текст сносок представлен в том виде, в каком он был получен от Государств-членов.

3. Как указано выше, настоящий документ не содержит замечаний по другим темам или пояснений в отношении конкретных предложений по формулировкам, которые можно найти в первоначальных материалах, размещенных на вебсайте Специального комитета в полученном виде и в их первоначальной редакции на момент получения.

4. По состоянию на 14 апреля 2022 года в секретариат поступило 24 материала, представляющих мнения 54 Государств-членов и Европейского союза.

II. Криминализация

Ангола

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

- Конвенция должна типизировать и криминализировать наиболее серьезные виды киберпреступлений, особенно когда они затрагивают критическую инфраструктуру, классифицировать их как кибертерроризм или преступления против человечности и определить приоритетные и неотложные правила международного сотрудничества в деле расследования и уголовного преследования субъектов киберпреступлений.
- Конвенция должна типизировать и криминализировать киберпреступные деяния, совершаемые с использованием криптовалют и криптоактивов в целях финансирования терроризма и отмывания денежных средств.

Криминализация

Киберзависимые преступления (преступления против конфиденциальности, целостности и доступности компьютерных систем и данных): незаконный доступ, незаконный перехват, повреждение компьютерных данных, компьютерный саботаж, фальсификация компьютерной информации, незаконное воспроизведение компьютерной программы.

Преступления, совершаемые посредством кибертехнологий (традиционные преступления, совершаемые с использованием информационно-коммуникационных технологий): мошенничество в сети Интернет, фишинг, экономические и финансовые преступления, совершаемые в сети Интернет, кража персональных данных в сети Интернет, сексуальное насилие над детьми и сексуальные посягательства на детей в сети Интернет, кибертравля, киберсталкинг, «порноместь», кибертерроризм.

Толкование понятий, характеризующих эти виды преступлений с точки зрения их юридической квалификации, можно найти в региональных и международных правовых документах, указанных выше[1].

Австралия

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

Криминализация

Новая конвенция дает возможность улучшить международное сотрудничество в отношении киберпреступности и вместе с тем обеспечить согласованность с существующими международными конвенциями по борьбе с преступностью и другими соответствующими документами и избежать их ненужного дублирования. Статьи, касающиеся криминализации, должны соответствовать существующим международным инструментам и исключать возможность возникновения коллизий между такими инструментами. Статьи, касающиеся криминализации, должны быть также надлежащим образом сбалансированы с точки зрения соблюдения принципов верховенства права, прав человека и основных свобод.

Австралия считает, что новая конвенция даст возможность повысить уровень глобальной согласованности подходов к преступлениям, совершаемым в киберпространстве. Это, в свою очередь, позволит уменьшить количество «убежищ» для киберпреступников и расширит возможности правоохранительных органов в борьбе с киберпреступной деятельностью в сети Интернет.

Положения новой конвенции, касающиеся вопросов материального уголовного права, должны быть конкретными и должны содержать четкие определения деяний, лежащих в основе соответствующих преступлений. В конвенции также следует уделить должное внимание основным правонарушениям и дополнительной ответственности за совершение киберзависимых преступлений и преступлений, совершаемых посредством кибертехнологий. Это предполагает стандартное расширение уголовной ответственности, предусмотренной такими документами, как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Организации Объединенных Наций против коррупции.

Киберзависимые преступления

Австралия считает, что новая конвенция должна установить стандарты для криминализации преступлений, нацеленных на компьютерные системы («киберзависимых преступлений»). Австралия предлагает включить в новую конвенцию следующие уголовно наказуемые киберзависимые преступления:

[1] Примечание секретариата: данная ссылка касается документов, указанных в части «Преамбула» материала, представленного Анголой, а именно: «Конвенции Африканского союза о кибербезопасности и защите персональных данных (Малабская конвенция), Конвенции Совета Европы о киберпреступности (Будапештская конвенция), Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Конвенции Организации Объединенных Наций против коррупции».

- незаконный доступ к любой части компьютерной системы (включая компьютерные данные) без правовых оснований;
- незаконный перехват передачи компьютерных данных без правовых оснований;
- незаконное воздействие на компьютерные данные (включая удаление, повреждение, изменение или подавление компьютерных данных) без правовых оснований;
- незаконное воздействие на функционирование компьютерной системы или сети;
- производство, поставка, распространение или получение вредоносных программ в целях совершения другого киберпреступления.

Преступления, совершаемые посредством кибертехнологий

Существующего внутреннего уголовного законодательства почти всех государств достаточно для того, чтобы охватить общеизвестные виды преступлений, в частности, посягательство на имущественные права, вандализм, кражу, преступления, связанные с наркотиками, и другие насильственные преступления.

Конвенция не требует переосмысления этих преступлений лишь по той причине, что для их совершения была задействована компьютерная система или цифровая технология, если только использование компьютерной системы при совершении преступления не меняет характер или серьезность самого преступного деяния.

Вместе с тем, по мнению Австралии, масштабы, размах и легкость совершения некоторых «традиционных» преступлений резко возросли за счет скорости, анонимности и широты охвата, которые обеспечивают информационно-коммуникационные сети. Эти преступления можно охарактеризовать как «преступления, совершаемые посредством кибертехнологий». В Конвенции к этим преступлениям следует подойти взвешенно, установив четкие рамки для определения того, почему определенные составы преступлений изменяются под влиянием «киберэлемента» настолько существенно, что нуждаются в установлении нового согласованного международного стандарта, обособляющего такие деяния от «традиционных» преступлений. Нет необходимости и в установлении в рамках конвенции новых категорий правонарушений для каждого существующего состава преступления, который может включать «киберэлемент», в частности в тех случаях, когда этот элемент не меняет существенным образом тяжесть, масштаб, размах или легкость совершения уголовно наказуемого деяния.

Хотя, по мнению Австралии, подход к включению в конвенцию положений о любых новых категориях преступлений должен быть достаточно сдержанным, Австралия готова выслушать аргументы в пользу того, чтобы действие Конвенции распространялось не только на киберзависимые преступления, но и на «преступления, совершаемые посредством кибертехнологий».

В этом отношении Австралия позитивно восприняла прозвучавшие в ходе первой сессии Специального комитета многочисленные призывы противодействовать той серьезной угрозе, которую представляют собой сексуальная эксплуатация детей и сексуальные надругательства над детьми в сети Интернет. Австралия считает, что по этому вопросу страны могут конструктивно достигнуть консенсуса. Признавая серьезный характер этого вида преступности, Австралия вносит отдельное предложение, касающееся преступлений, связанных с надругательствами над детьми в сети Интернет, включая завлечение детей через сеть Интернет и прямую трансляцию в сети сцен надругательств.

Австралия также рассматривает значительное увеличение числа случаев мошенничества и краж, совершаемых посредством кибертехнологий, включая вымогательство посредством вредоносных программ-вымогателей, в качестве

проблемы, которая получила широкое распространение и по которой государства могут достигнуть консенсуса в части криминализации таких деяний для целей конвенции.

Криминализация преступлений, связанных с надругательствами над детьми в сети Интернет

Статья [A] — Оборот материалов о надругательствах над детьми через компьютерную систему

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно [без законного основания][2]:

a) осуществление доступа к материалам с изображением надругательств над детьми, а также регулирование, передача, распространение, предложение, приобретение, производство или предоставление в пользование таких материалов через компьютерную систему[3], или

b) владение материалами с изображением надругательств над детьми, полученными в результате совершения деяний, указанных в подпункте 1(a).

2. Для целей статьи [A] в понятие «материалы о надругательствах над детьми» включаются материалы, изображающие или описывающие ребенка либо представляющие ребенка, который, как подразумевается или предполагается,участвует в сексуальных действиях, или представляющие в любом виде в присутствии лица, участвующего в сексуальных действиях, половые органы ребенка[4], главным образом в сексуальных целях, или жертвы пыток, жестокого, бесчеловечного или унижающего достоинство обращения или наказания.

Статья [B] — Содействие обороту материалов о надругательствах над детьми через компьютерную систему

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно [без законного основания][5], создание, разработку, изменение, обеспечение функционирования, регулирование, модерирование,

---

[2] Эта оговорка включена для обеспечения того, чтобы положение о составе данного преступления не охватывало непреднамеренно некоторые допускаемые законом ситуации — например, когда необходимость доступа к материалам или производство материалов, которые в ином случае подпадали бы под действие данного положения, может быть обусловлена медицинскими соображениями.

[3] «Компьютерная система» означает любое устройство или группу взаимосвязанных или смежных устройств, среди которых одним или несколькими из них выполняется автоматическая обработка данных в соответствии с заложенной программой. Система может включать устройства для приема, передачи и хранения информации. Она также может включать автономные системы или одну такую систему в составе сети вместе с другими устройствами. Следует отметить, что для обеспечения соответствия с другими положениями настоящего проекта конвенции это понятие (или его определение) может быть изменено.
Самогенерируемый материал может включать как материал, созданный по собственному желанию, так и самогенерируемый материал, созданный по принуждению или вследствие вымогательства. В этом отношении данное положение направлено на обеспечение в целом более осторожного подхода к вопросам криминализации при сохранении в то же время права принятия решений о применении соразмерных и разумных мер реагирования за национальными правовыми системами.

[4] Терминология взята из Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии.

[5] См. сноску 2.

поддержку[6], предоставление в пользование, рекламирование или продвижение компьютерной системы для целей содействия обороту материалов с изображением надругательств над детьми, как они определены в статье [A].

2. Для целей пункта 1 понятие «содействие обороту материалов о надругательствах над детьми» включает любое указанное в пункте 1 деяние, совершаемое в целях предоставления лицам возможности иметь доступ к «материалам о надругательствах над детьми», а также передавать, распространять, предлагать или предоставлять в пользование или производить «материалы о надругательствах над детьми» для себя или для других лиц.

Статья [C] — Завлечение или вербовка ребенка для сексуальных целей через компьютерную систему

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно [через компьютерную систему], завлечение, соблазнение, вербовку или принуждение ребенка с целью склонить его к личной встрече, присутствию при совершении сексуальных действий или участию в таких действиях.

Статья [X] — Общие положения, касающиеся предложенных формулировок

1. Для целей статей [A, B, C] понятие «ребенок» означает любое лицо, не достигшее 18 лет. Кроме того, для целей статьи [C] «ребенок» также означает лицо, которое считается не достигшим 18 лет[7]. Однако для целей статей [A, B, C] Государство-участник может потребовать установления и более низких возрастных пределов, но не ниже 16 лет.

2. Для целей статей [A, B, C] уголовная ответственность распространяется на лиц в возрасте 18 лет и старше. Каждое Государство-участник может в любое время заявить о распространении такой уголовной ответственности также на лиц, не достигших 18 лет. Если Государство-участник делает такое заявление, оно должно обеспечить в своем внутреннем законодательстве надлежащие гарантии для защиты обвиняемого ребенка, учитывая то воздействие, которое может оказать на ребенка процедура отправления уголовного правосудия.

3. Если Государство-участник намерено установить уголовную ответственность для лиц моложе 18 лет на основании статьи [A], оно обязано должным образом учесть необходимость избегать чрезмерной криминализации детей, имеющих самогенерируемый материал, указанный в пункте 2 статьи [A], а также необходимость соблюдения их обязательств согласно Конвенции о правах ребенка и Протоколам к ней.

Сопутствующие наказания

Мы предлагаем включить статью, предусматривающую обязательство государств-участников принять законодательные или другие меры, какие могут потребоваться для обеспечения того, чтобы любые уголовно наказуемые деяния, признанные таковыми согласно настоящей Конвенции, наказывались путем применения эффективных, соразмерных и сдерживающих мер, которые могут включать лишение свободы.

---

[6] В конечном итоге такое деяние, как «поддержка», можно охватить, расширив общие положения об уголовной ответственности. Такая формулировка сохранится до тех пор, пока эти положения не будут рассмотрены.

[7] Формулировка «считается не достигшим» добавлена здесь для того, чтобы охватить ситуации, когда лицо, находящееся под подозрением, или лицо, находящееся под следствием в связи с завлечением или вербовкой детей для сексуальных целей, сотрудничает с представителем правоохранительных органов через сеть Интернет в качестве негласного осведомителя.

Бразилия

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

Глава II
Криминализация

Статья 4
Незаконный доступ[8]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправный доступ ко всей компьютерной системе или к любой ее части. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с намерением завладеть компьютерными данными или с иным бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья 5
Воздействие на данные[9]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порчу, изменение или подавление компьютерных данных. Сторона может оставить за собой право потребовать, чтобы под описанными в этом пункте деяниями подразумевались только те деяния, которые влекут за собой серьезный ущерб.

Статья 6
Воздействие на функционирование системы[10]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Статья 7
Незаконный перехват[11]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно с помощью технических средств, противоправный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

---

[8] *Источник*: Конвенция Совета Европы о киберпреступности (Будапештская конвенция).
[9] *Источник*: Конвенция Совета Европы о киберпреступности.
[10] *Источник*: Конвенция Совета Европы о киберпреступности.
[11] *Источник*: Конвенция Совета Европы о киберпреступности.

Статья 8
Мошенничество с использованием компьютерных технологий[12]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное лишение другого лица его собственности путем:

a) любого ввода, изменения, удаления или подавления компьютерных данных,

b) любого воздействия на функционирование компьютерной системы

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

Статья 9
Незаконный доступ к паролям и учетным данным[13]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное приобретение, присвоение или получение паролей или учетных данных, обеспечивающих доступ к компьютерной системе.

Статья 10
Неправомерное использование устройств[14]

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного прежде всего для целей совершения любого из преступлений, признанных таковыми в соответствии со статьями 4–9;

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части,

с намерением использовать их для совершения любого из преступлений, признанных таковыми в соответствии со статьями 4–9; и

b) владение предметом, указанным в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать его в целях совершения любого из преступлений, признанных таковыми в соответствии со статьями 4–9. Сторона может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми

[12] *Источник*: Конвенция Совета Европы о киберпреступности.
[13] *Источник*: первоначальное предложение Бразилии.
[14] *Источник*: Конвенция Совета Европы о киберпреступности.

в соответствии со статьями 4–9 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может оставить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Статья 11
Подлог с использованием компьютерных технологий[15]

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно, ввод, изменение, удаление или подавление компьютерных данных, влекущие за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Сторона может потребовать, чтобы уголовная ответственность наступала при наличии умысла совершить обман или аналогичного бесчестного умысла.

Статья 12
Преступления, связанные с детской порнографией[16]

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) производство детской порнографической продукции в целях ее распространения через компьютерную систему;

b) предложение или предоставление в пользование детской порнографии через компьютерную систему;

c) распространение или передачу детской порнографии через компьютерную систему;

d) приобретение детской порнографии через компьютерную систему для себя или для другого лица;

e) владение детской порнографией, размещенной в компьютерной системе или на электронно-цифровых носителях данных.

2. Для целей пункта 1 выше в понятие «детская порнография» включаются порнографические материалы, изображающие:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

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

c) реалистические сцены участия несовершеннолетнего лица в откровенных сексуальных действиях.

3. Для целей пункта 2 выше в понятие «несовершеннолетние» включаются любые лица, не достигшие 18 лет. Однако Сторона может потребовать установления и более низких возрастных пределов, но не ниже 16 лет.

[15] *Источник*: Конвенция Совета Европы о киберпреступности.
[16] *Источник*: Конвенция Совета Европы о киберпреступности.

4. Каждая Сторона может оставить за собой право не применять, полностью или частично, положения подпунктов (d) и (e), пункта 1 и подпунктов (b) и (c) пункта 2.

Статья 13
Склонение к самоубийству или доведение до его совершения[17]

Каждая Сторона принимает такие законодательные и другие меры, которые необходимы для признания в качестве преступления согласно ее внутреннему законодательству склонения к самоубийству или доведения до его совершения, в том числе несовершеннолетних, совершенных посредством оказания психологического или иных видов воздействия в информационно-телекоммуникационных сетях, включая сеть Интернет.

Статья 14
Нарушение авторских и смежных прав с использованием информационно-коммуникационных технологий[18]

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству нарушения авторских и смежных прав, как они определены в законодательстве этого Государства-участника, когда такие деяния совершаются умышленно с использованием информационно-коммуникационных технологий, включая незаконное использование программ для компьютерных систем или баз данных, являющихся объектами авторского права, и присвоение авторства.

Статья 15
Покушение и пособничество или подстрекательство[19]

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, пособничество совершению любого из преступлений, признанных таковыми в соответствии с главой II настоящей Конвенции, или подстрекательство к его совершению.

2. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, покушение на совершение какого-либо из преступлений, признанных таковыми в соответствии с главой II настоящей Конвенции.

3. Каждая Сторона может оставить за собой право не применять, полностью или частично, положения пункта 2 настоящей статьи.

Статья 16
Корпоративная ответственность[20]

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться для обеспечения возможности привлечения юридического лица к ответственности за уголовное преступление, признанное таковым в соответствии с настоящей Конвенцией, если это преступление совершено в его пользу любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в этом юридическом лице руководящую должность на основании:

---

[17] *Источник*: предложение Китая и Российской Федерации.
[18] *Источник*: предложение Китая и Российской Федерации.
[19] *Источник*: Конвенция Совета Европы о киберпреступности с изменениями, внесенными Бразилией.
[20] *Источник*: Конвенция Совета Европы о киберпреступности.

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, уже предусмотренным в пункте 1 настоящей статьи, каждая Сторона принимает меры, необходимые для обеспечения возможности возложения на юридическое лицо ответственности в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение уголовного преступления, признанного таковым в соответствии с настоящей Конвенцией, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от правовых принципов Сторон ответственность юридического лица может быть уголовной, гражданско-правовой или административной.

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

Статья 17
Санкции и меры[21]

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться для обеспечения того, чтобы в случае совершения уголовных преступлений, признанных таковыми в соответствии с главой II настоящей Конвенции, применялись эффективные, соразмерные и оказывающие сдерживающее воздействие санкции, включая лишение свободы.

2. Каждая Сторона обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии со статьей 16, эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций или мер, включая денежные санкции.

Бурунди

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

Глава II. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Раздел 1
Деяния, направленные против конфиденциальности компьютерных систем

Раздел 2
Незаконный доступ

Государства — участники настоящей Конвенции признают согласно их внутреннему законодательству в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправный доступ ко всей компьютерной системе или к любой ее части.

Раздел 3
Воздействие на компьютерную систему

Государства — участники настоящей Конвенции признают согласно их внутреннему законодательству в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порча, изменение или подавление компьютерных данных.

[21] *Источник*: Конвенция Совета Европы о киберпреступности.

Раздел 4
Воздействие на данные

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Раздел 5
Незаконные производство, продажа, приобретение, использование, импорт, распространение компьютерных систем или владение ими и склонение к самоубийству

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых деяний производство, продажу, приобретение, использование, импорт, распространение компьютерного устройства или компьютерной системы или владение ими или обеспечение доступа к данным, программам или компьютерным системам с намерением их использовать или предоставить в пользование другому лицу в целях совершения преступлений.

Раздел 6
Мошенничество с использованием компьютерных технологий

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное причинение имущественного ущерба другому лицу путем: a) введения, изменения, удаления или подавления компьютерных данных или b) любого воздействия на функционирование компьютерной системы с мошенническим или преступным умыслом извлечения неправомерной экономической выгоды для себя или для другого лица.

§1. Мошенничество с использованием компьютерных систем

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых мошеннические деяния, совершаемые с использованием средств электронной коммуникации в целях присвоения или получения либо совершения попытки присвоения или получения денежных средств, движимого имущества, облигаций, депозитов, ценных бумаг, залоговых обязательств, приходных квитанций, документов о погашении обязательств или всего имущества другого лица или части этого имущества.

§2. Кража цифровых персональных данных

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния присвоение цифровых персональных данных другого лица или использование отдельных или нескольких данных любого характера, позволяющих идентифицировать это лицо, в целях нарушения его спокойствия или покушения на его репутацию, частную жизнь или имущество или на репутацию, честь, частную жизнь или имущество третьей стороны для извлечения выгоды или введения в заблуждение других лиц.

§3. Фишинг

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния использование веб-сайта или отправку с помощью компьютерной системы электронного сообщения с намерением получить конфиденциальную информацию от посетителя сайта или адресата сообщения для ее использования в преступных целях.

§4. Злоупотребление доверием в отношении компьютерных данных

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния присвоение или передачу другим лицам компьютерных данных, вверенных лицу на условиях их возврата или использования в конкретных целях.

§5. Неправомерное получение компьютерных данных

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния владение в любом качестве компьютерными данными, полученными в результате совершения преступления, когда известно, каким образом эти данные были получены.

§ 6. Вымогательство компьютерных данных

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния любую попытку завладеть компьютерными данными посредством применения силы, насилия или принуждения.

§7. Шантаж и публикация слухов

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых деяний использование письменных или устных угроз, разглашение или предъявление бездоказательно порочащих обвинений или вымогательство или попытки вымогательства компьютерных данных.

§ 8. Рассылка спама

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых следующие деяния:

1. рассылку незапрашиваемых сообщений многократно или большому количеству лиц с использованием компьютерного устройства или компьютерной системы;

2. использование компьютерного устройства или компьютерной системы после получения сообщения для пересылки этого сообщения большому количеству лиц или для его многократной пересылки лицу, которое в нем не нуждается.

Раздел 7
Преступления, связанные с содержанием данных

§1. Преступления, связанные с детской порнографией

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно: производство детской порнографической продукции в целях ее распространения через компьютерную систему; предложение или предоставление в пользование детской порнографии через соответствующую систему.

Раздел 8
Распространение через компьютерную систему письменных и визуальных материалов расистского или ксенофобского характера

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых деяний создание, скачивание, распространение или предоставление в пользование в каком-либо виде, будь то в виде текстов, сообщений, фотографий, рисунков, видеозаписей или в любом другом виде, материалов, отражающих идеи или теории

расистского или ксенофобского характера, с использованием для этих целей компьютерной системы.

Раздел 9
Нанесение оскорбления с использованием компьютерной системы

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния нанесение оскорбления лицу по причине его принадлежности к группе, отличительным признаком которой является раса, цвет кожи, родовое происхождение, национальная или этническая принадлежность или религия, если предлогом для такого деяния служит любой из указанных факторов, или нанесение оскорбления группе лиц, отличающихся по одному из вышеперечисленных признаков.

Раздел 10
Преступления, связанные с использованием компьютерного устройства или компьютерной системы для осуществления террористической деятельности, изготовления оружия или торговли людьми или незаконного оборота наркотиков

§1. Создание или публикация веб-сайтов для террористических групп

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемых деяний:

1. создание, публикацию или использование веб-сайта террористической группы с помощью сети Интернет, компьютерного устройства или компьютерной системы для содействия коммуникации ее руководителей или ее членов;

2. сбор средств или распространение ее идей или сведений о том, каким образом она осуществляет свою террористическую деятельность.

§2. Распространение информации о способах или средствах уничтожения

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния распространение или предоставление посредством компьютерной системы в пользование другому лицу, за исключением лиц, имеющих соответствующее разрешение, инструкций или методических пособий, позволяющих изготавливать такое огнестрельное оружие, такие его части, компоненты и боеприпасы к нему, которые могут причинить ущерб жизни человека, имуществу или окружающей среде.

§3. Создание или публикация веб-сайта для целей торговли людьми

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния создание или публикацию с помощью информационной сети, компьютерного оборудования или компьютерной системы веб-сайта, предназначенного для осуществления торговли людьми или содействия совершению подобных действий.

§4. Создание или публикация веб-сайта для целей незаконного оборота или распространения психоактивных средств или наркотиков

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния создание или публикацию с помощью информационной сети, компьютерного оборудования или компьютерной системы веб-сайта, предназначенного для незаконного оборота или распространения психоактивных средств или наркотиков или содействия совершению подобных действий.

Раздел 11
Преступное сообщество лиц, использующих компьютерные технологии

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния преднамеренное участие в сформированном сообществе или сговоре в целях приготовления или совершения одного или нескольких преступлений.

Раздел 12
Преступления, связанные с нарушением прав интеллектуальной собственности и смежных прав

Государства — участники настоящей Конвенции признают без ущерба для своего внутреннего законодательства в качестве уголовно наказуемого деяния любое нарушение прав интеллектуальной собственности.

Глава III. Ответственность юридических лиц

Государства — участники настоящей Конвенции принимают такие положения, которые необходимы для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией.

Принять необходимые меры для обеспечения возможности привлечения к ответственности юридического лица в случае отсутствия надзора или контроля со стороны работающего в нем физического лица. Ответственность юридического лица может быть уголовной, гражданско-правовой или административной.

Канада

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

Преступления

Незаконный доступ к компьютерной системе

Признать в качестве уголовно наказуемого деяния, когда оно совершается с мошенническими целями, противоправный доступ ко всей компьютерной системе или к любой ее части.

Незаконный перехват передачи не предназначенных для общего пользования данных компьютерной системы

Признать в качестве уголовно наказуемого деяния, когда оно совершается с мошенническими целями, противоправный перехват с помощью любых технических средств не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие данные.

Воздействие на компьютерные данные

Признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порчу, изменение или подавление компьютерных данных.

Воздействие на функционирование компьютерной системы

Признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное создание серьезных препятствий для функционирования компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Неправомерное использование устройств

1. Признать в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) производство, продажу, приобретение для использования, импорт, распространение или иную форму предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного главным образом для совершения любого из киберпреступлений, включенных в настоящую Конвенцию,

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей *компьютерной системе* или к любой ее части, с намерением использовать их для совершения любого из киберпреступлений, включенных в настоящую Конвенцию; и

b) владение предметом, указанным в подпункте (i) или (ii) пункта 1 (a), с намерением использовать его в целях совершения любого из киберпреступлений, включенных в настоящую Конвенцию.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1, не преследуют цель совершения киберпреступления, включенного в настоящую Конвенцию, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

Преступления, связанные с сексуальной эксплуатацией детей

1. Признать в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) производство материалов с изображением сексуальной эксплуатации детей в целях их распространения через компьютерную систему;

b) предложение, рекламу или предоставление в пользование материалов с изображением сексуальной эксплуатации детей через компьютерную систему;

c) распространение или передачу материалов с изображением сексуальной эксплуатации детей через компьютерную систему;

d) приобретение через компьютерную систему материалов с изображением сексуальной эксплуатации детей для себя или для другого лица;

e) обеспечение доступа к материалам с изображением сексуальной эксплуатации детей или владение такими материалами, размещенными в компьютерной системе или на компьютерном носителе данных.

2. Для целей пункта 1 в понятие «материалы с изображением сексуальной эксплуатации детей» включается детская порнография, как она определена в Факультативном протоколе к Конвенции о правах ребенка, касающемся торговли детьми, детской проституции и детской порнографии, и любые:

a) визуальные материалы, включая фото, видео материалы и прямую трансляцию в сети Интернет, показывающие:

i) ребенка, участвующего в сексуальных действиях или присутствующего при совершении таких действий;

ii) лицо, кажущееся ребенком, участвующее в сексуальных действиях или присутствующее при совершении таких действий;

iii) реалистические изображения участия ребенка в сексуальных действиях или его присутствия при совершении таких действий;

b) письменные материалы, которые:

i) пропагандируют сексуальные действия с ребенком;

ii) написаны с сексуальной целью и имеют в качестве основной характеристики описание сексуальных действий с ребенком; и

c) аудиозаписи, которые:

i) пропагандируют сексуальные действия с ребенком;

ii) произведены с сексуальной целью и имеют в качестве основной характеристики описание сексуальных действий с ребенком.

Завлечение и соблазнение ребенка

1. Признать в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) передачу, распространение, продажу или предоставление в пользование через компьютерную систему материалов откровенно сексуального характера ребенку или лицу, кажущемуся ребенком;

b) общение с ребенком или лицом, кажущимся ребенком, через компьютерную систему; или

c) получение соответствующего согласия от ребенка или лица, кажущегося ребенком, или вступление с ребенком или лицом, кажущимся ребенком, в соответствующие договоренности через компьютерную систему

в целях содействия совершению любых связанных с сексуальной эксплуатацией детей преступлений, признанных таковыми согласно настоящей Конвенции, Факультативному протоколу к Конвенции о правах ребенка, касающемуся торговли детьми, детской проституции и детской порнографии, или внутреннему законодательству Государства-участника.

2. Лицо не подлежит уголовной ответственности, если им были предприняты разумные шаги для того, чтобы убедиться, что соответствующее лицо не является ребенком.

Распространение интимных изображений без согласия («порноместь»)

1. Признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно, опубликование, распространение, передачу, продажу, предоставление в пользование или рекламирование интимного изображения человека с помощью любых средств компьютерной системы, когда известно, что человек, запечатленный на изображении, не давал своего согласия на совершение таких действий, или невзирая на наличие или отсутствие согласия этого человека на совершение таких действий.

2. Для целей пункта 1 интимное изображение означает визуальную запись человека, произведенную любым способом, включая фотографическую, кино- или видеозапись:

a) на которой человек обнажен, показывает свои половые органы, анальную область или грудь, или совершает откровенные сексуальные действия;

b) в связи с которой в момент записи имелись обстоятельства, дававшие разумные основания ожидать, что она останется конфиденциальной; и

c) в связи с которой у изображенного человека сохранялись в момент совершения преступления разумные основания ожидать, что она останется конфиденциальной.

3. Уголовная ответственность не предусмотрена в случае, если распространение интимных изображений без согласия осуществляется для общественного блага или имеет законную цель.

Колумбия

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

3. Криминализация

В отношении киберзависимых преступлений каждое Государство-член должно принять такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать уголовно наказуемыми в рамках своей внутренней правовой системы следующие деяния:

a) незаконный доступ: неправомерный доступ ко всей компьютерной системе или к любой ее части[22];

b) незаконный перехват: неправомерный перехват компьютерных данных при их создании или поступлении адресату или внутри информационной системы, либо в процессе электромагнитных излучений компьютерной системы, несущей такие компьютерные данные[23];

c) воздействие на данные: повреждение, уничтожение, удаление, порча, изменение или подавление компьютерных данных или системы обработки информации или ее логических элементов или частей[24];

d) воздействие на систему: неправомерное создание препятствий функционированию компьютерной системы или нормальному доступу к такой системе, к содержащимся в ней данным или к телекоммуникационной сети[25];

e) неправомерное использование устройств: производство и приобретение устройства, включая компьютерную программу, а также компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части, и владение ими или их распространение или продажу в целях совершения любого из преступлений, указанных в пунктах (a), (b), (c) и (d) настоящей статьи[26];

f) подлог с использованием компьютерных технологий: умышленное противоправное введение, изменение, удаление или подавление компьютерных данных, влекущее за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных[27].

---

[22] Статья 2 Будапештской конвенции о киберпреступности. Соответствует статье 269A Закона № 1273 от 2009 года

[23] Статья 3 Будапештской конвенции о киберпреступности. Соответствует статье 269C Закона № 1273 от 2009 года.

[24] Статья 4 Будапештской конвенции о киберпреступности. Соответствует статье 269D Закона № 1273 от 2009 года.

[25] Статья 5 Будапештской конвенции о киберпреступности. Соответствует статье 269B Закона № 1273 от 2009 года.

[26] Статья 6 Будапештской конвенции о киберпреступности.

[27] Статья 7 Будапештской конвенции о киберпреступности.

В отношении преступлений, совершаемых посредством кибертехнологий, каждое Государство-член должно принять такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать уголовно наказуемыми в рамках своей внутренней правовой системы следующие деяния:

a) преступления, связанные с материалами о сексуальном насилии над детьми: производство, предложение, распространение, передача или приобретение материалов о сексуальном насилии над детьми или владение такими материалами, размещенными в компьютерной системе[28];

b) мошенничество с использованием компьютерных технологий: введение, изменение, удаление или подавление компьютерных данных или воздействие на функционирование компьютерной системы с мошенническим или преступным умыслом неправомерного извлечения экономической выгоды для себя или для другого лица в ущерб имущественному положению другого лица[29];

c) нарушение конфиденциальности персональных данных: несанкционированные получение, компиляция, изъятие, предложение, продажа, обмен, отправка, покупка, перехват, раскрытие, изменение или использование персональных данных, содержащихся в файлах, архивах, базах данных или на аналогичных носителях информации, в целях извлечения выгоды для себя или для третьей стороны[30];

физических лиц и денежные санкции в случае юридических лиц[31].

Египет

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

Глава II
Криминализация, уголовное судопроизводство и правоохранительная деятельность

Статья 5
Криминализация

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для предупреждения и выявления преступлений, предусмотренных настоящей Конвенцией, или любых других преступлений, совершаемых с использованием информационно-коммуникационных технологий, включая блокирование и удаление контента, связанного с такими преступлениями, преследование лиц, совершивших такие преступления, выдачу преступников, содействие процедурам международного сотрудничества и сбор доказательств в отношении таких преступлений, подтверждая при этом важность принципа технологической нейтральности.

2. Каждое Государство-участник принимает также такие законодательные и другие меры, которые необходимы для введения уголовной ответственности за совершение следующих деяний:

[28] Статья 9 Будапештской конвенции о киберпреступности.
[29] Статья 8 Будапештской конвенции о киберпреступности.
[30] Статья 269F, Закон № 1773 от 2009 года.
[31] Статья 13 Будапештской конвенции о киберпреступности. Соответствует статье 30 Конвенции Организации Объединенных Наций против коррупции и статье 11 Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

Статья 6
Неправомерное использование или содействие неправомерному использованию информационно-коммуникационных услуг и технологий

Незаконное использование или содействие другим лицам в использовании услуг связи или каналов аудио- или видеовещания с помощью информационной сети или информационно-коммуникационных технологий.

Статья 7
Неправомерный доступ и/или превышение права доступа

1. Превышение лицом временных ограничений или ограничений уровня доступа в рамках предоставленного ему права на доступ к веб-сайту, личной учетной записи или информационной системе.

2. Неправомерный доступ ко всей информационно-технологической системе или ее части, присутствие во всей системе или ее части или связь со всей системой или ее частью, или продолжение такого доступа, присутствия и связи.

3. Строгость наказания повышается, если такой доступ, присутствие, связь или их продолжение приводит к:

a) стиранию, изменению, искажению, копированию, передаче или уничтожению сохраненных данных, электронных устройств и систем или сетей связи либо наносят ущерб пользователям и бенефициарам;

b) получению конфиденциальной государственной информации.

Статья 8
Атака на сайт

Неправомерное повреждение, нарушение, замедление работы, искажение, сокрытие или изменение сайта компании, учреждения, организации или физического лица.

Статья 9
Неправомерный перехват

Умышленный и неправомерный перехват потока данных любыми техническими средствами или посредством прерывания передачи или приема данных информационных технологий.

Статья 10
Нарушение целостности данных

Умышленное и неправомерное уничтожение, стирание, создание препятствий для передачи, изменение или блокирование данных информационных технологий.

Статья 11
Неправомерное использование информационных технологий

Производство, продажа, покупка, импорт, распространение, предоставление любых разработанных или адаптированных инструментов или программного обеспечения, пароля или аналогичной информации, с помощью которых можно получить доступ к информационной системе, или владение ими с намерением использовать эту информационную систему для совершения преступления, предусмотренного настоящей Конвенцией, или создание вредоносного программного обеспечения, предназначенного для уничтожения, блокирования, изменения, копирования или распространения цифровой информации или нейтрализации средств защиты цифровой информации, за исключением законно проводимых исследований.

Статья 12
Фальсификация

Использование информационных технологий для изменения содержания данных с намерением использовать их в качестве достоверных данных для нанесения вреда.

Статья 13
Мошенничество

Умышленное и неправомерное причинение ущерба бенефициарам и пользователям с целью мошенничества для реализации интересов правонарушителя или других лиц и получения ими выгод незаконным способом, в том числе посредством мошеннических электронных преступлений, связанных с виртуальной валютой (цифровой валютой или криптовалютой).

Статья 14
Угрозы и шантаж

Использование информационно-коммуникационных технологий или любых других технических средств для запугивания или шантажирования какого-либо лица с целью принуждения его к совершению или отказу от совершения какого-либо действия.

Статья 15
Порнография

1. Изготовление, показ, распространение, предоставление, опубликование, покупка, продажа или импорт порнографических материалов с целью проституции или эксплуатации женщин или несовершеннолетних с использованием информационно-коммуникационных технологий, в соответствии с внутренним законодательством каждого государства.

2. Изготовление, показ, распространение, предоставление, опубликование, покупка, продажа или импорт порнографических материалов с изображением детей или несовершеннолетних, включая хранение материалов с изображением детей или несовершеннолетних, которые считаются непристойными, на информационно-коммуникационных технических средствах или носителях информационно-коммуникационных технологий.

Статья 16
Другие преступления, связанные с порнографией

Сексуальная эксплуатация или домогательства, в особенности в отношении женщин, детей или несовершеннолетних.

Статья 17
Побуждение или принуждение к совершению самоубийства

Побуждение или принуждение к совершению самоубийства, в том числе несовершеннолетних, посредством психологического или иного давления через информационно-коммуникационные сети, включая сеть Интернет, как в процессе прямого взаимодействия, так и с помощью современных технологий или электронных игр.

Статья 18
Вовлечение несовершеннолетних в совершение противоправных деяний

Вовлечение несовершеннолетних с помощью информационно-коммуникационных технологий в совершение противоправных деяний, которые ставят под угрозу их жизнь, физическое или психическое здоровье.

Статья 19
Нарушение неприкосновенности частной жизни

Нарушение неприкосновенности частной жизни с помощью информационно-коммуникационных технологий, включая создание электронной почты, веб-сайта или личной учетной записи и ложное присвоение их физическому или юридическому лицу.

Статья 20
Преступления террористической направленности, совершенные с использованием информационных технологий

1. Распространение, пропаганда или оправдание идей и принципов террористических групп.

2. Финансирование террористических актов или обучение их проведению, содействие коммуникации между террористическими организациями или оказание материально-технической поддержки исполнителям террористических актов.

3. Распространение информации о методах изготовления взрывных устройств, используемых, в частности, в террористических актах.

4. Распространение вражды, смуты, ненависти или расизма.

5. Государства принимают необходимые меры для предотвращения распространения такого контента с помощью информационно-коммуникационных технологий, включая блокирование или удаление контента, имеющего отношение к этим преступлениям.

Статья 21
Финансовые преступления, включая отмывание денежных средств

1. Использование информационно-коммуникационных технологий для совершения финансовых преступлений или неправомерное использование виртуальной валюты (цифровой валюты и криптовалюты).

2. Проведение операций по отмыванию денежных средств, обращение за помощью для проведения операций по отмыванию денежных средств или публикация информации о методах отмывания денежных средств.

Статья 22
Незаконное использование электронных средств платежа

1. Подделка, изготовление или установка любого устройства или материалов, позволяющих подделывать или имитировать любое электронное средство платежа любым способом.

2. Присвоение, использование или предоставление другим лицам данных любого средства платежа или содействие получению таких данных другими лицами.

3. Использование информационной сети или информационных технологий для получения несанкционированного доступа к номерам или данным любого средства платежа.

4. Сознательное принятие поддельного средства платежа.

Статья 23
Совершенные с использованием информационных технологий преступления, имеющие отношение к организованной или транснациональной преступности

1. Пропаганда или незаконный оборот наркотических средств или психотропных веществ.

2. Незаконное распространение фальсифицированных лекарственных средств или медицинских изделий.

3. Незаконный ввоз мигрантов.

4. Незаконная торговля людьми и человеческими органами.

5. Незаконная торговля оружием.

6. Незаконный оборот культурных ценностей.

Статья 24
Преступления, связанные с нарушением авторских и смежных прав

Нарушение авторских или смежных прав в соответствии с определением, действующим в законодательстве Государства-участника, если такое нарушение совершено умышленно.

Статья 25
Несанкционированный доступ к критической информационной инфраструктуре

1. Создание, распространение или использование программного обеспечения либо иной цифровой информации, предназначенных для предоставления несанкционированного доступа к критической информационной инфраструктуре, в том числе для уничтожения, блокирования, изменения, копирования информации, содержащейся в ней, или нейтрализации средств защиты.

2. Нарушение правил использования носителей, предназначенных для хранения, обработки или передачи защищенной цифровой информации, содержащейся в критической информационной инфраструктуре или информационных системах в соответствии с внутренним законодательством Государства-участника, информационно-коммуникационных сетей, относящихся к критической информационной инфраструктуре, или средств доступа к ним, если такое нарушение наносит ущерб критической информационной инфраструктуре.

Статья 26
Подстрекательство к подрывной или вооруженной деятельности или другим уголовным преступлениям

Передаваемые с помощью информационно-коммуникационных технологий призывы, пропагандирующие саботаж или вооруженные действия, направленные против режима другого государства, которые могут подорвать общественную безопасность и стабильность; или призывы к совершению уголовных преступлений, за которые предусмотрено наказание в виде лишения свободы сроком не менее одного года.

Статья 27
Преступления экстремистской направленности

Распространение с помощью информационно-коммуникационных технологий материалов, призывающих к совершению незаконных действий по политическим, идеологическим, социальным или этническим мотивам, или любых других незаконных действий, пропагандирующих этническую или религиозную ненависть или вражду в целом, а также их пропаганда, оправдание или предоставление доступа к ним.

Статья 28
Покушение на совершение преступления или участие в совершении преступления

Совершение или покушение на совершение уголовного преступления, предусмотренного Конвенцией, и/или участие в качестве сообщника в уголовном преступлении, предусмотренном Конвенцией, и/или организация

уголовного преступления или руководство другими лицами для совершения уголовного преступления, предусмотренного Конвенцией.

Статья 29
Иные незаконные деяния

Настоящая Конвенция не препятствует Государству-участнику вводить уголовную ответственность за любое другое незаконное деяние, умышленно совершенное с использованием информационно-коммуникационных технологий.

Статья 30
Ответственность юридических лиц

1. Каждое Государство-участник обязуется, в соответствии со своим внутренним законодательством, установить уголовную ответственность юридических лиц за преступления, совершенные их представителями от их имени или в их интересах, что не должно исключать вынесения наказаний физическим лицам, совершившим данное преступление, включая администраторов сайтов.

2. Без ущерба для положений настоящей Конвенции поставщики услуг/администраторы сайтов и их подчиненные выполняют следующие требования, нарушение которых влечет за собой уголовную ответственность:

a) сохранение и хранение в журнале информационной системы или журнале информационной технологии в течение (срок предстоит определить) следующих данных:

- данных, позволяющих идентифицировать пользователей услуг,
- данных, относящихся к контенту, обрабатываемому в информационных системах, когда такие данные находятся под контролем поставщика услуг,
- данных о трафике связи,
- данных о периферийных устройствах связи,
- любых других данных, определенных государством для целей осуществления Конвенции;

b) соблюдение конфиденциальности сохраненных и хранимых данных, включая личные данные любого пользователя услуг либо любые данные или информацию о сайтах, которые посещались такими пользователями, или о личных учетных записях, которыми они пользовались, либо о лицах или субъектах, с которыми эти пользователи осуществляют связь, а также отказ от разглашения этих данных без обоснованного распоряжения компетентного органа;

c) обеспечение защиты данных и информации с соблюдением их конфиденциальности и недопущением их взлома и повреждения;

d) предоставление легкого, прямого и постоянного доступа к следующим данным и информации для пользователей своих услуг и любого компетентного органа:

- название и адрес поставщика услуг,
- контактная информация поставщика услуг, включая адрес электронной почты,
- данные лицензии, идентифицирующие поставщика услуг и компетентный орган, осуществляющий надзор за его деятельностью;

e) предоставление по запросу компетентных органов, определенных государством, всех технических средств, необходимых для того, чтобы эти органы могли осуществлять свои полномочия.

Сальвадор

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

Положения о криминализации

Государствам следует принять соответствующие законодательные и иные меры, с тем чтобы признать уголовными преступлениями по своему национальному законодательству — с применением уголовных и иных санкций, включая тюремное заключение, учитывающих число жертв и размер причиненного ущерба, — следующие деяния:

Незаконный доступ

Доступ ко всей или любой части компьютерной системы без надлежащего разрешения, когда он совершается умышленно. Это положение не применяется к санкционированным испытаниям или следственным действиям, которые являются законными и поддаются проверке, при условии, что они не наносят серьезного косвенного ущерба.

Неправомерный перехват

Осуществленный без надлежащего разрешения с помощью технических средств перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные, когда он совершается умышленно и неправомерно.

Воздействие на данные

Повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без надлежащего разрешения, когда они совершаются умышленно и неправомерно.

Воздействие на функционирование компьютерных систем

Создание серьезных препятствий для функционирования компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных, когда оно совершается умышленно и неправомерно.

Неправомерное использование устройств

Производство, продажа, приобретение для использования, импорт, распространение или предоставление в пользование — когда они совершаются умышленно и неправомерно — любого устройства, включая компьютерные программы, разработанного или приспособленного главным образом для целей совершения любого из правонарушений, предусмотренных настоящей Конвенцией; либо паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или ее части для целей совершения любого из правонарушений, предусмотренных настоящей Конвенцией. Это положение не применяется к санкционированным испытаниям или следственным действиям, которые являются законными и поддаются проверке, при условии, что они не наносят серьезного косвенного ущерба.

Подлог с использованием компьютерных технологий

Внесение, изменение, удаление или блокирование компьютерных данных, приводящее к появлению неаутентичных данных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными, когда оно совершается умышленно и неправомерно. В качестве условия наступления уголовной ответственности может требоваться наличие намерения совершить обман или аналогичного бесчестного намерения.

Мошенничество, совершенное с использованием информационно-коммуникационных технологий

Действия, причиняющие ущерб имуществу другого лица путем любого ввода, изменения, удаления или блокирования компьютерных данных или любого вмешательства в функционирование компьютерной системы с намерением совершить мошенничество или обман в целях извлечения экономической выгоды для себя или другого лица, когда они совершаются умышленно и неправомерно.

Преступления, связанные с материалами, содержащими надругательства над детьми

Такие деяния, как производство, воспроизведение, распространение, публикация, импорт, экспорт, предложение, финансирование, продажа, маркетинг, распространение или хранение таких материалов на любом типе технического устройства или носителя, когда они совершаются умышленно и неправомерно.

Нарушение прав интеллектуальной собственности и смежных прав

Нарушение прав интеллектуальной собственности и смежных прав, определенных в законодательстве Государства-участника, когда такие действия являются умышленными и совершаются с использованием информационно-коммуникационных технологий, включая незаконное использование компьютерных программ и баз данных, защищенных авторским правом, и плагиат.

Пособничество или подстрекательство и покушение на совершение преступления

Участие в преступлении в качестве сообщника, пособника или подстрекателя или в любой другой роли; любая попытка совершить преступление или приготовление к преступлению, признанному таковым в соответствии с настоящей Конвенцией.

Ответственность

Каждое Государство-участник принимает такие меры, которые могут потребоваться в соответствии с его правовыми принципами, для установления ответственности юридических лиц за участие в преступлениях, признанных таковыми в настоящей Конвенции, если такие преступления совершаются в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа юридического лица, занимающего в нем руководящую должность на основании: полномочий представлять данное юридическое лицо; права принимать решения от имени этого юридического лица или права осуществлять контроль внутри этого юридического лица.

В дополнение к случаям, предусмотренным предыдущим пунктом, каждое Государство-участник принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в предыдущем пункте, делает возможным совершение правонарушения, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

В зависимости от правовых принципов Государства-участника такая ответственность может быть уголовной, гражданско-правовой или административной. Привлечение к такой ответственности не исключает привлечения к уголовной ответственности физических лиц, совершивших преступление.

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

Преследование, вынесение судебного решения и санкции

Каждое Государство-участник предусматривает применение таких санкций за совершение какого-либо преступления, признанного таковым в соответствии со статьями настоящей Конвенции, которые учитывают степень опасности этого преступления.

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

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

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

Каждое Государство-участник в надлежащих случаях устанавливает согласно своему внутреннему законодательству длительный срок давности для возбуждения уголовного преследования за любое преступление, охватываемое настоящей Конвенцией, и более длительный срок давности в тех случаях, когда лицо, подозреваемое в совершении преступления, уклоняется от правосудия.

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

Отмывание доходов от преступлений, совершенных с использованием информационно-коммуникационных технологий

Каждое Государство-участник принимает, в соответствии с основополагающими принципами своего внутреннего законодательства, такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений следующие деяния, когда они совершаются умышленно:

a) конверсию или перевод имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника этого имущества или в целях оказания помощи любому лицу, участвующему в совершении основного правонарушения, с тем чтобы оно могло уклониться от ответственности за свои деяния;

b) сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежность, если известно, что такое имущество представляет собой доходы от преступлений;

c) приобретение, владение или использование имущества, если в момент его получения известно, что такое имущество представляет собой доходы от преступлений;

d) участие, причастность или вступление в сговор с целью совершения любого из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, покушение на его совершение, а также пособничество, подстрекательство, содействие или дача советов при его совершении.

Для целей осуществления или применения положений настоящего пункта каждое Государство-участник стремится:

a) применять положения настоящего пункта к самому широкому кругу основных правонарушений;

b) включать в число основных правонарушений преступления, признанные таковыми в соответствии со статьями настоящей Конвенции. В случае, когда законодательство Государств-участников содержит перечень конкретных основных правонарушений, в него включается как минимум всеобъемлющий круг преступлений, связанных с деятельностью организованных преступных групп;

c) для целей подпункта (b) основные правонарушения включают преступления, совершенные как в пределах, так и за пределами юрисдикции соответствующего Государства-участника. Однако, преступления, совершенные за пределами юрисдикции какого-либо Государства-участника, представляют собой основные правонарушения только при условии, что соответствующее деяние является уголовно наказуемым согласно внутреннему законодательству государства, в котором оно совершено, и было бы уголовно наказуемым согласно внутреннему законодательству Государства-участника, в котором осуществляется или применяется настоящая статья, если бы оно было совершено в нем;

d) каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам или их описание.

Воспрепятствование осуществлению правосудия

Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться, с тем чтобы признать в качестве уголовных преступлений следующие деяния, когда они совершаются умышленно:

a) применение физической силы, угроз или запугивания или обещание, предложение или предоставление неправомерного преимущества с целью склонения к даче ложных показаний или вмешательства в процесс дачи показаний или представления доказательств в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией;

b) применение физической силы, угроз или запугивания с целью вмешательства в выполнение должностных обязанностей должностным лицом судебных или правоохранительных органов в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией. Ничто в настоящем

подпункте не наносит ущерба праву Государств-участников иметь законодательство, обеспечивающее защиту других категорий публичных должностных лиц.

Юрисдикция

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:

a) преступление совершено на территории этого Государства-участника;

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

Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, когда:

a) преступление совершено на территории этого Государства-участника;

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

c) преступление совершено против этого Государства-участника.

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 лишь на том основании, что оно является одним из его граждан.

Если Государство-участник, осуществляющее свою юрисдикцию согласно предыдущим пунктам, получает уведомление или иным образом узнает о том, что другое Государство-участник осуществляет 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 с целью координации своих действий.

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

Европейский союз и его государства-члены

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

Глава II
Криминализация и правоохранительная деятельность

Статья 5
Противозаконный доступ

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, неправомерный доступ к компьютерной системе в целом или любой ее части, если он совершен с нарушением мер безопасности.

2. Государство-участник может требовать, чтобы такое деяние считалось преступным, если оно было совершено с намерением завладеть компьютерными данными или иным умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 6
Неправомерный перехват

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, неправомерный перехват с использованием технических средств не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные.

2. Государство-участник может требовать, чтобы такое деяние считалось преступным, если оно было совершено с умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 7
Неправомерное воздействие на данные

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений, когда такие деяния совершаются умышленно, неправомерное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.

2. Государство-участник может квалифицировать в качестве уголовного преступления только те предусмотренные пунктом 1 деяния, которые влекут за собой серьезный ущерб.

Статья 8
Неправомерное воздействие на функционирование системы

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, неправомерное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Статья 9
Противозаконное использование устройств

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений следующие деяния, когда они совершаются умышленно и неправомерно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройств, включая компьютерные программы, разработанных или приспособленных главным образом для целей совершения любого из правонарушений, предусмотренных положениями статей 5–8 настоящей Конвенции;

ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части;

с намерением использовать их в целях совершения любого из правонарушений, предусмотренных статьями 5–8 настоящей Конвенции; и

b) владение предметами, указанными в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать их в целях совершения любого из правонарушений, предусмотренных статьями 5–8 настоящей Конвенции. Государство-участник может требовать, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иные формы предоставления в пользование или владение, упомянутые в пункте 1 настоящей статьи, не имеют целью совершение правонарушений, предусмотренных статьями 5–8 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждое Государство-участник может не применять пункт 1 настоящей статьи при условии, что оговорка об этом не будет касаться продажи, распространения и или иных форм предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Статья 10
Покушение, пособничество и подстрекательство

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений, когда такие деяния совершаются умышленно, пособничество в совершении или подстрекательство к совершению любого правонарушения, предусмотренного положениями статей 5–9 настоящей Конвенции.

2. Каждое Государство-участник может принять такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, покушение на совершение любого правонарушения, предусмотренного положениями статей 5–9 настоящей Конвенции.

Статья 11
Ответственность юридических лиц

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться, с учетом его правовых принципов, для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями, предусмотренными положениями статей 5–10 настоящей Конвенции.

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

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

Статья 12
Преследование, вынесение судебного решения и санкции

1. Каждое Государство-участник за совершение какого-либо преступления, признанного таковым в соответствии со статьями 5–10 настоящей Конвенции, предусматривает применение эффективных, соразмерных и оказывающих сдерживающее воздействие санкций в отношении как физических, так и юридических лиц.

2. Каждое Государство-участник стремится обеспечить использование любых предусмотренных в его внутреннем законодательстве дискреционных юридических полномочий, относящихся к уголовному преследованию лиц за

преступления, охватываемые настоящей Конвенцией, для достижения максимальной эффективности правоохранительных мер в отношении этих преступлений и с должным учетом необходимости воспрепятствовать совершению таких преступлений.

3. Каждое Государство-участник создает и поддерживает действенную основанную на верховенстве права национальную систему уголовного правосудия, которая может обеспечить привлечение к ответственности любого лица, преследуемого за преступления, охватываемые настоящей Конвенцией, при обеспечении полной защиты прав человека и основных свобод, включая право на справедливое судебное разбирательство и права защиты.

Гана

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

Глава II. Положения о криминализации[32]

Киберзависимые преступления: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Статья 5
Несанкционированный доступ к компьютерной системе

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, получение доступа к компьютерной системе в целом или любой ее части без разрешения или с превышением пределов разрешенного доступа. Сторона может требовать, чтобы такое деяние считалось преступным, если оно совершено с нарушением мер безопасности, с намерением завладеть компьютерными данными или иным бесчестным намерением или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 6
Несанкционированный доступ к критической информационной инфраструктуре

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления, когда такое деяние совершается умышленно, получение доступа к критической информационной инфраструктуре в целом или любой ее части без разрешения.

Статья 7
Несанкционированный перехват

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, осуществленный без разрешения перехват с использованием технических средств не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы,

[32] За основу текста настоящего раздела взяты тексты Конвенции Совета Европы о киберпреступности, Конвенции Африканского союза об укреплении безопасности в киберпространстве и защите личных данных, Закона об электронных сделках 2008 года (Закон 772) и Закона о кибербезопасности 2020 года (Закон 1038). Эти документы формируют законодательную базу Ганы в области борьбы с киберпреступностью.

включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные.

Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено с бесчестным намерением или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 8
Воздействие на данные

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, повреждение, удаление, ухудшение качества, изменение, копирование или блокирование компьютерных данных без разрешения.

2. Сторона может сохранить за собой право квалифицировать в качестве уголовного преступления только те предусмотренные пунктом 1 деяния, которые влекут за собой серьезный ущерб.

Статья 9
Воздействие на функционирование системы

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, создание без разрешения серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Статья 10
Противозаконное использование устройств

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству следующие деяния, когда они совершаются умышленно и неправомерно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройств, включая компьютерные программы, разработанных или приспособленных главным образом для целей совершения любого из правонарушений, предусмотренных положениями статей 5–9;

ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения любого из правонарушений, предусмотренных статьями 5–9; и

b) владение предметами, указанными в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать их в целях совершения любого из правонарушений, предусмотренных статьями 5–9. Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иные формы предоставления в пользование или владение, упомянутые в пункте 1 данной статьи, не имеют целью совершение правонарушений, предусмотренных статьями 5–9 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может сохранить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иных форм предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Преступления с использованием кибертехнологий: преступления, масштабы, скорость и последствия которых возросли в результате появления компьютерных систем[33]

Статья 11
Подлог с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству, когда такие деяния совершаются умышленно и неправомерно, ввод, изменение, удаление или блокирование компьютерных данных, влекущие появление неаутентичных данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Сторона может требовать, чтобы условием наступления уголовной ответственности являлось наличие намерения совершить обман или аналогичного бесчестного намерения.

Статья 12
Подлог с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно и неправомерно, причинение имущественного ущерба другому лицу путем:

a) любого ввода, изменения, удаления или блокирования компьютерных данных;

b) любого вмешательства в функционирование компьютерной системы;

с намерением совершить мошенничество или обман в целях неправомерного извлечения экономической выгоды для себя или другого лица.

Преступления в отношении детей

Статья 13
Преступления, связанные с сексуальной эксплуатацией детей и надругательствами над ними в сети Интернет

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству следующие деяния, когда они совершаются умышленно и неправомерно:

a) производство материалов, содержащих сцены сексуальной эксплуатации детей и сексуальных надругательств над ними с целью публикации и распространения через компьютерную систему;

b) приобретение для себя или для другого лица материалов, содержащих сцены сексуальной эксплуатации детей и сексуальных надругательств над ними;

[33] Мошенничество с использованием компьютерных технологий, подлог с использованием компьютерных технологий и преступления, направленные против детей, толкуются в соответствии с Конвенцией Совета Европы о киберпреступности, Конвенцией Африканского союза об укреплении безопасности в киберпространстве и защите личных данных и Законом о кибербезопасности 2020 года (Закон 1038).

c) предложение материалов, содержащих сцены сексуальной эксплуатации детей и сексуальных надругательств над ними, или предоставление доступа к таким материалам через компьютерную систему или электронное устройство;

d) публикацию, распространение, трансляцию (включая прямую трансляцию), передачу материалов, содержащих сцены сексуальной эксплуатации детей и сексуальных надругательств над ними, через компьютер или электронное устройство; или

e) хранение материалов, содержащих сцены сексуальной эксплуатации детей и сексуальных надругательств над ними, в компьютерной системе или на компьютере или электронном носителе информации.

2. Для целей пункта (c) подраздела 1 лицо публикует материалы, содержащие сцены сексуальной эксплуатации детей и сексуальных надругательств над ними, если это лицо:

a) передает имеющиеся у него материалы, содержащие сцены сексуальной эксплуатации детей и сексуальных надругательств над ними, во владение другому лицу; или

b) демонстрирует или предлагает материалы, содержащие сцены сексуальной эксплуатации детей и сексуальных надругательств над ними.

3. Для целей настоящего раздела в понятие «материалы, содержащие сцены сексуальной эксплуатации детей и сексуальных надругательств над ними» включаются материальные изображения, записи устройств визуальной регистрации, видеоматериалы, аудиоматериалы, материалы прямых трансляций, рисунки или тексты, которые демонстрируют или описывают:

a) участие ребенка в откровенных сексуальных или непристойных действиях;

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

c) изображения ребенка, участвующего в откровенных сексуальных или непристойных действиях;

d) сексуально откровенные изображения детей;

e) процесс или материал для просмотра сцен сексуальной эксплуатации детей и надругательств над ними в режиме реального времени, часто с участием преступника, чинящего надругательство;

f) любые письменные материалы, визуальные изображения или аудиозаписи, в которых пропагандируются или рекомендуются незаконные сексуальные действия с детьми;

g) любые письменные материалы, основной характерной особенностью которых является описание с сексуальной целью незаконных сексуальных действий с ребенком;

h) любые аудиозаписи, основной характерной особенностью которых является описание с сексуальной целью незаконных сексуальных действий с ребенком.

Статья 14
Сношение с ребенком в целях сексуального надругательства

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, использование:

a) компьютерного онлайн-сервиса;

b) услуг, предоставляемых в сети Интернет;

c) местных служб публикации объявлений; или

d) любого другого устройства, способного сохранять или передавать электронные данные;

для соблазнения, уговоров, заманивания, ухаживания или обольщения, либо попыток соблазнения, уговоров, заманивания, ухаживания или обольщения в отношении ребенка или другого лица, которое, по мнению данного лица, является ребенком, с целью поощрения, побуждения, подстрекательства к незаконным сексуальным действиям, предложения таких действий ребенку или в отношении ребенка, либо с целью визуального изображения таких действий.

Статья 15
Киберпреследование ребенка

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, использование компьютерного онлайн-сервиса, услуг, предоставляемых в сети Интернет, или местной интернет-службы публикации объявлений или любого другого электронного устройства для сбора, передачи, публикации, воспроизведения, покупки, продажи, получения, обмена или распространения сведений, содержащих имя, номер телефона, адрес электронной почты, адрес проживания, фотографическое изображение, физическое описание, характеристики или любую другую идентифицирующую информацию о ребенке для дальнейшей организации встречи с ребенком с целью вступления в половую связь, побуждения к сексуально откровенному поведению или незаконным сексуальным действиям.

Другие сексуальные преступления в сети Интернет[34]

Статья 16
Секс-шантаж

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству, когда такие деяния совершаются умышленно, угрозы распространить по почте, электронной почте, текстовыми сообщениями или передать с помощью электронных средств или иным образом интимное изображение или движущиеся изображения другого лица, участвующего в откровенных сексуальных действиях, с конкретным намерением:

a) подвергнуть это лицо преследованию, угрозам, принуждению, запугиванию или оказать на него ненадлежащее влияние, особенно с целью вымогательства денег или другого вознаграждения или принуждения жертвы к участию в нежелательных сексуальных действиях; или

b) фактически вымогать деньги или иное вознаграждение или принудить жертву к участию в нежелательных сексуальных действиях.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, угрозу распространить по почте, электронной почте, текстовыми сообщениями или передать с помощью электронных средств или иным образом частное изображение или движущиеся изображения ребенка, участвующего в откровенных сексуальных действиях, с конкретным намерением:

[34] В соответствии с положениями Закона о кибербезопасности.

a) подвергнуть ребенка преследованию, угрозам, принуждению, запугиванию или оказать на него ненадлежащее влияние, особенно с целью вымогательства денег или другого вознаграждения или принуждения жертвы к участию в нежелательных сексуальных действиях; или

b) фактически вымогать деньги или иное вознаграждение или принудить жертву к участию в нежелательных сексуальных действиях.

3. Для целей пунктов 1 и 2 в понятие «интимное изображение» может включаться такое изображение, где генитальная или анальная область тела другого лица обнажена или прикрыта только нижним бельем; или показана грудь ниже верхней границы ареолы, которая либо не прикрыта, либо хорошо видна через одежду.

Статья 17
Распространение интимных изображений без согласия

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для признания в качестве уголовных преступлений в соответствии с ее внутренним законодательством умышленного распространения или умышленного побуждения другого лица к распространению интимного изображения или запрещенной визуальной записи другого идентифицируемого лица без согласия лица, которое запечатлено на интимном изображении, с намерением причинить тяжелые нравственные страдания, и в отношении которого в момент создания изображения или визуальной записи и/или в момент совершения преступления имелись разумные основания ожидать соблюдения неприкосновенности частной жизни.

2. Для целей данного пункта в понятие причинения «тяжелых нравственных страданий» включается любое умышленное поведение, которое приводит к таким психическим реакциям, как страх, нервозность, горе, беспокойство, тревога, стыд, шок, чувство унижения и оскорбления достоинства, а также к физической боли.

Статья 18
Угроза распространения запрещенного интимного изображения или визуальной записи

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, угрозу распространить запрещенное интимное изображение или визуальную запись другого лица, таким образом, что эти действия могут причинить этому другому лицу обоснованно возникающие при всех обстоятельствах страдания, и угроза осуществляется таким образом, что это может вызвать у этого другого лица обоснованно возникающие при всех обстоятельствах опасения, что угроза будет исполнена.

Статья 19
Преступления, связанные с нарушением авторских и смежных прав[35]

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству нарушение авторского права, как оно определено в законодательстве этой Стороны во исполнение обязательств, взятых ею на себя по Парижскому Акту от 24 июля 1971 года в отношении Бернской конвенции об охране литературных и художественных произведений, Соглашения по торговым аспектам прав интеллектуальной собственности и Договора

[35] В соответствии с Конвенцией Совета Европы о киберпреступности и Конвенцией Африканского союза об укреплении безопасности в киберпространстве и защите личных данных.

Всемирной организации интеллектуальной собственности (ВОИС) по авторскому праву, за исключением любых моральных прав, предоставляемых такими конвенциями, когда такие действия совершаются умышленно, в коммерческих масштабах и с помощью компьютерной системы.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству нарушение смежных прав, как они определены законодательством этой Стороны во исполнение обязательств, взятых ею на себя по Международной конвенции об охране прав исполнителей, производителей фонограмм и вещательных организаций («Римская конвенция»), Соглашению по торговым аспектам прав интеллектуальной собственности и Договору ВОИС по исполнениям и фонограммам, за исключением любых моральных прав, предоставляемых такими конвенциями, когда такие действия совершаются умышленно, в коммерческих масштабах и с помощью компьютерной системы.

3. Сторона может сохранить за собой право в ограниченных обстоятельствах не вводить уголовную ответственность согласно положениям пунктов 1 и 2 настоящей статьи при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не приведет к отступлению от выполнения Стороной ее международных обязательств, изложенных в международных документах, упомянутых в пунктах 1 и 2 настоящей статьи.

Статья 20
Покушение, пособничество или подстрекательство

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству, когда такие деяния совершаются умышленно, пособничество в совершении или подстрекательство к совершению любого из преступлений, признанных таковыми в соответствии со статьями 5–19 настоящей Конвенции, с намерением добиться совершения такого преступления.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, покушение на совершение любого из преступлений, признанных таковыми в соответствии со статьями 7–9; 11; 12; пунктами 1 (a), (b) и (e) статьи 13; 14; 15; 16; и 17.

Статья 21
Корпоративная ответственность

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлением, признанным в качестве такового в соответствии с настоящей Конвенцией, если это преступление совершено в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа юридического лица, занимающего в нем руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, предусмотренным пунктом 1 настоящей статьи, каждая Сторона принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение преступления, предусмотренного в

соответствии с настоящей Конвенцией, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от правовых принципов Государства-участника ответственность юридического лица может быть уголовной, гражданско-правовой или административной.

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

Статья 22
Санкции и меры

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для обеспечения того, чтобы уголовные преступления, признанные таковыми в соответствии со статьями 5–20, наказывались эффективными, соразмерными и сдерживающими санкциями, включающими лишение свободы.

2. Каждая Сторона обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии со статьей 21, эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций, включая денежные санкции.

Иран (Исламская Республика)

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

2. Криминализация

Преступники все чаще организуют и осуществляют противоправную деятельность не только против, но и с помощью устройств, в которых используются информационно-коммуникационные технологии. Хотя преступные деяния могут быть признаны преступлениями независимо от неправомерного использования информационно-коммуникационных технологий, или наоборот, в некоторых случаях тяжесть и другие факторы, характеризующие правонарушение, требуют криминализации противоправного деяния, совершенного с использованием информационно-коммуникационных технологий. Это в особенности касается тех случаев, когда использование информационно-коммуникационных технологий усиливает совершение преступлений, в частности, с точки зрения масштабов вреда, который они наносят жертвам. Поэтому в дополнение к преступлениям, зависимым от информационно-коммуникационных технологий, в рамках конвенции должны быть криминализированы преступления, совершаемые с помощью этих технологий. Тем не менее, с юридической точки зрения это может потребовать индивидуального подхода в каждом конкретном случае, поскольку различные формы преступления могут отражать различные элементы, а также actus reus и mens rea. При принятии мер по квалификации правонарушений следует учитывать основополагающие принципы национальных правовых систем.

Следует также установить ответственность юридических лиц, чтобы обеспечить всеобъемлющий характер реагирования на преступную деятельность и лишить правонарушителей свободы действий под прикрытием юридических лиц. Такая мера должна предусматривать ответственность юридических лиц за преднамеренное или иное осознанное участие в совершении преступлений, которые будут признаны таковыми в соответствии с конвенцией.

Япония

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

1. Криминализация

1.1. Киберзависимые преступления

1.1.1. Япония признает, что в Специальном комитете существует общий консенсус относительно криминализации киберзависимых преступлений, которые в основном представляют собой преступления, связанные с нарушением конфиденциальности, целостности и доступности компьютерных данных и систем. Исходя из этого признания, Япония поддерживает криминализацию киберзависимых преступлений.

1.1.2. Мы считаем, что многие деяния, которые необходимо криминализировать для решения сегодняшних проблем, имеющих, по мнению каждого Государства-члена, большое значение, таких как атаки с использованием вирусов-вымогателей и атаки на компьютерные системы критической инфраструктуры, входят в круг киберзависимых преступлений. Такие киберзависимые преступления могут включать незаконный доступ, незаконный перехват, воздействие на компьютерные данные или компьютерные системы, противозаконное использование устройств и другие правонарушения.

1.1.3. Япония признает важность мер противодействия атакам на компьютерные системы информационных инфраструктур и объектов. Однако, поскольку такие злонамеренные действия, как кража или изменение данных путем взлома, могут рассматриваться в рамках киберзависимых преступлений, нет необходимости рассматривать эти правонарушения как проблемы, присущие лишь сфере информационных инфраструктур или объектов. Кроме того, поскольку важно сделать готовящуюся конвенцию применимой в долгосрочной перспективе, следует отметить, что положения о криминализации потеряют свою универсальность, если они будут слишком сосредоточены на отдельных характерных особенностях преступлений. Кроме того, важно, чтобы в новой конвенции были предусмотрены основные и существенные положения, которые могли бы соблюдаться и применяться как можно большим числом Государств-членов. В свете этого обсуждение следует начать с таких распространенных киберпреступлений, как противозаконный доступ. Во избежание дублирования положений о криминализации следует тщательно рассмотреть вопрос о необходимости принятия специального положения об атаках на компьютерные системы информационных инфраструктур и объектов в дополнение к положениям об общих киберпреступлениях.

1.1.4. Кроме того, необходимо избежать риска сдерживающего воздействия на такие законные операции и виды деятельности, как разработка технологий, и злоупотребления полномочиями со стороны правоохранительных органов, вызванного чрезмерно широкой сферой криминализации. Например, во избежание введения абсолютной ответственности при криминализации незаконного доступа может потребоваться оговорка об отсутствии законных оснований для доступа и осознании этого факта.

1.1.5. Кроме того, требование единого наказания за покушение на преступление или пособничество и подстрекательство к преступлению, или требование наказания на стадии подготовки или вступления в сговор, что недостаточно для признания состава покушения, было бы чрезмерным вмешательством во внутреннее уголовное законодательство отдельных государств. Криминализация этих правонарушений должна быть оставлена на усмотрение национального законодательства каждого Государства-члена. Что касается мер противодействия киберпреступлениям, имеющим транснациональный характер, очень важно не создавать безопасную гавань для киберпреступности. Поэтому необходимо

избегать установления положений, ограничивающих число Государств-членов, которые могут заключить новую конвенцию, ввиду различий в основных правовых концепциях, неизбежно существующих между Государствами-членами.

1.2. Свобода выражения мнений

1.2.1. При рассмотрении вопроса о криминализации деятельности в киберпространстве следует ссылаться на международные договоры по правам человека. При определении того, какие деяния могут быть признаны киберпреступлениями в соответствии с новой конвенцией, особенно в отношении криминализации деяний, связанных с вредоносным контентом в сети Интернет, Государства-члены не должны забывать о важности защиты свободы выражения мнений.

1.2.2. Например, согласно пункту 2 статьи 19 Международного пакта о гражданских и политических правах, свобода выражения мнений «включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно, посредством печати или художественных форм выражения, или иными способами по своему выбору». Помня о том, что в пункте 3 статьи 19 предусмотрены определенные ограничения этого права, мы должны обеспечить возможность разработки национальных законов с учетом фактической ситуации в каждом Государстве-члене, с тем чтобы не были несправедливо ущемлены права и свободы, касающиеся академических исследований, культурной и художественной деятельности и прессы.

1.2.3. В целях защиты свободы выражения мнений необходимо избегать сдерживающего воздействия на виды деятельности, связанные с самовыражением. Поэтому криминализация деяний, связанных с вредоносным контентом в сети Интернет, должна осуществляться только в той мере, в какой все Государства-члены могут договориться об определении таких деяний, и при наличии доказуемых оснований, оправдывающих необходимость наказания.

1.2.4. Мы полагаем, что для того, чтобы Конвенция стала договором, который смогут заключить как можно больше Государств-членов, и дождаться, пока принесут свои плоды обсуждения как на национальном, так и на международном уровне, целесообразнее всего оставить вопрос о криминализации деяний, связанных с вредоносным контентом, для будущего дополнительного протокола.

1.3. Обычные преступления с использованием киберпространства

1.3.1. Что касается преступлений, связанных с терроризмом, преступлений, связанных с огнестрельным оружием, и преступлений, связанных с наркотиками, то они могут представлять собой обычные преступления, даже если они совершены с использованием сети Интернет, и к ним также могут применяться существующие договоры, такие как Конвенция Организации Объединенных Наций против транснациональной организованной преступности.

1.3.2. Вопрос о криминализации этих действий должен быть тщательно продуман во избежание дублирования вышеупомянутых существующих документов. Следует также обратиться к обсуждениям, состоявшимся в процессе разработки существующих договоров, чтобы положения, которые намеренно не были включены в них, не были закреплены в настоящей Конвенции лишь в другой форме.

1.4. Возможные преступления с использованием кибертехнологий, которые подлежат рассмотрению

Что касается преступлений с использованием кибертехнологий, то помимо преступлений, связанных с вредоносным контентом (см. пункт 1.2 выше), некоторые правонарушения с использованием кибертехнологий, которые признаются значимыми в плане криминализации в качестве киберпреступлений в

соответствии с данной Конвенцией, могут подлежать обсуждению на предмет криминализации при условии, что все Государства-члены смогут договориться об определении таких деяний и что существуют доказуемые основания, оправдывающие необходимость наказания. К таким преступлениям с использованием кибертехнологий относятся правонарушения, сфера охвата, скорость и масштаб ущерба от которых увеличиваются вследствие применения компьютеров. Эти преступления могут включать нижеследующие правонарушения.

1.4.1. Подлог с использованием компьютерных технологий

Обнаружить подделку компьютерных данных с помощью человеческих органов чувств довольно сложно. Кроме того, в современном мире, где многие бизнес-процессы выполняются с помощью компьютера, социальные последствия подрыва доверия к компьютерным данным весьма значительны. Поэтому Япония могла бы поддержать криминализацию ввода, изменения, удаления или блокирования компьютерных данных, влекущих за собой появление неаутентичных данных, в случае умышленного и неправомерного совершения таких деяний.

1.4.2. Мошенничество с использованием компьютерных технологий

Мошенничество с компьютерными данными, когда оно совершается путем подлога компьютерных данных или воздействия на функционирование компьютерных систем, легко совершается против широкого круга потенциальных жертв и может нанести серьезный материальный ущерб во многих Государствах-членах. Поэтому мы могли бы поддержать криминализацию причинения имущественного ущерба другому лицу путем любого ввода, изменения, удаления или блокирования компьютерных данных или любого воздействия на функционирование компьютерной системы с намерением совершить мошенничество или обман в целях извлечения выгоды.

1.4.3. Нарушение авторских прав

В сети Интернет можно без труда копировать данные и воспроизводить содержание, и такое содержание быстро распространяется, что может повысить степень нарушения авторских прав. Мы считаем, что было бы полезно ввести уголовную ответственность за нарушение авторских и смежных прав, если такие действия совершаются умышленно, в коммерческих масштабах и с помощью компьютерной системы, со ссылкой на существующие международные соглашения, касающиеся авторского права.

1.4.4. Сексуальные надругательства над детьми и их сексуальная эксплуатация

Производство и распространение материалов, содержащих сцены сексуальных надругательств над детьми, являются крайне злонамеренными деяниями, оказывающими вредное воздействие на психическое и физическое здоровье изображаемых детей и серьезно нарушающими их права человека. Удаление материалов, содержащих сцены сексуальных надругательств над детьми, после их распространения через сеть Интернет сопряжено с трудностями, и эти материалы продолжают серьезно препятствовать полноценному воспитанию детей. С точки зрения защиты прав детей мы поддерживаем введение уголовной ответственности за производство и распространение материалов, содержащих визуальные изображения ребенка, участвующего в откровенных сексуальных действиях.

Тем не менее, мы считаем, что следует тщательно рассмотреть вопрос о том, трактовать ли реалистические изображения, представляющие лицо, кажущееся несовершеннолетним, или несуществующего ребенка, участвующего в откровенных сексуальных действиях, как материалы о сексуальных надругательствах над детьми и криминализировать ли правонарушения, связанные с этими изображениями, принимая во внимание тот факт, что существующее несовершеннолетнее лицо не является объектом прямого надругательства, а также важность свободы выражения мнений.

1.5. Ответственность юридических лиц

Мы поддерживаем введение ответственности юридических лиц в определенной степени в тех случаях, когда организации таких юридических лиц совершают многочисленные киберпреступления в связи с ведением своего бизнеса, при условии, что ответственность может быть уголовной, гражданской или административной в соответствии с правовыми принципами каждого Государства-члена. Распределение ролей между уголовными, гражданскими и административными делами и необходимость применения санкций — это вопросы, которые следует оставить на усмотрение внутреннего законодательства каждого Государства-члена, поскольку они должны рассматриваться в свете государственной структуры каждого Государства-члена и паритета с управлением вне киберсектора в каждом Государстве-члене.

Иордания

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

Иорданское Хашимитское Королевство предлагает ввести уголовную ответственность за следующие деяния в соответствии с проектом конвенции:

- неправомерный доступ к информационной сети, информационной системе или любой их части любым способом, без разрешения или в нарушение разрешения; строгость наказания за это преступление должна повышаться в случае неправомерного доступа к информационной сети, информационной системе или любой их части, принадлежащей официальному, государственному, охранному, финансовому или банковскому учреждению, а также неправомерного доступа к критической инфраструктуре и данным или информации, недоступным для общественности, которые затрагивают национальную безопасность, международные отношения государства, общественную безопасность или национальную экономику;
- незаконный перехват трафика данных;
- взлом данных или информации, связанных с электронными методами платежей, выполнением электронных финансовых или банковских операций или переводом средств с использованием информационной сети или информационной системы;
- электронное мошенничество;
- мошенничество с IP-адресами;
- сексуальная эксплуатация с использованием информационных сетей или веб-сайтов;
- распространение слухов или ложных новостей с использованием информационных систем, сетей или веб-сайтов;
- ненавистнические высказывания или действия, связанные с оскорблением религий или государств с использованием информационных сетей или веб-сайтов;
- неправомерное вмешательство в информационные системы или информационные сети путем внедрения или установки вредоносного программного обеспечения;
- создание веб-сайта, похожего на реальный сайт, для введения в заблуждение или обмана пользователей с целью кражи данных для входа в систему или личной информации или незаконного сбора пожертвований;

- отправка электронных писем или текстовых сообщений с целью фишинга для кражи данных, распространения вредоносного программного обеспечения или попытки доступа к сетям или информационным системам, доступ к которым запрещен;
- создание поддельных страниц, групп или учетных записей в социальных сетях с целью введения в заблуждение или обмана пользователей, незаконного сбора пожертвований или электронного попрошайничества;
- целенаправленное использование устройств пользователей для создания информационной сети без ведома пользователей с целью ее использования для атак, направленных на подрыв доверия, или в противоправных целях;
- использование или попытка использования уязвимости системы безопасности информационных сетей или систем с целью проникновения в них или кражи, уничтожения или изменения данных;
- сканирование или попытка сканирования интернет-протоколов или портов доступа к сети без разрешения с целью сбора информации или выявления уязвимости системы безопасности;
- несанкционированное использование оборудования или программного обеспечения для подбора паролей или имен пользователей;
- использование технологии искусственного интеллекта для совершения противоправных деяний;
- деяния, связанные с выдачей себя за другого пользователя;
- деяния, связанные с нарушением неприкосновенности частной жизни;
- деяния, связанные с интеллектуальной собственностью и незаконным использованием программного обеспечения;
- деяния, представляющие собой атаку на цепи поставок;
- деяния, связанные с несанкционированным использованием данных поставщиками услуг;
- деяния, связанные с распространением, поддержкой или пропагандой террористической идеологии;
- деяния, связанные с использованием информационно-коммуникационных технологий в террористических целях;
- деяния, связанные с электронным мошенничеством;
- деяния, связанные со сбытом наркотических средств или торговлей ими с помощью электронных средств;
- деяния, связанные с отмыванием денежных средств с помощью электронных средств.

Мексика

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

Криминализация

Основополагающим элементом для определения обязательств по криминализации является национальная юрисдикция. В этой связи Мексика считает, что Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Организации Объединенных Наций против коррупции являются примерами положений, применимых по смыслу к противодействию преступлениям, связанным с использованием

информационно-коммуникационных технологий, за исключением случаев, связанных с информацией, хранящейся в «облаке», которые потребуют дальнейшего анализа и обсуждения на основе недавнего опыта конкретных расследований.

Отправной точкой для криминализации должно стать рассмотрение в Конвенции тех деяний, которые признаны международным правом преступлениями, особенно в соответствии с терминологией других договоров, принятых в рамках системы Организации Объединенных Наций, и которые совершаются с помощью информационно-коммуникационных технологий, электронных и цифровых средств. Таким образом, в Конвенцию рекомендуется включить следующую статью:

«Государства-участники признают в качестве преступлений для целей настоящей Конвенции все признаваемые действующим международным правом преступные деяния, которые совершаются с помощью информационных технологий и электронных средств».

Для правительства Мексики крайне важно, чтобы среди прочих уголовных преступлений в Конвенцию были включены преступления, связанные с сексуальной эксплуатацией детей, а также преступления, связанные с гендерным насилием с помощью информационно-коммуникационных технологий.

Рекомендуется включить в Конвенцию оперативные элементы для усиления расследования и уголовного преследования; затем уместно будет рассмотреть возможность включения приложений с этими шаблонами, в которых указываются данные, необходимые для выполнения запросов о предоставлении информации.

Поскольку предполагается, что Конвенция будет охватывать не все виды уголовных преступлений, а в первую очередь киберзависимые преступления, и в целях предотвращения несовместимости или дублирования национальных законов рекомендуется включить в документ общее обязательство Государств-участников при необходимости согласовывать свои законодательства.

«Ничто в настоящей Конвенции не затрагивает права, обязательства и ответственность государств и отдельных лиц в соответствии с действующим международным правом, направленные на предупреждение и пресечение использования информационно-коммуникационных технологий в преступных целях».

«Во всех действиях, направленных на осуществление настоящей Конвенции, первоочередное внимание уделяется наилучшему обеспечению интересов жертв преступлений, признанных таковыми в настоящей Конвенции, — отдельных лиц, а также учреждений и организаций».

Новая Зеландия

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

Положения о криминализации

1. В ходе первой сессии была выражена широкая поддержка включению в Конвенцию положений, направленных на борьбу с киберпреступностью, в частности с киберзависимыми преступлениями и ограниченным кругом преступлений с использованием кибертехнологий, причем возражений против включения этих положений выдвинуто не было.

2. В приложении 1 к настоящему документу мы предлагаем список положений о криминализации, по которым, по мнению Новой Зеландии, с наибольшей вероятностью может быть достигнут консенсус и которые поэтому должны быть

в центре внимания Специального комитета, учитывая ограниченность ресурсов и ограниченный запас времени. Мы также приводим некоторые предложения по тексту в целях содействия в составлении его проекта, главным образом на основе текстов других соответствующих международных документов, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности, Конвенция Организации Объединенных Наций против коррупции и Конвенция Совета Европы о киберпреступности (Будапештская конвенция).

3. Новая Зеландия поддерживает включение положения о юрисдикции, отражающего, где это применимо, содержание существующих документов, таких как статья 42 Конвенции Организации Объединенных Наций против коррупции, с дополнительными элементами, требующими от государств осуществлять юрисдикцию, если преступление или любая часть преступления совершены на территории Государства-участника, с целью учета того факта, что киберпреступления могут совершаться в киберпространстве, вследствие чего преступник, жертва, данные и используемая компьютерная система могут находиться в разных юрисдикциях.

Приложение 1 — Положения о криминализации

Незаконный доступ к компьютерным системам

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, неправомерное получение доступа к компьютерной системе в целом или любой ее части. Сторона может требовать, чтобы такое деяние считалось преступным, если оно совершено с нарушением мер безопасности, с намерением завладеть компьютерными данными или иным умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Незаконный перехват компьютерных данных

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, неправомерно осуществленный перехват с использованием технических средств не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено с умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Воздействие на компьютерные данные

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно, неправомерное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных.

2. Сторона может сохранить за собой право квалифицировать в качестве уголовного преступления только те предусмотренные пунктом 1 деяния, которые влекут за собой серьезный ущерб.

Воздействие на функционирование компьютера

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается

умышленно, неправомерное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Противозаконное использование устройств или компьютерных программ

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству следующие деяния, когда они совершаются умышленно и неправомерно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройств, включая компьютерные программы, разработанных или приспособленных главным образом для целей совершения любого из правонарушений, предусмотренных в соответствии с положениями [соответствующих статей];

ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения любого из правонарушений, предусмотренных [соответствующими статьями]; и

b) владение предметами, указанными в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать их в целях совершения любого из правонарушений, предусмотренных [соответствующими статьями]. Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иные формы предоставления в пользование или владение, упомянутые в пункте 1 настоящей статьи, не имеют целью совершение правонарушений, предусмотренных [соответствующими статьями], а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может сохранить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иных форм предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Криминализация кибервымогательства

1. Новая Зеландия поддерживает включение положения, предусматривающего уголовную ответственность за:

a) вымогательство у пользователя компьютерной системы для разблокировки данных;

b) вымогательство у пользователя компьютерной системы с угрозами несанкционированного раскрытия данных или личной информации.

2. Новая Зеландия надеется на сотрудничество с коллегами в деле разработки точных формулировок в отношении этого правонарушения.

Мошенничество с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления по своему внутреннему законодательству, когда такое деяние совершается умышленно и неправомерно, причинение имущественного ущерба другому лицу путем:

a) любого ввода, изменения, удаления или блокирования компьютерных данных;

b) любого вмешательства в функционирование компьютерной системы;

с намерением совершить мошенничество или обман в целях неправомерного извлечения экономической выгоды для себя или другого лица.

Подлог с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений по своему внутреннему законодательству, когда такие деяния совершаются умышленно и неправомерно, ввод, изменение, удаление или блокирование компьютерных данных, влекущие появление неаутентичных данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Сторона может требовать, чтобы условием наступления уголовной ответственности являлось наличие намерения совершить обман или аналогичного бесчестного намерения.

Сексуальная эксплуатация детей с использованием компьютерных систем

1. Мы надеемся на сотрудничество с коллегами в разработке эффективных и всеобъемлющих положений о криминализации, касающихся борьбы с сексуальной эксплуатацией детей и надругательством над ними в сети Интернет.

2. Как минимум, к этой категории преступлений следует отнести правонарушения, связанные с использованием компьютерной системы в целях:

a) производства материалов, содержащих сцены сексуальной эксплуатации детей;

b) предложения материалов, содержащих сцены сексуальной эксплуатации детей, или предоставления доступа к таким материалам;

c) распространения или передачи материалов, содержащих сцены сексуальной эксплуатации детей;

d) приобретения для себя или для другого лица материалов, содержащих сцены сексуальной эксплуатации детей;

e) владения материалами, содержащими сцены сексуальной эксплуатации детей;

f) ухаживания за детьми с целью их сексуальной эксплуатации.

Размещение или распространение визуальной записи интимного характера без согласия

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать уголовным преступлением по своему внутреннему законодательству передачу, пересылку, публикацию, распространение или препровождение иным путем с помощью компьютерной системы интимной визуальной записи жертвы без разумного оправдания:

a) если субъекту правонарушения известно, что жертва не давала согласия на размещение информации; или

b) если субъект правонарушения проявил безразличие в отношении того, дала ли жертва согласие на размещение информации.

2. Пояснение: ребенок или подросток в возрасте до 16 лет не может давать согласие на размещение интимной визуальной записи, объектом которой он является.

Участие и покушение

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления в соответствии со своим внутренним законодательством участие в любом качестве, например, в качестве сообщника, пособника или подстрекателя, в совершении какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

2. Каждое Государство-участник может принять такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления в соответствии со своим внутренним законодательством любое покушение на совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

3. Каждое Государство-участник может принять такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного преступления в соответствии со своим внутренним законодательством приготовление к совершению какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

Ответственность юридических лиц

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

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

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

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

5. Юридические лица не подлежат ответственности за действие, совершенное или не совершенное добросовестно:

a) при исполнении или предполагаемом исполнении обязанности, налагаемой настоящей Конвенцией или в соответствии с ней; или

b) при осуществлении или предполагаемом осуществлении функции или полномочий, предусмотренных настоящей Конвенцией или в соответствии с ней.

Криминализация отмывания денежных средств

1. Каждое Государство-участник принимает, в соответствии с основополагающими принципами своего внутреннего законодательства, такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных преступлений следующие деяния, когда они совершаются умышленно:

a) i) конверсию или перевод имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника этого имущества или в целях оказания помощи любому лицу, участвующему в совершении основного правонарушения, с тем чтобы оно могло уклониться от ответственности за свои деяния;

ii) сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежность, если известно, что такое имущество представляет собой доходы от киберпреступлений;

b) при условии соблюдения основных принципов своей правовой системы:

i) приобретение, владение или использование имущества, если в момент его получения известно, что такое имущество представляет собой доходы от киберпреступлений;

ii) участие, причастность или вступление в сговор с целью совершения любого из преступлений, признанных таковыми в соответствии с настоящей статьей, покушение на его совершение, а также пособничество, подстрекательство, содействие или дача советов при его совершении.

2. Для целей осуществления или применения пункта 1 настоящей статьи:

a) каждое Государство-участник стремится применять пункт 1 настоящей статьи к самому широкому кругу основных правонарушений;

b) каждое Государство-участник включает в число основных правонарушений [соответствующие преступления, признанные таковыми в соответствующей статье настоящей Конвенции и] преступления, признанные таковыми в [соответствующих статьях] настоящей Конвенции. В случае, когда законодательство Государств-участников содержит перечень конкретных основных правонарушений, в него включается как минимум всеобъемлющий круг преступлений, связанных с киберпреступностью;

c) для целей подпункта (b) основные правонарушения включают преступления, совершенные как в пределах, так и за пределами юрисдикции соответствующего Государства-участника. Однако преступления, совершенные за пределами юрисдикции какого-либо Государства-участника, представляют собой основные правонарушения только при условии, что соответствующее деяние является уголовно наказуемым согласно внутреннему законодательству государства, в котором оно совершено, и было бы уголовно наказуемым согласно внутреннему законодательству Государства-участника, в котором осуществляется или применяется настоящая статья, если бы оно было совершено в нем;

d) каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам или их описание;

e) если этого требуют основополагающие принципы внутреннего законодательства Государства-участника, то можно предусмотреть, что преступления, указанные в пункте 1 настоящей статьи, не относятся к лицам, совершившим основное правонарушение;

f) осознание, умысел или цель как элементы состава преступления, указанного в пункте 1 настоящей статьи, могут быть установлены из объективных фактических обстоятельств дела.

Воспрепятствование осуществлению правосудия

Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться, с тем чтобы признать в качестве уголовных преступлений следующие деяния, когда они совершаются умышленно:

a) применение физической силы, угроз или запугивания или обещание, предложение или предоставление неправомерного преимущества с целью склонения к даче ложных показаний или вмешательства в процесс дачи показаний или представления доказательств в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией;

b) применение физической силы, угроз или запугивания с целью вмешательства в выполнение должностных обязанностей должностным лицом судебных или правоохранительных органов в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией. Ничто в настоящем подпункте не наносит ущерба праву Государств-участников иметь законодательство, обеспечивающее защиту других категорий публичных должностных лиц.

Норвегия

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

Криминализация

1. Мы полагаем, что в конвенции должны криминализироваться преступления, которые являются киберзависимыми. Несмотря на то, что киберпреступность меняется с каждым днем, национальные и международные учреждения смогли выявить основные повторяющиеся типы преступных деяний. Сегодня во многих Государствах-членах за эти преступления уже предусмотрена уголовная ответственность. В этой связи правительство Королевства Норвегия рекомендует рассмотреть по меньшей мере следующие преступления, совершаемые в информационной среде:

- незаконный доступ, т. е. получение несанкционированного доступа к компьютеру или компьютерной системе;
- незаконный перехват, т. е. неправомерный перехват в режиме реального времени содержания передаваемой информации или технических параметров трафика, относящихся к передаче информации;
- воздействие на данные или систему, т. е. использование вредоносного программного обеспечения, атак типа «отказ в обслуживании», программ-вымогателей, удаление либо изменение данных;
- противоправное использование устройств, т. е. незаконная торговля данными о кредите, паролями и личной информацией, которые позволяют получить доступ к ресурсам, или их незаконное использование.

2. Мы хотели бы, чтобы перечень был кратким.

3. В Конвенции также следует избегать дублирования положений о преступлениях, которые охватываются другими правовыми документами.

4. Текст должен быть нейтральным в отношении технологий.

5. В дополнение к краткому перечню киберзависимых преступлений в конвенцию следует включить положения о преступлениях, связанных с материалами, содержащими сцены сексуальных надругательств над детьми.

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

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

Глава II
Криминализация, уголовное производство и правоохранительная деятельность

Раздел 1
Установление ответственности

Статья 5
Установление ответственности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству деяний, предусмотренных как минимум статьями 6, 7, 9–12, 14–17, 19–20, 22–26 и 28 настоящей Конвенции, применяя при этом такие уголовные и иные санкции, включая лишение свободы, которые учитывают степень общественной опасности конкретного деяния и размер причиненного ущерба.

Статья 6
Неправомерный доступ к цифровой информации

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного неправомерного доступа к цифровой информации, повлекшего ее уничтожение, блокирование, модификацию либо копирование.

Статья 7
Неправомерный перехват

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного перехвата цифровой информации осуществляемого без соответствующих прав и/или с нарушением установленных норм, в том числе с использованием технических средств перехвата технических параметров трафика и данных, обрабатываемых с использованием информационно-коммуникационных технологий и не предназначенных для общего пользования.

Статья 8
Неправомерное воздействие на цифровую информацию

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству умышленного неправомерного воздействия на цифровую информацию путем ее повреждения, удаления, изменения, блокирования, модификации либо копирования информации в цифровой форме.

Статья 9
Нарушение функционирования информационно-коммуникационных сетей

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного неправомерного действия,

направленного на нарушение функционирования информационно-коммуникационных сетей, повлекшего тяжкие последствия или создавшее угрозу их наступления.

Статья 10
Создание, использование и распространение вредоносных программ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленных создания, в том числе адаптирования, использования и распространения вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования, распространения цифровой информации или нейтрализации средств ее защиты, за исключением случаев правомерного проведения исследований.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, создания или использования бот-сети для целей совершения какого-либо из деяний, предусмотренных положениями статей 6–12 и 14 настоящей Конвенции.

Статья 11
Неправомерное воздействие на критическую информационную инфраструктуру

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленных создания, распространения и (или) использования компьютерных программ либо иной цифровой информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой цифровой информации, содержащейся в критической информационной инфраструктуре, или информационных систем, информационно-коммуникационных сетей, относящихся к критической информационной инфраструктуре, либо правил доступа к ним, если оно повлекло причинение вреда критической информационной инфраструктуре.

Статья 12
Несанкционированный доступ к персональным данным

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания согласно его внутреннему законодательству в качестве преступления несанкционированного доступа к персональным данным в целях их уничтожения, изменения, копирования, распространения.

Статья 13
Незаконный оборот устройств

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству незаконных производства, продажи, приобретения для использования, импорта, экспорта или иных форм предоставления в пользование устройств, разработанных или адаптированных прежде всего для целей совершения какого-либо из преступлений, предусмотренных положениями статей 6–12 настоящей Конвенции.

Положения настоящей статьи не распространяются на случаи, когда производство, продажа, приобретение для использования, импорт, экспорт или иные формы предоставления в пользование устройств связаны, например, с разрешенным испытанием или защитой компьютерной системы.

Статья 14
Хищение с использованием информационно-коммуникационных технологий

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству хищения имущества, либо незаконного приобретения права на него, в том числе посредством мошенничества, путем уничтожения, блокирования, модификации либо копирования цифровой информации или иного вмешательства в функционирование информационно-коммуникационных технологий.

2. Каждое Государство-участник может оставить за собой право считать хищение имущества, либо незаконного приобретения права на него, в том числе посредством мошенничества, с использованием информационно-коммуникационных технологий признаком, отягчающим наказание при совершении хищения в формах, определенных внутренним законодательством.

Статья 15
Преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием информационно-коммуникационных технологий

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству в случае совершения умышленно и неправомерно следующих деяний:

a) производство детской порнографической продукции в целях распространения через информационно-коммуникационные сети, включая сеть Интернет;

b) предложение или предоставление в пользование детской порнографии через информационно-коммуникационные сети, включая сеть Интернет;

c) распространение, передача, публичная демонстрация или рекламирование детской порнографии с использованием информационно-коммуникационных сетей, включая сеть Интернет;

d) приобретение детской порнографии посредством использования информационно-коммуникационных технологий для себя или для другого лица;

e) владение детской порнографией, находящейся в компьютерной системе или на электронно-цифровых носителях информации.

2. Для целей пункта 1 настоящей статьи в понятие «детская порнография» включаются порнографические материалы, изображающие:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

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

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

Для целей настоящей статьи термин «несовершеннолетние» означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

Статья 16
Склонение к самоубийству или доведение до его совершения

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству склонения к самоубийству или доведения до самоубийства, в том числе несовершеннолетних, совершенных посредством оказания психологического и иных видов воздействия в информационно-телекоммуникационных сетях, включая сеть Интернет.

Статья 17
Преступления, связанные с вовлечением несовершеннолетних к совершению противоправных действий, опасных для их жизни и здоровья

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству вовлечение несовершеннолетних посредством использования информационно-коммуникационных технологий в совершение противоправных деяний, представляющих опасность для их жизни, за исключением действий, предусмотренных статьей 16 настоящей Конвенции.

Статья 18
Создание и использование цифровой информации для введения пользователя в заблуждение

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству умышленного противоправного создания и использования цифровой информации, сходной до степени смешения с уже известной пользователю и вызывающей доверие информацией, повлекших причинение существенного ущерба.

2. Каждое Государство-участник может оставить за собой право считать такие деяния преступными, если они совершены в совокупности с иными преступлениями, предусмотренными внутренним законодательством такого Государства-участника, или содержали умысел совершения указанных преступлений.

Статья 19
Подстрекательство к подрывной или вооруженной деятельности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству, совершенных с использованием информационно-коммуникационных технологий призывов к проведению подрывных или вооруженных действий, направленных на насильственное изменение государственного строя другого государства.

Статья 20
Преступления, связанные с террористической деятельностью

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенные с использованием информационно-коммуникационных технологий призывов к осуществлению террористической деятельности, склонения, вербовки или иного вовлечения в нее, пропаганды и оправдания терроризма, сбора или предоставления средств для целей его финансирования.

Статья 21
Преступления, связанные с экстремистской деятельностью

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству распространения материалов, содержащих призывы к совершению противоправных деяний по мотивам политической, идеологической, социальной, расовой, национальной или религиозной ненависти и вражды, пропаганды или оправдания таких деяний, либо обеспечения доступа к ним, совершенных с использованием информационно-коммуникационных технологий.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству унижения лица или группы лиц по признакам расы, национальности, языка, происхождения, отношения к религии, совершенных с использованием информационно-коммуникационных технологий.

Статья 22
Преступления, связанные с распространением наркотических средств и психотропных веществ

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного умышленно, посредством использования информационно-коммуникационных технологий незаконного оборота наркотических средств и психотропных вещества также материалов, необходимых для их изготовления.

Статья 23
Преступления, связанные с незаконным оборотом оружия

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного умышленно, посредством использования информационно-коммуникационных технологий незаконного оборота оружия, боеприпасов, взрывных устройств и взрывчатых веществ.

Статья 24
Реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности

Каждое государство принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству, совершенного с использованием информационно-коммуникационных технологий умышленного распространения материалов, в которых отрицаются факты, одобряются или оправдываются действия, являющиеся геноцидом или преступлениями против мира и человечности, установленные приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 года.

Статья 25
Незаконное распространение фальсифицированных лекарственных средств и медицинских изделий

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного умышленно посредством использования информационно-коммуникационных технологий незаконного распространения фальсифицированных лекарственных средств и медицинских изделий.

Статья 26
Использование информационно-коммуникационных технологий для совершения деяний, признанных преступлениями в соответствии с международным правом

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству использования информационно-коммуникационных технологий с целью совершения какого-либо деяния, представляющего собой преступление, охватываемое каким-либо международным договором из перечисленных в Приложении[36] к настоящей Конвенции.

2. При сдаче на хранение своих ратификационных грамот или документов о принятии, утверждении или присоединении государство, не являющееся участником какого-либо из договоров, перечисленных в Приложении к настоящей Конвенции, может заявить, что при применении настоящей Конвенции к этому Государству-участнику считается, что этот договор не включен в упомянутое приложение. Такое заявление перестает действовать, как только этот договор вступает в силу для данного Государства-участника, которое уведомляет об этом факте депозитария.

3. Когда Государство-участник перестает быть стороной какого-либо из договоров, перечисленных в Приложении к настоящей Конвенции, оно может сделать, заявление в отношении этого договора (договоров), как это предусматривается в пункте 2 настоящей статьи.

Статья 27
Нарушение авторских и смежных прав с использованием информационно-коммуникационных технологий

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству нарушения авторских и смежных прав, как они определены в законодательстве этого Государства-участника, когда такие деяния совершаются умышленно с использованием информационно-коммуникационных технологий, включая незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, и присвоение авторства.

Статья 28
Соучастие в преступлении, приготовление к преступлению и покушение на преступление

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления в соответствии со своим внутренним законодательством приготовления и покушения на какое-либо преступление, признанное таковым в соответствии с положениями настоящей Конвенции.

2. Каждое Государство-участник рассматривает возможность принятия таких законодательных и иных мер, которые необходимы для признания в качестве преступления в соответствии со своим внутренним законодательством изготовления или приспособления лицом орудий и иных средств совершения преступления, вербовки соучастников преступления, сговора на совершение преступления либо иного умышленного создания условий для совершения преступления, предусмотренного настоящей Конвенцией, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

3. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы согласно его внутреннему законодательству, для установления ответственности, наряду с непосредственными исполнителями

[36] Примечание Секретариата: см. приложение к документу A/75/980.

какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, в отношении участвующих в его совершении организатора, подстрекателя или пособника, а также усиления ответственности за групповые преступления, включая организованные группы и преступные сообщества.

Статья 29
Иные противоправные деяния

Настоящая конвенция не является препятствием для признания Государством-участником в качестве преступления любого другого противоправного деяния, совершенного умышленно с использованием информационно-коммуникационных технологий и повлекшего существенный ущерб.

Статья 30
Ответственность юридических лиц

1. Каждое Государство-участник принимает такие законодательные и иные правовые меры, которые необходимы для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями и иными противоправными деяниями, признанными в качестве таковых в соответствии с настоящей Конвенцией, если эти деяния совершены в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

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

3. В зависимости от правовых принципов Государства-участника ответственность юридического лица может быть уголовной, гражданско-правовой или административной. Государство-участник обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности, эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, включая финансовые.

4. Привлечение к ответственности юридических лиц не исключает привлечения к ответственности физических лиц, совершивших преступление и иное противоправное деяние.

Южная Африка

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

Глава II. Криминализация

Статья 5. Незаконный доступ

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно и неправомерно, незаконный доступ ко всей

компьютерной системе или к любой ее части без соответствующих правовых оснований. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с намерением неправомерно завладеть компьютерными данными или с иным бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья 6. Незаконный перехват

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно и неправомерно, осуществляемый с помощью технических средств без правовых оснований перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья 7. Несанкционированное воздействие на цифровую информацию

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и неправомерно, противоправные повреждение, удаление, порча, изменение или подавление компьютерных данных.

2. Сторона может оставить за собой право потребовать, чтобы под такими преступлениями подразумевались описанные в пункте 1 деяния, приведшие к серьезному ущербу (физическим и юридическим лицам и экономике Государства-участника).

Статья 8. Воздействие на систему и нарушение функционирования информационно-коммуникационных сетей

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно и неправомерно и без законных оснований, создание серьезных препятствий функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Статья 9. Создание, использование и распространение устройств

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и неправомерно и без законных оснований:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного главным образом для целей совершения любого из преступлений, признанных таковыми в соответствии со статьями 5–26;

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части, с намерением использовать их для целей совершения

любого из преступлений, признанных таковыми в соответствии со статьями 5–26; и

b) владение предметом, указанным подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать его в целях совершения любого из преступлений, признанных таковыми в соответствии со статьями 5–26. Сторона может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми в соответствии со статьями 5–26 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может оставить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Статья 10. Подлог с использованием кибертехнологий

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и неправомерно и без законных оснований, ввод, изменение, удаление или подавление компьютерных данных, влекущие за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Сторона может потребовать, чтобы уголовная ответственность наступала при наличии намерения совершить обман или аналогичного бесчестного умысла.

Статья 11. Мошенничество с использованием кибертехнологий

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно и неправомерно и без законных оснований, лишение другого лица его имущества путем:

a) любого ввода, изменения, удаления или подавления компьютерных данных;

b) любого воздействия на функционирование компьютерной системы с мошенническим или бесчестным умыслом противозаконно извлечь экономическую выгоду для себя или для другого лица.

Статья 12. Преступления, связанные с материалами о сексуальных надругательствах над детьми

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и неправомерно:

a) производство материалов о сексуальных надругательствах над детьми в целях их распространения через компьютерную систему или с использованием информационно-коммуникационных технологий;

b) предложение или предоставление в пользование материалов о сексуальных надругательствах над детьми через компьютерную систему или с использованием информационно-коммуникационных технологий;

c) распространение или передачу материалов о сексуальных надругательствах над детьми через компьютерную систему или с использованием информационно-коммуникационных технологий;

d) приобретение материалов о сексуальных надругательствах над детьми через компьютерную систему или с использованием информационно-коммуникационных технологий для себя или для другого лица;

e) владение материалами о сексуальных надругательствах над детьми, размещенными в компьютерной системе или информационно-коммуникационных сетях или на компьютерном носителе данных.

2. Для целей пункта 1 выше в понятие «материалы о сексуальном насилии над детьми» включаются материалы, которые визуально изображают:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях; и

c) реалистические сцены участия несовершеннолетнего лица в откровенных сексуальных действиях.

3. Для целей пункта 2 выше термин «несовершеннолетний» означает любое лицо, не достигшее 18 лет. Однако Сторона может потребовать установления и более низких возрастных пределов, но не ниже 16 лет.

Статья 13. Преступления, связанные с нарушением авторских и смежных прав

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния в соответствии со своим внутренним законодательством и обязательствами, принятыми им согласно различным международным договорам и соглашениям, нарушение авторских прав, как они определены в законодательстве этого Государства, за исключением любых моральных прав, закрепленных в таких конвенциях, в случаях, когда такое деяние совершается умышленно, в коммерческих масштабах и с использованием компьютерной системы или информационно-коммуникационных технологий.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния в соответствии с его внутренним законодательством и обязательствами, принятыми им согласно Международной конвенции об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Римская конвенция), Соглашению по торговым аспектам прав интеллектуальной собственности и Договору ВОИС по исполнениям и фонограммам, нарушение смежных прав, как они определены в законодательстве этого Государства, за исключением любых моральных прав, закрепленных в таких конвенциях, в случаях, когда такое деяние совершается умышленно, в коммерческих масштабах и с помощью компьютерной системы или информационно-коммуникационных технологий.

3. Государство-участник может оставить за собой право не устанавливать уголовную ответственность на основании пунктов 1 и 2 настоящей статьи в ограниченных обстоятельствах при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не приводит к отступлению от международных обязательств этого Государства, изложенных в международных документах, упомянутых в пунктах 1 и 2 настоящей статьи.

Статья 14. Преступления, связанные с распространением наркотических средств и психотропных веществ

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяния, связанные с использованием информационно-коммуникационных технологий для содействия незаконному обороту наркотических средств, психотропных веществ и материалов, необходимых для их изготовления.

Статья 15. Защита лиц, сообщающих информацию

Каждое Государство-участник рассматривает возможность включения в свою внутреннюю правовую систему надлежащих мер для обеспечения защиты от любого несправедливого обращения любых лиц, добросовестно и на разумных основаниях сообщающих компетентным органам о любых фактах, касающихся использования информационно-коммуникационных технологий для совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

Каждое Государство-участник рассматривает возможность включения в свое внутреннее законодательство положений об освобождения от судебного преследования, при условии соблюдения стандартов/условий, принятых этим Государством, любого лица, которое всесторонне сотрудничает и проявляет добрую волю при взаимодействии с соответствующими правоохранительными органами.

Статья 16. Сотрудничество с правоохранительными органами

1. Каждое Государство-участник принимает надлежащие меры для того, чтобы поощрять лиц, которые участвуют или участвовали в совершении с использованием информационно-коммуникационных технологий какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, к добросовестному предоставлению информации, полезной для компетентных органов в проведении расследований и доказывании, и предоставлению компетентным органам фактической, конкретной помощи, которая может способствовать лишению преступников доходов от преступлений и принятию мер по возвращению таких доходов.

2. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть возможность смягчения, в надлежащих случаях, наказания обвиняемого лица, которое добросовестно существенным образом сотрудничает в расследовании и уголовном преследовании в связи с совершенным с использованием информационно-коммуникационных технологий преступлением, признанным таковым в соответствии с настоящей Конвенцией.

3. Каждое Государство-участник рассматривает вопрос о том, чтобы предусмотреть возможность, в соответствии с основополагающими принципами своего внутреннего законодательства, освобождения от судебного преследования лица, которое добросовестно существенным образом сотрудничает в расследовании или уголовном преследовании в связи с совершенным с использованием информационно-коммуникационных технологий преступлением, признанным таковым в соответствии с настоящей Конвенцией.

4. Защита таких лиц, mutatis mutandis, осуществляется в порядке, предусмотренном в статье 22 настоящей Конвенции.

5. В случаях, когда лицо, о котором говорится в пункте 1 настоящей статьи, может, находясь в одном Государстве-участнике, существенным образом сотрудничать с компетентными органами другого Государства-участника, эти Государства-участники могут в соответствии со своим внутренним законодательством рассмотреть возможность заключения соглашений или договоренностей

относительно возможного предоставления такому лицу другим Государством–участником режима, предусмотренного пунктами 2 и 3 настоящей статьи.

6. Каждое государство-участник в соответствии с основополагающими принципами своего внутреннего законодательства ведет реестр идентифицирующей информации обо всех регистраторах доменных имен, торговцах криптовалютными активами и криптовалютных активах, находящихся в его юрисдикции, и предоставляет такую информацию компетентным органам для целей проведения расследований и доказывания.

Статья 17. Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений, совершаемых с использованием информационно-коммуникационных технологий и признанных таковыми в соответствии с настоящей Конвенцией, когда:

a) преступление совершено на территории этого Государства-участника; или

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

2. При условии соблюдения статьи 4 настоящей Конвенции Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, совершаемого с использованием информационно-коммуникационных технологий, 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 с подпунктом (ii) пункта 1 (b) статьи 17 настоящей Конвенции, и совершено за пределами его территории с целью совершения какого-либо преступления с использованием информационно-коммуникационных технологий, признанного таковым в соответствии со статьей 15 настоящей Конвенции, на его территории; или

d) преступление совершено против этого Государства-участника или прямо влияет на дела такого 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, совершаемых с использованием информационно-коммуникационных технологий и признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории и оно не выдает такое лицо лишь на том основании, что оно является одним из его граждан.

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

5. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что 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 с целью координации своих действий.

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

Швейцария

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

2.2 Положения, касающиеся криминализации

a. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Незаконный доступ

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправный доступ ко всей компьютерной системе или к любой ее части. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с намерением завладеть компьютерными данными или с иным бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Незаконный перехват

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, осуществляемый с помощью технических средств противоправный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Воздействие на данные

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порчу, изменение или подавление компьютерных данных.

2. Сторона может оставить за собой право потребовать, чтобы под такими преступлениями подразумевались описанные в пункте 1 деяния, приведшие к серьезному ущербу.

Воздействие на систему

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно

совершается умышленно, противоправное создание серьезных препятствий функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Неправомерное использование устройств

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного главным образом для целей совершения любого из преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции, касающимися незаконного доступа, незаконного перехвата, воздействия на данные или воздействия на систему;

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части, с намерением использовать их для целей совершения любого из преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции, касающимися незаконного доступа, незаконного перехвата, воздействия на данные или воздействия на систему; и

b) владение предметом, указанным в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать его в целях совершения любого из преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции, касающимися незаконного доступа, незаконного перехвата, воздействия на данные или воздействия на систему. Сторона может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции, касающимися незаконного доступа, незаконного перехвата, воздействия на данные или воздействия на систему, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может оставить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

b. Преступления, связанные с использованием компьютерных средств

Подлог с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно, ввод, изменение, удаление или подавление компьютерных данных, влекущие за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Сторона может

потребовать, чтобы уголовная ответственность наступала при наличии намерения совершить обман или аналогичного бесчестного умысла.

Мошенничество с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное лишение другого лица его имущества путем:

a) любого ввода, изменения, удаления или подавления компьютерных данных;

b) любого воздействия на функционирование компьютерной системы с мошенническим или бесчестным умыслом извлечь в нарушение установленных прав экономическую выгоду для себя или для другого лица.

c. Преступления, связанные с содержанием данных

Преступления, связанные с материалами о сексуальной эксплуатации детей и сексуальных надругательствах над детьми

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) производство материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми в целях их распространения через компьютерную систему;

b) предложение или предоставление в пользование через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми;

c) распространение или передачу через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми;

d) приобретение через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми для себя или для другого лица;

e) владение материалами с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми, размещенными в компьютерной системе или на компьютерном носителе данных.

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

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

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

c) реалистические сцены участия несовершеннолетнего лица в откровенных сексуальных действиях.

3. Для целей пункта 2 выше термин «несовершеннолетний» означает любое лицо, не достигшее 18 лет. Однако Сторона может потребовать установления и более низких возрастных пределов, но не ниже 16 лет.

4. Каждая Сторона может оставить за собой право не применять, полностью или частично, подпункты (d) и (e) пункта 1 и подпункты (b) и (c) пункта 2.

d. Дополнительная ответственность и санкции

Покушение и пособничество или подстрекательство

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, пособничество совершению любого из преступлений, признанных таковыми в соответствии с положениями настоящей Конвенции, касающимися криминализации, или подстрекательство к нему с умыслом совершить такое преступление.

2. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, покушение на совершение любого из преступлений, признанных таковыми в соответствии с положениями о настоящей Конвенции, касающимися криминализации.

3. Каждая Сторона может оставить за собой право не применять, полностью или частично, положения пункта 2 настоящей статьи.

Ответственность юридических лиц

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться для обеспечения возможности привлечения к ответственности юридических лиц в связи с уголовным преступлением, признанным таковым в соответствии с положениями настоящей Конвенции, касающимися криминализации, если оно совершено в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, предусмотренным пунктом 1 настоящей статьи, каждая Сторона принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение уголовного преступления, признанного таковым согласно настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от правовых принципов Сторон ответственность юридических лиц может быть уголовной, гражданско-правовой или административной.

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

Санкции и меры

1. Каждая Сторона принимает такие законодательные и другие меры, которые могут потребоваться для обеспечения возможности применения в связи с уголовными преступлениями, признанные таковыми в соответствии с положениями настоящей Конвенции, касающимися криминализации, эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, включая лишение свободы.

2. Каждая Сторона обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии с положением настоящей Конвенции, касающимися ответственности юридических лиц, эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций или мер, включая денежные санкции.

Соединенное Королевство Великобритании и Северной Ирландии

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

Глава — Криминализация

Киберзависимые преступления

Соединенное Королевство считает, что Конвенция должна включать положения о киберзависимых преступлениях с такими описаниями и определениями, которые будут приемлемы для всех сторон и будут соответствовать существующим международным соглашениям в этой области.

Статья 5
Незаконный доступ

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправный доступ ко всей компьютерной системе или к любой ее части. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с намерением завладеть компьютерными данными или с иным бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья 6
Незаконный перехват

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, осуществляемый с помощью технических средств противоправный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Сторона может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

Статья 7
Воздействие на данные

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порчу, изменение или подавление компьютерных данных.

2. Сторона может оставить за собой право потребовать, чтобы под такими преступлениями подразумевались описанные в пункте 1 деяния, приведшие к серьезному ущербу.

Статья 8
Воздействие на систему

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное создание серьезных препятствий функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

Статья 9
Неправомерное использование устройств

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного главным образом для целей совершения любого из преступлений, признанных таковыми согласно соответствующим разделам;

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части, с намерением использовать их для целей совершения любого из преступлений, признанных таковыми в соответствии с положениями других четырех статей настоящего раздела; и

b) владение предметом, указанным в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать его в целях совершения любого из преступлений, признанных таковыми в соответствии с положениями других четырех статей настоящего раздела. Сторона может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми в соответствии с положениями статей, касающихся незаконного доступа, незаконного перехвата, воздействия на данные и воздействия на систему, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждая Сторона может оставить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

Преступления, совершаемые посредством кибертехнологий

Соединенное Королевство также считает, что положения, касающиеся преступлений, совершаемых посредством кибертехнологий, должны быть включены применительно к случаям, когда такие преступления совершаются в основном в сети Интернет, когда масштаб и скорость совершения таких преступлений изменяются с помощью компьютеров и когда определения таких преступлений понимаются всеми сторонами одинаково.

Статья 10
Мошенничество

Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния общий состав преступления мошенничества, когда оно совершается полностью или частично в сети Интернет. Такой состав преступления включает, хотя и не только, действия, совершаемые внутри страны и за ее пределами с помощью сети Интернет или других киберзависимых/цифровых средств с использованием следующих методов:

a) мошенничество посредством умышленного введения в заблуждение;

b) мошенничество посредством непредоставления информации;

c) мошенничество посредством злоупотребления служебным положением с обманным или бесчестным умыслом причинить другому лицу убыток или получить для другого лица финансовую выгоду или другое имущество.

Статья 11
Преступления, связанные с сексуальной эксплуатацией детей и сексуальными надругательствами над детьми в сети Интернет, включая оборот материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми и завлечение детей через сеть Интернет

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно и противоправно:

a) производство материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми в целях их распространения через компьютерную систему;

b) предложение или предоставление в пользование через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми;

c) распространение или передача через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми;

d) приобретение через компьютерную систему материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми для себя или для другого лица;

e) владение материалами с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми, размещенными в компьютерной системе или на компьютерном носителе данных;

f) просмотр материалов с изображением сексуальной эксплуатации детей и сексуальных надругательств над детьми, размещенных в компьютерной системе или на компьютерном носителе данных.

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

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

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

c) реалистические сцены участия несовершеннолетнего лица в откровенных сексуальных действиях;

d) в любом виде половые органы несовершеннолетнего лица, главным образом в сексуальных целях.

3. Для целей пункта 2 выше термин «несовершеннолетний» означает любое лицо, не достигшее 18 лет. Однако Сторона может потребовать установления и более низких возрастных пределов, но не ниже 16 лет.

4. Каждая Сторона может оставить за собой право не применять, полностью или частично, подпункты (d) и (e) пункта 1 и подпункты (b) и (c) пункта 2.

Статья 12
Преступления, связанные с нарушением авторских и смежных прав

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния согласно ее внутреннему законодательству и обязательствам, принятым ею в соответствии с Парижским актом от 24 июля 1971 года, касающимся Бернской конвенции по охране литературных и художественных произведений, Соглашением по торговым аспектам прав интеллектуальной собственности и Договором Всемирной организации интеллектуальной собственности (ВОИС) по авторскому праву, нарушение авторских прав, как они определены в законодательстве этой Стороны, за исключением любых моральных прав, закрепленных в таких конвенциях, когда такое деяние совершается умышленно, в коммерческих масштабах и с помощью компьютерной системы.

2. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния согласно ее внутреннему законодательству и обязательствам, принятым ею в соответствии с Международной конвенцией об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Римская конвенция), Соглашением по торговым аспектам прав интеллектуальной собственности и Договором ВОИС по исполнениям и фонограммам, нарушение смежных прав, как они определены в законодательстве этой Стороны, за исключением любых моральных прав, закрепленных в таких конвенциях, когда такое деяние совершается умышленно, в коммерческих масштабах и с помощью компьютерной системы.

3. Сторона может оставить за собой право не устанавливать уголовную ответственность на основании пунктов 1 и 2 настоящей статьи в ограниченных обстоятельствах при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не приводит к отступлению от международных обязательств этой Стороны, изложенных в международных документах, упомянутых в пунктах 1 и 2 настоящей статьи.

Статья 13
Покушение, пособничество и подстрекательство

1. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемых деяний, когда они совершаются умышленно, пособничество совершению любого из преступлений, признанных таковыми в соответствии с [настоящей Конвенцией], или подстрекательство к нему с умыслом совершить такое преступление.

2. Каждая Сторона принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовно наказуемого деяния, когда оно совершается умышленно, покушение на совершение любого из преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

3. Каждая Сторона может оставить за собой право не применять, полностью или частично, положения пункта 2 настоящей статьи.

Статья 14
Преследование, вынесение судебного решения и санкции

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

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

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

4. Каждая Сторона обеспечивает, чтобы ее суды или другие компетентные органы учитывали опасный характер преступлений, охватываемых настоящей Конвенцией, при рассмотрении вопроса о возможности досрочного или условного освобождения лиц, осужденных за такие преступления.

5. Каждая Сторона в надлежащих случаях устанавливает согласно своему внутреннему законодательству длительный срок давности для возбуждения уголовного преследования за любое преступление, охватываемое настоящей Конвенцией, и более длительный срок давности в тех случаях, когда лицо, подозреваемое в совершении преступления, уклоняется от правосудия.

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

Статья 15
Юрисдикция

1. Каждая Сторона принимает такие меры, какие могут потребоваться для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда:

a) преступление совершено на территории этой Стороны; или

b) преступление совершено на борту судна, которое несло флаг этой Стороны в момент совершения преступления, или воздушного судна, которое зарегистрировано в соответствии с законодательством этой Стороны в такой момент.

2. При условии соблюдения соответствующих статей настоящей Конвенции Сторона может также установить свою юрисдикцию в отношении любого такого преступления, когда:

a) преступление совершено против гражданина этой Стороны; или

b) преступление совершено гражданином этой Стороны или лицом без гражданства, которое обычно проживает на ее территории; или

c) преступление совершено против этой Стороны.

3. Для целей любой статьи настоящей Конвенции, касающейся выдачи, каждая Сторона принимает такие меры, какие могут потребоваться для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на ее территории и она не выдает такое лицо лишь на том основании, что оно является одним из ее граждан.

4. Каждая Сторона может также принять такие меры, какие могут потребоваться для установления своей юрисдикции в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на ее территории и она не выдает его.

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 с целью координации своих действий.

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

Дополнительные замечания

Соединенное Королевство считает, что использование цифровых технологий для общения с несовершеннолетним, когда это общение носит сексуальный характер или осуществляется с намерением побудить несовершеннолетнего к сексуальному общению или сексуальным действиям и когда это общение имеет целью получение сексуального удовлетворения, должно быть криминализировано, и мы предоставим соответствующий текст в ходе переговоров.

Торговля женщинами и девочками и их сексуальная эксплуатация — это преступления, имеющие особо тяжкие последствия, и соответствующие жертвы в период их эксплуатации подвергаются многочисленным актам насилия, что причиняет им огромные физические и эмоциональные страдания. Поскольку такая эксплуатация в значительной мере организуется и обеспечивается через сеть Интернет, эта проблема приобрела глобальный характер, и Соединенное Королевство считает, что нам необходим единый подход к устранению данной угрозы. Соединенное Королевство поддерживает включение в настоящую Конвенцию положения о криминализации современного рабства и торговли людьми, включая торговлю людьми и сексуальную эксплуатацию через веб-сайты интим-услуг (ВСИУ).

Соединенное Королевство считает, что вред от несанкционированного обмена интимными изображениями требует от нас скоординированного подхода к предотвращению подобных нарушений, включая удаление таких изображений и обеспечение того, чтобы в отношении тех, кто обменивается несанкционированными изображениями, действовали эффективные меры наказания. Соединенное Королевство хотело бы включить положения, направленные на борьбу с этим вредом.

Объединенная Республика Танзания

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

4. Криминализация

В последнее время наблюдается стремительный рост использования информационно-коммуникационных технологий в преступных целях группами преступников по всему миру, что обусловлено соответствующими технологическими достижениями.

4.1. Перечень преступлений

С учетом неотложного характера этой проблемы Объединенная Республика Танзания считает необходимым, чтобы каждое Государство-участник приняло такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых преступлений, когда они совершаются умышленно и преднамеренно, следующие деяния, хотя их перечень может быть расширен:

a) незаконный доступ;

b) незаконный перехват;

c) незаконное уничтожение электронных данных и компьютерных систем;

d) шпионаж в целях получения данных;

e) незаконное воздействие на систему;

f) владение незаконными устройствами и/или программами в целях совершения преступлений;

g) подлог и мошенничество с использованием компьютерных технологий;

h) порнография и детская порнография;

i) преступления, связанные с использованием персональных данных;

(j) публикация ложной информации;

k) оборот материалов расистского и ксенофобского характера;

l) геноцид и преступления против человечности;

m) кибертравля;

n) покушение, пособничество и подстрекательство;

o) участие в организованной преступной группе.

4.2. Корпоративная ответственность

Объединенная Республика Танзания предлагает, чтобы Конвенция обязывала Государства-члены включить в их внутреннее законодательство положения, устанавливающие ответственность юридических лиц в связи с преступлениями, признанными таковыми согласно настоящей Конвенции. Ответственность может распространяться и на физических лиц, действующих как по поручению корпоративного юридического лица, так и якобы от его имени.

Соединенные Штаты Америки

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

Криминализация

Криминализация киберпреступлений

«Незаконный доступ»

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправный доступ ко всей компьютерной системе или к любой ее части. Государство-участник может потребовать, чтобы такое деяние считалось преступным, если оно совершается с нарушением мер безопасности, с намерением завладеть компьютерными данными или с иным бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

«Незаконный перехват»

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, осуществляемый с помощью технических средств противоправный перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Государство-участник может потребовать, чтобы такое деяние считалось преступным, если оно совершается с бесчестным умыслом или в отношении компьютерной системы, которая соединена с другой компьютерной системой.

«Воздействие на данные»

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно, противоправные повреждение, удаление, порчу, изменение или подавление компьютерных данных.

2. Государство-участник может оставить за собой право потребовать, чтобы под такими преступлениями подразумевались описанные в пункте 1 деяния, приведшие к серьезному ущербу.

«Воздействие на систему»

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное создание серьезных препятствий функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

«Неправомерное использование устройств»

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно:

а) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройства, включая компьютерную программу, разработанного или адаптированного главным образом для целей совершения любого из преступлений, признанных таковыми в соответствии с предыдущими статьями настоящей главы;

ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части,

с намерением использовать их для целей совершения любого из преступлений, признанных таковыми в соответствии с предыдущими статьями настоящей главы; и

b) владение предметом, указанным в подпункте (i) или (ii) пункта 1 (a) выше, с намерением использовать его в целях совершения любого из преступлений, признанных таковыми в соответствии с предыдущими статьями настоящей главы. Государство-участник может потребовать в законодательном порядке, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, распространение или иная форма предоставления в пользование или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми в соответствии с предыдущими статьями настоящей главы, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Каждое Государство-участник может оставить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления в пользование предметов, указанных в подпункте (ii) пункта 1 (a) настоящей статьи.

«Подлог с использованием компьютерных технологий»

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются умышленно и противоправно, ввод, изменение, удаление или подавление компьютерных данных, влекущие за собой изменение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Государство-участник может потребовать, чтобы уголовная ответственность наступала при наличии намерения совершить обман или аналогичного бесчестного умысла.

«Мошенничество с использованием компьютерных технологий»

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния, когда оно совершается умышленно, противоправное лишение другого лица его имущества путем:

a) любого ввода, изменения, удаления или подавления компьютерных данных;

b) любого воздействия на функционирование компьютерной системы;

с мошенническим или бесчестным умыслом противозаконно извлечь экономическую выгоду для себя или для другого лица.

«Преступления, связанные с использованием компьютерных технологий для оборота материалов о сексуальных надругательствах над детьми»

1. Каждое Государство-участник принимает необходимые законодательные или другие меры, с тем чтобы обеспечить криминализацию следующих деяний, когда они совершаются сознательно с использованием компьютерной системы:

a) производство материалов о сексуальных надругательствах над детьми;

b) организацию прямой трансляции участия ребенка в откровенных сексуальных действиях;

c) предложение или предоставление в пользование материалов о сексуальных надругательствах над детьми;

d) распространение или передачу материалов о сексуальных надругательствах над детьми;

e) приобретение материалов о сексуальных надругательствах над детьми для себя или для другого лица;

f) владение материалами о сексуальных надругательствах над детьми;

g) сознательное получение с помощью информационно-коммуникационных технологий доступа к материалам о сексуальных надругательствах над детьми или просмотр прямой трансляции участия ребенка в откровенных сексуальных действиях.

2. Каждое Государство-участник принимает необходимые законодательные или другие меры для криминализации сознательных деяний, совершаемых с помощью информационно-коммуникационных технологий в целях подстрекательства, склонения, привлечения или принуждения ребенка или лица, которое считается ребенком, к участию в любых незаконных сексуальных действиях. Каждое Государство-участник принимает такие законодательные или другие меры, которые необходимы для обеспечения того, чтобы его национальное законодательство не требовало в качестве условия для криминализации указанных деяний, чтобы они совершались во время личной встречи между взрослым лицом и ребенком.

«Преступления, связанные с использованием компьютерных технологий для нарушения авторских и смежных прав»

1. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния согласно обязательствам, принятым им в соответствии с Парижским актом от 24 июля 1971 года, касающимся Бернской конвенции по охране литературных и художественных произведений, Соглашением по торговым аспектам прав интеллектуальной собственности и Договором Всемирной организации интеллектуальной собственности (ВОИС) по авторскому праву, нарушение авторских прав, как они определены в законодательстве этого Государства-участника, за исключением любых моральных прав, закрепленных в таких конвенциях, когда такое деяние совершается умышленно, в коммерческих масштабах и с помощью компьютерной системы.

2. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемого деяния согласно его внутреннему законодательству и обязательствам, принятым им в соответствии с Международной конвенцией об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Римская конвенция), Соглашением по торговым аспектам прав интеллектуальной собственности и Договором ВОИС по исполнениям и фонограммам, нарушение смежных прав, как они определены в законодательстве этого Государства-участника, за исключением любых моральных прав, закрепленных в таких

конвенциях, когда такое деяние совершается умышленно, в коммерческих масштабах и с помощью компьютерной системы.

3. Государство-участник может оставить за собой право не устанавливать уголовную ответственность на основании пунктов 1 и 2 настоящей статьи в ограниченных обстоятельствах при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не приводит к отступлению от международных обязательств этого Государства-участника, изложенных в международных документах, упомянутых в пунктах 1 и 2 настоящей статьи.

«Участие и покушение»[37]

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

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

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

Ответственность юридических лиц[38]

1. Каждое Государство-участник принимает такие меры, какие с учетом его правовых принципов могут потребоваться для установления ответственности юридических лиц за участие в преступлениях, признанных таковыми в соответствии со статьями настоящей Конвенции, касающимися криминализации.

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

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

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

Преследование, вынесение судебного решения и санкции[39]

1. Каждое Государство-участник за совершение какого-либо преступления, признанного таковым в соответствии со статьями настоящей Конвенции, касающимися криминализации, предусматривает применение таких уголовных санкций, которые учитывают степень опасности этого преступления.

---

[37] Конвенция Организации Объединенных Наций против коррупции, статья 27.

[38] Конвенция Организации Объединенных Наций против транснациональной организованной преступности, статья 10, и Конвенция Организации Объединенных Наций против коррупции, статья 26.

[39] Конвенция Организации Объединенных Наций против транснациональной организованной преступности, статья 11.

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

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

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

5. Каждое Государство-участник в надлежащих случаях устанавливает согласно своему внутреннему законодательству длительный срок давности для возбуждения уголовного преследования за любое преступление, охватываемое настоящей Конвенцией, и более длительный срок давности в тех случаях, когда лицо, подозреваемое в совершении преступления, уклоняется от правосудия.

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

Криминализация отмывания доходов от киберпреступлений[40]

1. Каждое Государство-участник принимает в соответствии с основополагающими принципами своего внутреннего законодательства такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно:

a) i) конверсию или перевод имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника этого имущества или в целях оказания помощи любому лицу, участвующему в совершении основного правонарушения, с тем чтобы оно могло уклониться от ответственности за свои деяния;

ii) сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежность, если известно, что такое имущество представляет собой доходы от преступлений;

b) при условии соблюдения основных принципов своей правовой системы:

[40] Адаптировано на основе статьи 6 Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

i) приобретение, владение или использование имущества, если в момент его получения известно, что такое имущество представляет собой доходы от преступлений;

ii) участие, причастность или вступление в сговор с целью совершения любого из преступлений, признанных таковыми в соответствии с настоящей статьей, покушение на его совершение, а также пособничество, подстрекательство, содействие или дача советов при его совершении.

2. Для целей осуществления или применения пункта 1 настоящей статьи:

a) каждое Государство-участник включает в число основных правонарушений преступления, признанные таковыми в соответствии со статьями настоящей Конвенции, касающимися криминализации. В случае, когда законодательство Государств-участников содержит перечень конкретных основных правонарушений, они включают в него как минимум преступления, указанные в настоящей Конвенции;

b) для целей подпункта (b) основные правонарушения включают преступления, совершенные как в пределах, так и за пределами юрисдикции соответствующего Государства-участника. Однако преступления, совершенные за пределами юрисдикции какого-либо Государства-участника, представляют собой основные правонарушения только при условии, что соответствующее деяние является уголовно наказуемым согласно внутреннему законодательству государства, в котором оно совершено, и было бы уголовно наказуемым согласно внутреннему законодательству Государства-участника, в котором осуществляется или применяется настоящая статья, если бы оно было совершено в нем;

c) каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам или их описание;

d) если этого требуют основополагающие принципы внутреннего законодательства Государства-участника, то можно предусмотреть, что преступления, указанные в пункте 1 настоящей статьи, не относятся к лицам, совершившим основное правонарушение;

e) осознание, умысел или цель как элементы состава преступления, указанного в пункте 1 настоящей статьи, могут быть установлены из объективных фактических обстоятельств дела.

Криминализация воспрепятствования осуществлению правосудия[41]

Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых следующие деяния, когда они совершаются умышленно:

a) применение физической силы, угроз или запугивания или обещание, предложение или предоставление неправомерного преимущества с целью склонения к даче ложных показаний или вмешательства в процесс дачи показаний или представления доказательств в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией;

b) применение физической силы, угроз или запугивания с целью вмешательства в выполнение должностных обязанностей должностным лицом судебного или правоохранительного органа в ходе производства в связи с совершением преступлений, охватываемых настоящей Конвенцией. Ничто в настоящем подпункте не наносит ущерба праву Государств-участников иметь законодательство, обеспечивающее защиту других категорий публичных должностных лиц.

[41] Конвенция Организации Объединенных Наций против транснациональной организованной преступности, статья 23.

Венесуэла (Боливарианская Республика)

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

5. Криминализация

В Конвенции можно было бы закрепить обязательство Государств-участников установить уголовную и другую ответственность за соответствующие преступления, с тем чтобы охватить широкий спектр неправомерных деяний, связанных с использованием информационно-коммуникационных технологий, в тех ситуациях, когда деяния, определенные в Конвенции, еще не признаны в качестве преступлений согласно их внутреннему законодательству. При этом в одних случаях можно было бы возложить на Государства юридическое обязательство ввести ответственность за преступления, а в других случаях, с тем чтобы учесть различия в национальном законодательстве, можно было бы обязать их разработать соответствующие законодательные акты.

Исходя из этого, следует четко определить, какие уголовные деяния, совершаемые с использованием информационно-коммуникационных технологий, широко признаются таковыми в международном сообществе. Конвенция должна обеспечить перспективную основу для координации усилий в таких областях, как криминализация, удовлетворение текущих и будущих потребностей развития информационно-коммуникационных технологий и борьба с преступностью.

С учетом вышеизложенного каждому Государству-участнику следует принять такие законодательные, директивные и другие меры, какие могут потребоваться, с тем чтобы признать указанные преступления уголовно наказуемыми. В связи с этим Конвенция должна содержать положения, обеспечивающие, чтобы государства, которым необходимо адаптировать свое национальное законодательство и свои национальные программы, имели время для того, чтобы сделать это, и могли получить необходимую поддержку.

В число основных правонарушений, которые должны быть охвачены Конвенцией, следует включить:

- несанкционированный доступ к цифровой информации, когда такой доступ влечет за собой уничтожение, блокирование или модификацию этой информации;
- преднамеренный перехват цифровой информации без надлежащей санкции и/или в нарушение установленных норм, в том числе с использованием технических средств, с целью перехвата технических параметров трафика и не предназначенных для общего пользования компьютерных данных, обрабатываемых с помощью информационно-коммуникационных технологий;
- неправомерное манипулирование цифровой информацией посредством ее повреждения, удаления, изменения, блокирования или модификации;
- преднамеренные неправомерные деяния, преследующие цель нарушить функционирование информационно-коммуникационных сетей и влекущие или порождающие риск серьезных последствий;
- использование и распространение вредоносных программ, предназначенных для несанкционированных уничтожения, блокирования, модификации или распространения цифровой информации или для нейтрализации средств защиты;
- умышленное преднамеренное создание, распространение и/или использование компьютерных программ или другой цифровой информации в целях незаконного манипулирования критической информационной инфраструктурой, в том числе для уничтожения, блокирования или модификации содержащейся в ней информации или нейтрализации средств защиты;

- умышленное создание, распространение и/или использование компьютерной программы или другой цифровой информации, заведомо предназначенной для неправомерного воздействия на критическую информационную инфраструктуру, включая компьютерную программу или другую цифровую информацию, предназначенную для уничтожения, блокирования, модификации или копирования содержащейся в ней информации или нейтрализации средств защиты;
- нарушение правил эксплуатации средств, используемых для хранения, обработки и передачи защищенной цифровой информации, содержащейся в критической информационной инфраструктуре, или информационных систем или информационно-коммуникационных сетей, относящихся к критической информационной инфраструктуре, или нарушение правил доступа к ним, если такое нарушение приводит к повреждению критической информационной инфраструктуры;
- хищение имущества или незаконное приобретение прав собственности, в том числе мошенническим путем, посредством уничтожения, блокирования или модификации цифровой информации или иного воздействия на функционирование информационно-коммуникационных технологий;
- совершение с использования информационно-коммуникационных технологий призывов к проведению подрывных или вооруженных действий, направленных на насильственное свержение правительства другого государства;
- совершение с использованием информационно-коммуникационных технологий призывов к склонению, вербовке или иному вовлечению в террористическую деятельность, пропаганде и оправданию терроризма, а также к сбору или предоставлению средств для целей его финансирования;
- незаконный оборот наркотических средств и психотропных веществ и препаратов, необходимых для их производства, с использованием информационно-коммуникационных технологий;
- незаконный оборот оружия, боеприпасов, взрывных устройств и взрывчатых веществ с использованием информационно-коммуникационных технологий;
- несанкционированный доступ к персональным данным в целях их уничтожения, модификации, копирования или распространения;
- преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершаемые с использованием информационно-коммуникационных технологий;
- преступления, связанные с вовлечением несовершеннолетних в совершение противоправных действий, опасных для их жизни и здоровья.

Вьетнам

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

Глава II. Криминализация

5. Каждое Государство-участник принимает такие законодательные и другие меры, какие могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых деяний, когда они совершаются несанкционированно и умышленно:

a) изготовление технических средств, оборудования или компьютерных программ, а также торговля ими и их передача в целях совершения атаки на компьютерную сеть, телекоммуникационную сеть или электронное устройство, с тем чтобы использовать их для преступной деятельности, указанной в настоящей Конвенции;

b) распространение компьютерной программы, наносящей вред компьютерной сети, телекоммуникационной сети или электронному устройству;

c) удаление, саботаж или модификация компьютерной программы или цифровых данных;

d) воспрепятствование передаче данных компьютерной сети, телекоммуникационной сети или электронного устройства;

e) воспрепятствование нормальному функционированию компьютерной сети, телекоммуникационной сети или электронного устройства или создание помех их нормальному функционированию;

f) установление контроля над функционированием электронного устройства или вмешательство в его функционирование путем обхода системы безопасности или защиты, нарушения прав другого лица на управление этим устройством или любым другим способом;

g) кража, модификация, саботаж или фальсификация информации или данных;

h) использование компьютерной сети, телекоммуникационной сети или электронного устройства в следующих целях:

i) использование информации о банковском счете или банковской карте организации или физического лица с целью незаконного присвоения активов;

ii) изготовление поддельных банковских карт, а также владение и торговля такими картами или их использование с целью незаконного присвоения активов;

iii) получение несанкционированного доступа к счетам государственных учреждений, организаций и частных лиц с целью незаконного присвоения активов;

iv) совершение мошеннических действий в сферах электронной торговли, электронных платежей, торговли валютой через сеть Интернет, финансовых инвестиций через сеть Интернет, многоуровневого маркетинга или торговли ценными бумагами через сеть Интернет с целью незаконного присвоения имущества;

v) несанкционированное создание или предоставление телекоммуникационных или интернет-услуг с целью присвоения имущества;

i) сбор информации о банковских счетах физических лиц и организаций, а также владение и торговля такой информацией, ее передача или предание гласности;

j) торговля конфиденциальной информацией государственных учреждений, организаций или частных лиц, а также передача, модификация и предание гласности такой информации без согласия ее владельцев;

k) использование киберпространства, информационных технологий или электронных устройств для совершения террористического акта или финансирования терроризма.

6. Ничто в настоящей Конвенции не препятствует Государствам-членам принимать такие законодательные и другие меры, какие могут потребоваться для признания в качестве уголовных преступлений любых других деяний,

связанных с использованием информационно-коммуникационных технологий в преступных целях.

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