Организация Объединенных Наций A/AC.291/4

Генеральная Ассамблея

Distr.: General
17 November 2021
Russian
Original: Arabic/Chinese/English/
Spanish

Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

Подборка мнений, представленных государствами-членами, относительно сферы применения, целей и структуры (элементов) всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

Записка Секретариата

Резюме

Настоящая записка подготовлена Секретариатом в рамках подготовки к первой сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях по поручению Председателя Комитета. В ней изложены мнения, полученные от государств-членов, относительно сферы применения, целей и структуры (элементов) новой конвенции.

V.21-08422 (R) 141221 130122

Содержание

I. Введение

1. В рамках подготовки к первой сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях Председатель Комитета г-жа Фаузия Бумайза Мебарки (Алжир) 11 августа 2021 года предложила государствам-членам представить свои мнения относительно сферы применения, целей и структуры (элементов) новой конвенции. Крайний срок для представления мнений, установленный на 29 октября 2021 года, был впоследствии продлен до 5 ноября 2021 года.

2. Председатель также поручил Секретариату составить подборку полученных мнений и перевести их на шесть официальных языков Организации Объединенных Наций для представления Специальному комитету на его первой сессии.

3. Настоящая записка подготовлена Секретариатом по поручению Председателя и содержит полученные от государств-членов мнения относительно сферы применения, целей и структуры (элементов) новой конвенции.

II. Ответы, полученные от государств-членов

Австралия

[Подлинный текст на английском языке]
[29 октября 2021 года]

Австралия приветствует возможность высказать свое мнение относительно сферы применения, структуры и целей новой международной конвенции о киберпреступности. Новая конвенция предлагает уникальную возможность достичь широкого консенсуса по вопросам международного сотрудничества в области противодействия киберпреступности, позволяющего государствам эффективнее бороться с этой распространенной и постоянно растущей угрозой.

Новая конвенция будет иметь ценность только в том случае, если сможет заручиться широкой поддержкой большинства государств-членов на основе консенсуса, достигнутого в результате честного обсуждения под эгидой Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, который был учрежден в соответствии с резолюциями 74/247 и 75/282 Генеральной Ассамблеи. В этой связи Австралия привержена открытому, инклюзивному, прозрачному и многостороннему процессу, который с наибольшей вероятностью позволит государствам прийти к результату, приемлемому для как можно большего числа государств. Это соответствует принципам, изложенным в материалах, прежде представленных Австралией Специальному комитету, а также в совместных представлениях с участием Австралии. Австралия пользуется случаем, чтобы повторить соображения, сформулированные в этих материалах.

Киберпреступность представляет угрозу всем государствам, но особые проблемы создает для малых государств. Эффективное международное сотрудничество по проблеме киберпреступности особенно важно для малых островных развивающихся государств, поскольку способствует укреплению их внутренних возможностей бороться с транснациональной киберпреступностью. Крайне важно, чтобы малые островные развивающиеся государства могли конструктивно участвовать в работе Специального комитета. Австралия привержена обеспечению того, чтобы у тихоокеанских островных стран были адекватные возможности для участия в работе Специального комитета. Австралия приветствует решение поддержать гибридное (в очной форме и онлайн) участие в

сессиях Специального комитета и подчеркивает важность обеспечения адекватного времени на подготовку и участие для небольших делегаций.

Организации частного сектора играют уникальную и неоценимую роль в борьбе с киберпреступностью. Поэтому для достижения успеха Специальному комитету в своей работе необходимо учитывать ценные экспертные знания и опыт, которыми делятся представители отрасли. Государствам также следует учитывать обширные профессиональные знания и опыт, которые другие негосударственные субъекты, такие как организации гражданского общества, академические круги и межправительственные органы, могут внести в обсуждение того, как лучше бороться с киберпреступностью. Чтобы обеспечить обсуждения на основе досконального знания темы и добиться эффективных результатов, Специальному комитету следует предоставлять этим группам как можно больше возможностей внести свой вклад.

Сфера применения

Переговоры должны пройти в сжатые сроки, и поэтому государства располагают ограниченным временем для достижения согласия по многим вопросам, составляющим новую конвенцию. Необходимо четко определить сферу применения конвенции, которая должна быть посвящена реагированию систем уголовного правосудия на киберпреступность. Она не должна затрагивать более широкие вопросы кибербезопасности, которые рассматриваются на других площадках.

Для ускорения работы государствам следует сосредоточить внимание на областях, требующих применения общих подходов к киберпреступности. В работе Специального комитета следует использовать такие концепции и терминологию, имеющие отношение к киберпреступности и международному сотрудничеству в области уголовного правосудия, которые уже хорошо понятны международному сообществу. Нам не нужно заново «изобретать велосипед», равно как и порождать неясность.

Таким образом, новая конвенция должна в значительной мере опираться на Конвенцию Организации Объединенных Наций против транснациональной организованной преступности и Конвенцию Организации Объединенных Наций против коррупции, а также на другие концепции, которые были согласованы консенсусом на конгрессах Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и на других форумах Организации Объединенных Наций, в зависимости от обстоятельств. Она должна учитывать эффективно действующие международные документы, уже принятые государствами на международном и региональном уровнях, такие как Конвенция Совета Европы о киберпреступности, и не должна подрывать существующие нормы, установленные в этих соглашениях. Это соответствует мандату, изложенному в резолюции 74/247 Генеральной Ассамблеи, в которой она призвала Специальный комитет в его работе в полной мере учитывать существующие международные документы и усилия, предпринимаемые на национальном, региональном и международном уровнях.

В частности, в конвенции следует по-прежнему использовать термин «киберпреступность». Он отражает общепонятную концепцию и используется в многих документах Организации Объединенных Наций, в том числе в итоговых документах двенадцатого, тринадцатого и четырнадцатого Конгрессов Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, а также в резолюциях Генеральной Ассамблеи (в частности, в резолюции 65/230) и многих других резолюциях и докладах Комиссии по предупреждению преступности и уголовному правосудию и Экономического и Социального Совета.

Элементы договора (структура и цели)

Криминализация

Новая конвенция дает возможность существенно улучшить международное сотрудничество в борьбе с киберпреступностью. Согласованные нормы, применимые к основному набору киберпреступлений, повысят способность государств противодействовать киберпреступности на глобальном, региональном и национальном уровнях.

Для этого, по мнению Австралии, конвенция должна быть четко ориентирована на те виды преступного поведения, которые были существенно изменены киберпреступностью. Внутреннего уголовного законодательства государств, как правило, более чем достаточно для определения таких привычных преступлений, как незаконное проникновение, вандализм, кража, наркопреступления и насильственные преступления. Нет необходимости переосмысливать в конвенции эти преступления просто потому, что при их совершении использовались компьютер или информационная система.

Новая конвенция должна предусматривать новые стандарты криминализации правонарушений, совершение которых возможно только с использованием информационно-коммуникационных систем и которые называются «чистыми компьютерными преступлениями» или «киберзависимыми преступлениями». Таких преступлений не было до появления информационно-коммуникационных сетей, и поэтому уголовное законодательство государств часто является недостаточным или непоследовательным с точки зрения применимости к таким преступлениям. В этом отношении введение согласованных стандартов криминализации даст значительные преимущества государствам как в плане их национальных усилий по борьбе с киберпреступностью, так и в плане содействия более широкому международному сотрудничеству.

При этом, по мнению Австралии, существуют некоторые «традиционные» преступления, масштабы, размах и легкость совершения которых резко возросли благодаря информационно-коммуникационным сетям, обеспечивающим скорость, анонимность и широту охвата. Иногда их называют «преступлениями, совершаемыми посредством кибертехнологий». В конвенции следует подойти к этим преступлениям разумно, установив четкие рамки для определения того, почему определенные составы преступлений настолько существенно изменяются «цифровым элементом», что требуют нового согласованного международного стандарта, обособляющего такое поведение от «традиционных» преступлений. Не требуется устанавливать в конвенции новые категории правонарушений для каждого существующего состава преступления, который может включать «цифровой элемент», особенно в тех случаях, когда тяжесть или масштаб уголовно наказуемого деяния существенно не меняются этим элементом.

Австралия считает, что есть два очевидных кандидата в категории преступлений, совершаемых посредством кибертехнологий, которых следует включить в конвенцию, а именно представляющие серьезную угрозу сексуальная эксплуатация детей и надругательство над ними в интернете и широко распространенные и все чаще встречающиеся мошенничество и кражи с использованием цифровых технологий, включая вымогательство с использованием программ-вымогателей. Австралия готова выслушать аргументы в поддержку включения других преступлений, совершаемых с использованием кибертехнологий, но по вышеизложенным причинам при разработке конвенции следует сдержанно относиться к включению любой новой категории преступлений.

В конвенции также следует уделить должное внимание основным правонарушениям и дополнительной ответственности за киберзависимые преступления и преступления с использованием кибертехнологий. Это предполагает стандартное расширение уголовной ответственности, закрепленное в таких документах, как Конвенция об организованной преступности и Конвенция против коррупции. Учитывая роль технологий, облегчающих совершение киберпреступлений,

при разработке конвенции следует также рассмотреть вопрос о согласованных уголовно-правовых нормах в отношении правонарушений, связанных с производством, приобретением или предоставлением технологий и программного обеспечения, приспособленных исключительно или главным образом для совершения киберпреступлений.

Киберпреступность — это быстро развивающееся явление, характеризуемое тем, что киберпреступники постоянно стремятся использовать новые технологии и методы, чтобы расширять свою деятельность и избегать разоблачения правоохранительными органами. Чтобы противостоять этой тенденции и чтобы конвенция оставалась актуальной и эффективной в будущем, содержащиеся в ней стандарты криминализации должны быть сформулированы нейтрально с точки зрения технологий и методов.

Процессуальные меры борьбы с киберпреступностью

Процессуальное право — важнейший элемент в расследовании киберпреступлений и судебном преследовании за них. Конвенция должна установить четкие рамки применения процессуальных мер, гарантирующих правоохранительным органам возможность получать доказательства, необходимые для борьбы с киберпреступностью. Сфера охвата любых таких рамок должна поддерживать четкие нормы внутреннего законодательства, достаточно жесткие для того, чтобы правоохранительные или другие соответствующие органы могли бороться с проблемами киберпреступности, в том числе посредством выявления, пресечения, предупреждения, расследования преступлений и судебного преследования за них.

Процессуальные меры должны также учитывать характер электронных данных, обеспечивая правоохранительным и другим соответствующим органам возможность оперативно и эффективно получать такие данные, чтобы методы и практики, используемые преступниками в киберпространстве, не препятствовали усилиям властей по сбору данных. Предусмотренные виды процессуальных мер могут включать полномочия на обыск и арест, полномочия, связанные с получением данных (например, на доступ к хранимому коммуникационному контенту и на действия по перехвату), а также экстренные или срочные запросы или распоряжения о раскрытии таких данных. Процессуальные меры должны подкрепляться надежными гарантиями и ограничениями, должным образом защищающими права человека и верховенство закона.

Государствам, вероятно, придется рассмотреть вопрос о том, как практика государств, касающаяся сбора электронных данных в разных юрисдикциях, будет отражена в новой конвенции.

Международное сотрудничество и техническая помощь

В подавляющем большинстве случаев киберпреступность носит транснациональный характер. Для способности государств эффективно расследовать киберпреступления и преследовать киберпреступников решающее значение имеет международное сотрудничество на основе единообразного порядка криминализации.

За последние десятилетия международное сообщество добилось значительного прогресса в международном сотрудничестве в сфере уголовного правосудия, разработав эффективные инструменты в виде целого ряда действующих международных договоров, регулирующих взаимную правовую помощь, выдачу и другие формы международного сотрудничества. Так, положения практически всеми принятых Конвенции об организованной преступности и Конвенции против коррупции обеспечивают прекрасную основу для такого сотрудничества.

Новая конвенция должна максимально использовать аналогичные положения Конвенции об организованной преступности и Конвенции против

коррупции, касающиеся взаимной правовой помощи, выдачи, передачи заключенных и возврата доходов от преступлений. Эти положения доказали свою эффективность и пользуются широкой международной поддержкой. В соответствии с мандатом, изложенным в резолюции 74/247 Генеральной Ассамблеи, следует также обеспечить, чтобы новая конвенция дополняла, а не подрывала другие существующие механизмы международного сотрудничества в области уголовного правосудия.

Другие международные и региональные режимы обеспечивают эффективную основу для международного сотрудничества в борьбе с киберпреступностью, подкрепленную надежными гарантиями и ограничениями. Новая конвенция должна в максимально возможной степени учитывать эти режимы. Главным из них является Конвенция Совета Европы о киберпреступности, которая продолжает служить эффективной основой для международного сотрудничества между многими государствами во всех регионах мира.

Помимо международного сотрудничества, новая конвенция должна придать серьезный импульс усилиям, направленным на укрепление международного потенциала в области борьбы с киберпреступностью. В тексте конвенции следует подтвердить основную роль Управления Организации Объединенных Наций по наркотикам и преступности в предоставлении технической помощи и наращивании потенциала, в том числе в качестве координатора Глобальной программы борьбы с киберпреступностью.

Гарантии защиты и поощрения прав человека

Доступ государства к электронным и коммуникационным данным физических лиц по своей сути затрагивает права личности. В конвенции следует подтвердить ответственность государств за поощрение и защиту прав человека отдельных лиц в контексте борьбы с киберпреступностью в соответствии с международными стандартами в области прав человека.

Права на неприкосновенность частной жизни, на свободу мнений и их выражения и на свободу объединений должны и впредь должным образом защищаться в соответствии с существующими международными стандартами. К другим правам, которые также должны быть защищены, относятся право на справедливое судебное разбирательство, включая равенство перед законом, а также право не подвергаться пыткам и бесчеловечному или унижающему достоинство обращению или наказанию, произвольному задержанию и дискриминации. Международное сообщество неоднократно подтверждало, что эти права применяются как в интернет-пространстве, так и вне его, и в конвенции следует подтвердить существующие обязанности государств по соблюдению этих прав в ходе их операций по борьбе с киберпреступностью.

Структура и методы работы

Австралия ожидает, что как только государства получат возможность выразить свои мнения относительно сферы применения конвенции на первой переговорной сессии, которая состоится в январе 2022 года, по структуре конвенции будет быстро достигнут консенсус.

Австралия предлагает предложить государствам, после того как в январе 2022 года они выскажут свои мнения относительно сферы применения, структуры и целей новой конвенции, представить предложения по статьям, которые будут включены в каждый структурный элемент новой конвенции (например, предложения по криминализации и международное сотрудничество). Затем Председатель, при необходимости консультируясь с Бюро, должен свести эти различные предложения в проект документа, который государства смогут обсудить, причем каждый набор статей будет рассматриваться по очереди в соответствии с планом работы, установленным Специальным комитетом на его первом совещании.

После начальных переговоров по каждому элементу структуры можно будет продолжить переговоры по конвенции в целом, опять же в соответствии с планом работы, установленным Специальным комитетом на его первом совещании, и в дальнейшем под руководством Председателя.

Бразилия

[Подлинный текст на английском языке]
[29 октября 2021 года]

Как и многие другие страны, Бразилия ведет борьбу с киберпреступностью — явлением, которое встречается все чаще и приобретает все более сложный характер. Использование цифровых средств для совершения различных преступлений обуславливает необходимость решительной модернизации надлежащих мер нормативного и правоохранительного реагирования на эти угрозы, в том числе на международном уровне. Географический охват и скорость совершения таких правонарушений бросают вызов традиционным механизмам сотрудничества между правоохранительными органами и правового сотрудничества во всем мире.

Эти вызовы колоссальны. Поставщики интернет-услуг, обладающие важной информацией, необходимой для расследования киберпреступлений и сбора электронных доказательств, нередко имеют фактическую штаб-квартиру в одной стране, услуги предоставляют на различных континентах, а информацию хранят на серверах в какой-либо еще точке планеты. В таком случае правоохранительные органы стремятся определить, кто обладает юрисдикцией в отношении необходимых данных и имеет прямой доступ к ним, чтобы надлежащим образом обратиться к этому субъекту.

Необходимым шагом вперед в осуществлении преследования за совершение киберпреступлений является согласованное международное взаимодействие между юрисдикциями. Необходимо расширять международное сотрудничество и повышать его эффективность. Для эффективного пресечения преступной деятельности требуются механизмы оперативного и прямого сотрудничества, с помощью которых правоохранительные органы смогут своевременно обмениваться доказательствами по разным делам, в которых фигурирует одна и та же преступная группа.

Бразилия активно участвует в переговорах по всеобъемлющей конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Это уникальная возможность установить общие стандарты сотрудничества в решении этой транснациональной по своей сути проблемы, опираясь на наилучшие традиции и практику в этой области.

По мнению Бразилии, чтобы будущая конвенция позволяла реагировать на все вышеупомянутые угрозы, при проработке ее целей, сферы действия и структуры следует учитывать нижеследующие соображения.

Цели

В первую очередь конвенция должна обеспечивать конкретный инструментарий для международного сотрудничества, с тем чтобы государства-участники могли оперативно получать доказательства и другую информацию, способствующую расследованию киберпреступлений и осуществлению преследования за их совершение. Хотя эта главная цель уже представляет самостоятельную ценность, по возможности данный правовой документ должен решать еще две задачи: a) установление в юрисдикции каждого государства-участника минимальных обязательств по криминализации (материальное уголовное право); и b) установление в юрисдикции каждого государства-участника минимальных обязательств, обеспечивающих своевременное реагирование, расследование и преследование (уголовно-процессуальное право).

Бразилия всецело поддерживает идею о выработке универсальной конвенции. Мы осознаем, что переговоры по правовому документу, в котором были бы закреплены минимальные нормы о криминализации, сопряжены с определенными трудностями, особенно если учесть новизну и изменчивость рассматриваемого явления. Вместе с тем на этом направлении имеются успешные прецеденты. В отношении некоторых других видов преступности переговоры завершились успехом, примером чего служат существующие универсальные конвенции по борьбе с преступностью, и большинство членов международного сообщества взяли на себя обязательства по введению минимальных материально-правовых норм. Отправной точкой в этой дискуссии должно быть не постулируемое противопоставление географического охвата и сферы применения криминализации, а понимание того, что самым надежным способом достижения наилучшего варианта минимально возможного консенсуса в отношении применения к киберпреступности норм материального уголовного права являются сами переговоры. Минимальный консенсус в отношении криминализации, опирающийся на нейтральные и общие понятия, хотя и может иметь достаточно узкую сферу охвата, способен тем не менее ограничить для киберпреступников возможности выбора юрисдикции, обеспечить обмен опытом и уменьшить нормативные противоречия между странами, требующими, чтобы в качестве условия для сотрудничества применялся принцип обоюдного признания того или иного деяния преступлением.

Оперативность международного сотрудничества всегда будет зависеть от того, какими процессуальными механизмами располагают следователи, прокуроры и судьи в наиболее отличающихся друг от друга юрисдикциях. Сами по себе такие традиционные механизмы правового сотрудничества, как судебные поручения и признание постановлений иностранных судов, не способны обеспечить надлежащее противодействие киберпреступности ни в одной стране. Транснациональный и крайне непредсказуемый характер этого явления требует стандартизации процедур, даже если она будет максимально универсальной и общей, чтобы охватить все особенности национальных правовых систем соответствующих государств. Вместе с тем в основе подобной стандартизации должны лежать некие минимальные нормы, предусматривающие оперативное обеспечение сохранности электронных доказательств, которое инициируется по оперативному прямому международному каналу, иначе идентифицировать преступников, особенно в делах об организованной преступности, будет невозможно.

Сфера действия

Конвенция должна служить основой для обмена доказательствами и данными, которые относятся a) к преступлениям против компьютерных систем; и b) к любым преступлениям, совершаемым с использованием электронных средств. По возможности необходимо предусмотреть положения, касающиеся электронных данных о соединениях, контенте и подписчиках.

Кроме того, конвенция должна позволять сторонам направлять просьбы о международном сотрудничестве (для оперативного обеспечения сохранности электронных доказательств и оказания взаимной правовой помощи) и по собственной инициативе передавать информацию другим юрисдикциям. Одну главу следует посвятить созданию международного сетевого объединения специалистов-практиков, которые будут отвечать за реагирование в экстренных случаях. Если предусматривается подобный оперативный механизм, то тем более для конвенции необходимо учредить и директивный орган для мониторинга и обзора хода ее осуществления.

Будучи рамочным документом, конвенция может предусматривать возможность заключения отдельных протоколов как дополнительного инструментария, который позволит расширить сотрудничество в борьбе с конкретными разновидностями киберпреступлений.

В этой связи конвенция должна представлять собой правовой документ, предназначенный для практического применения норм уголовного права, и не затрагивать вопросы политики в области международного мира и безопасности, вопросы кибероборонs или вопросы, касающиеся регулирования интернета на национальном, региональном или международном уровнях.

Структура

С учетом вышеизложенных соображений Бразилия полагает, что конвенция должна иметь следующую структуру:

Глава I. Криминализация

Глава II. Уголовно-процессуальные нормы, обеспечивающие своевременное расследование и преследование

Глава III. Международное сотрудничество

A. Оперативное обеспечение сохранности данных в электронной форме

B. Взаимная правовая помощь

C. Передача информации по собственной инициативе

Глава IV. Сетевое объединение для сотрудничества

Глава V. Механизм контроля для мониторинга и обзора хода осуществления

Канада

[Подлинный текст на английском языке]
[1 ноября 2021 года]

Настоящее сообщение представляется Канадой в ответ на просьбу изложить мнения о сфере действия, целях и структуре (элементах) новой конвенции, направленную государствам-членам 11 августа секретариатом Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

При подготовке данных замечаний Канада опиралась на результаты важной работы в области киберпреступности, которая уже 20 лет ведется в Организации Объединенных Наций под руководством Комиссии по предупреждению преступности и уголовному правосудию, в частности межправительственной Группой экспертов для проведения всестороннего исследования проблемы киберпреступности, Управлением Организации Объединенных Наций по наркотикам и преступности по линии его Глобальной программы борьбы с киберпреступностью, а также на конгрессах Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Благодаря этим инициативам была подготовлена почва для разработки конвенции Организации Объединенных Наций, которая должна быть посвящена исключительно борьбе с киберпреступностью и не затрагивать вопросы кибербезопасности, управления киберпространством и другие смежные вопросы, которые уместнее рассматривать на других форумах Организации Объединенных Наций.

В соответствии с резолюцией 75/282 Генеральной Ассамблеи и своими сообщениями, направленными ранее Специальному комитету, Канада вновь заявляет, что переговоры по новой конвенции должны представлять собой прозрачный и всеохватный процесс, полностью открытый для участия гражданского общества и других заинтересованных сторон.

Сфера действия

Новая конвенция должна служить основой для противодействия киберпреступности и серьезным уголовным правонарушениям, часто совершаемым с использованием компьютерных систем, и включать в себя следующие элементы:

a) положения об основных киберпреступлениях, а также о расследовании киберпреступлений и серьезных уголовных правонарушений, часто совершаемых с использованием компьютерных систем, и преследовании за их совершение;

b) положения о международном сотрудничестве в вышеуказанных вопросах, а также сотрудничестве для получения электронных доказательств в отношении других уголовных правонарушений;

c) указание мер, направленных на предупреждение киберпреступности;

d) указание мер, стимулирующих государства-члены и другие заинтересованные стороны осуществлять долговременные инициативы по оказанию технической помощи и наращиванию потенциала.

Элементы новой конвенции должны согласовываться с международными обязательствами в области прав человека, прежде всего касающимися свободы выражения мнений, свободы убеждений и свободы ассоциации, а также права не подвергаться противоправному и произвольному посягательству на неприкосновенность частной жизни.

Цели

Новая конвенция должна преследовать следующие цели:

a) установление на основе всеобщего взаимопонимания базовых параметров основных преступлений, процессуальных полномочий и международного сотрудничества в борьбе с киберпреступностью;

b) использование технически нейтральных формулировок, позволяющих избежать устаревания или невозможности применения тех или иных положений по мере развития технологий;

c) поощрение и облегчение международного сотрудничества в совместной борьбе с киберпреступностью;

d) закрепление полномочий на сбор, получение и передачу электронных доказательств по другим правонарушениям;

e) ликвидация безопасных убежищ для лиц, совершающих киберпреступления;

f) обеспечение соблюдения международных обязательств в области прав человека, прежде всего касающихся свободы выражения мнений, свободы убеждений и свободы ассоциации, а также права не подвергаться противоправному и произвольному посягательству на неприкосновенность частной жизни;

g) обеспечение согласованности с действующими договорами Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в частности с Конвенцией Организации Объединенных Наций против транснациональной организованной преступности и Конвенцией Организации Объединенных Наций против коррупции, и учет многосторонних правовых документов, уже доказавших свою эффективность в борьбе с киберпреступностью, в частности Конвенции Совета Европы о киберпреступности; и

h) поддержка развития потенциала государств-членов в области противодействия киберпреступности посредством технической помощи и деятельности по наращиванию потенциала.

Структура

Что касается структуры новой конвенции, то Канада считает, что помимо ясных определений и заключительных положений структура конвенции должна включать следующие пять элементов:

a) положения об основных правонарушениях, обязывающие государства-члены принимать законодательные и другие необходимые меры для:

i) введения уголовной ответственности за деяния, нарушающие конфиденциальность, целостность и доступность компьютерных систем, сетей и компьютерных данных, и за неправомерное использование компьютерных систем, сетей и компьютерных данных;

ii) установления в их уголовном законодательстве надлежащей ответственности за частое совершение конкретных традиционных преступлений с использованием компьютерных систем, например за распространение детской порнографии;

b) процессуальные положения, обязывающие государства-члены принимать законодательные и другие необходимые меры для утверждения полномочий на сохранение и получение электронных доказательств по уголовным правонарушениям, хранящихся в компьютерных системах, которые находятся в иностранных юрисдикциях, в нескольких юрисдикциях или в неустановленных юрисдикциях. Помимо следственных полномочий более общего характера, например полномочий на проведение обысков, изъятий и постановлений о предоставлении информации, в новой конвенции следует также предусмотреть возможность применения специального следственного инструментария с учетом скорости, с которой могут совершаться правонарушения, и недолговечности и изменчивости электронных доказательств. Эти положения должны быть подкреплены гарантиями, обеспечивающими соответствие правоохранительной деятельности международным обязательствам в области прав человека;

c) важную роль в борьбе с киберпреступностью играет международное сотрудничество. Новая конвенция должна предусматривать механизмы, облегчающие официальное и неофициальное международное сотрудничество, имеющее целью выявление и расследование киберпреступлений и осуществление преследования за их совершение, а также получение электронных доказательств по делам о других уголовных правонарушениях;

d) новая конвенция должна предусматривать также профилактические меры, аналогичные изложенным в Конвенции об организованной преступности и Конвенции против коррупции, например положения об информировании общественности и образовательных инициативах. Критически важную роль в этой работе могут играть партнерские объединения с участием многих заинтересованных сторон и гражданское общество, что должно найти отражение в данных положениях;

e) новая конвенция должна стимулировать государства-члены развивать потенциал в области противодействия киберпреступности за счет получения технической помощи и деятельности по наращиванию потенциала. Для этого могут быть предусмотрены следующие положения:

i) о поддержке участия в подобной деятельности многих заинтересованных сторон;

ii) о поощрении сотрудничества с Управлением Организации Объединенных Наций по наркотикам и преступности и участниками его Глобальной программы борьбы с киберпреступностью, нацеленного на повышение квалификации специалистов-практиков и сотрудников центральных органов в вопросах использования технологий для содействия международному сотрудничеству в борьбе с киберпреступностью; и

iii) о разработке программы обучения для следователей и прокуроров и поддержке обмена информацией и опытом с соответствующими заинтересованными сторонами.

Чили

[Подлинный текст на английском языке]
[5 ноября 2021 года]

Правительство Чили с удовлетворением представляет свой ответ на направленное государствам-членам предложение изложить свои мнения относительно сферы действия, целей и структуры (элементов) новой конвенции во исполнение резолюций 74/247 и 75/282 Генеральной Ассамблеи.

Чили считает, что новая конвенция не должна противоречить другим действующим договорам или соглашениям о борьбе с киберпреступностью. Основное внимание в ней следует уделить международному сотрудничеству и технической помощи как опорным элементам многостороннего подхода к борьбе с киберпреступностью. Чтобы обеспечить открытость, всеохватность и прозрачность процесса, а также участие в нем различных заинтересованных сторон, мнения всех стран должны считаться одинаково значимыми.

1. Общие соображения

a) *Юрисдикция*. Разработка новой конвенции — превосходный повод обсудить этот вопрос, от решения которого зависят многие процессуальные механизмы, заслуживающие рассмотрения.

b) Необходимо обеспечить тщательное формулирование определений, чтобы они сохраняли актуальность и оставались применимыми в условиях быстрого развития технологий. Так, следует предусмотреть определения для различных типов данных.

2. Материальное уголовное право

a) *Учет преступлений, заключающихся в получении компьютерных данных*. Несмотря на то, что в ряде стран применение понятия о данном типе преступлений носит ограниченный характер, представляется уместным оговорить в конвенции незаконное деяние, при котором объектом «кражи» становятся компьютерные данные, а лицо, располагающее такими данными, знает или не может не знать об их нелегальном происхождении.

b) Что касается субъектности и соучастия, то представляется необходимым отдельно упомянуть о содействии со стороны получателей денежных средств или ценных бумаг, похищенных в результате компьютерного мошенничества, поскольку с учетом специфики данного класса преступлений и трудностей, в большинстве случаев сопряженных с их расследованием, в отношении лиц, которые, как правило, являются первым звеном в преступной цепочке, уместно применять особый порядок преследования, и в этой связи исходя из степени их участия целесообразно присваивать им статус субъектов мошенничества, не исключая возможности смягчения наказания в случае успешного содействия с их стороны в поимке остальных компьютерных преступников.

3. Нормы процессуального права

a) Целесообразно обсудить новые способы и рабочий инструментарий, с помощью которых компетентные органы могли бы выявлять преступления, которые готовятся в интернете или которые планируется совершить в интернете, а также наиболее эффективные методы борьбы с ними.

b) Представляется уместным обсудить вопрос об обеспечении баланса между необходимой и надлежащей защитой граждан и их личных данных и

нуждами уголовного расследования, поскольку чрезмерная защита такого рода информации может влиять на разработку следственных процедур, обеспечивающих надлежащее и своевременное преследование за совершение такого рода преступлений, которым благоприятствуют условия анонимности, транснациональности и невозможности отслеживания, возникающие вследствие принятия подобных мер защиты.

4. Глава, посвященная международному сотрудничеству

a) Необходимо закрепить в конвенции принцип взаимной правовой помощи в уголовно-правовых вопросах.

b) Странам следует изучить возможности содействия оперативному и защищенному обмену информацией между следователями и прокурорами, которые специализируются на киберпреступлениях.

c) Странам необходимо тесно сотрудничать друг с другом, действуя сообразно своим внутренним правовым и административным системам, в целях повышения эффективности правоприменительных мер для борьбы с киберпреступлениями. Каждой стране следует принять эффективные меры для создания и обеспечения функционирования каналов связи между их компетентными органами, ведомствами и службами с целью содействовать защищенному и оперативному обмену информацией обо всех аспектах киберпреступлений.

d) Необходимо рассмотреть вопрос о том, чтобы использовать электронную передачу просьб об оказании взаимной правовой помощи не только в чрезвычайных ситуациях, а сделать ее полноценной и постоянной формой взаимодействия.

e) Необходимо предусмотреть положения об обеспечении сохранности и предоставлении данных.

f) Следует проанализировать пользу сетевых объединений, функционирующих в круглосуточном режиме, как инновационного элемента международного сотрудничества.

g) Необходимо предусмотреть положения, регламентирующие чрезвычайные ситуации.

h) Странам необходимо совместными усилиями установить наличие между ними «цифрового разрыва», поскольку некоторые страны не располагают ни возможностями, ни средствами для предупреждения, выявления и пресечения киберпреступлений и поэтому более уязвимы перед создаваемыми ими угрозами.

5. Специальный инструментарий для международного сотрудничества

a) Предоставление данных поставщиками интернет-услуг и их взаимоотношения с государствами.

b) Трансграничный доступ к данным.

c) Специальные методы расследования: оперативное внедрение в интернете, совместные следственные группы, проведение совместных расследований и пр.

6. Предупреждение киберпреступности

a) В деятельности по предупреждению киберпреступности должны участвовать различные заинтересованные стороны: правительства, правоохранительные органы, организации частного сектора, международные организации, неправительственные организации и научная общественность.

b) Необходимо содействовать внедрению стратегий предупреждения, ориентированных на защиту интересов потерпевших и предусматривающих меры предупреждения киберпреступлений против личности.

c) Странам следует рассмотреть вопрос о применении механизмов сотрудничества с отраслью, включая обращения в компетентные национальные органы и удаление из сети материалов вредоносного и преступного содержания, в частности материалов с изображением сцен сексуальной эксплуатации детей и других видов жестокого насилия.

7. Учет гендерного фактора в контексте конвенции о киберпреступности

a) В целях поощрения гендерного равенства и расширения прав и возможностей женщин, как онлайн, так и в реальном мире, следует учитывать гендерный фактор при выполнении положений конвенции и оценке результатов их выполнения, а также применять гендерный анализ в вопросах использования информационно-коммуникационных технологий, в частности при рассмотрении гендерных аспектов киберпреступности.

b) Борьба с киберпреступностью должна включать предотвращение и пресечение насилия в отношении женщин и детей.

Китай

[Подлинный текст на китайском языке]
[5 ноября 2021 года]

Китай приветствует инициативу Председателя Специального комитета Организации Объединенных Наций по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, предложившего государствам-членам поделиться мнениями относительно сферы применения, целей и структуры (элементов) конвенции. Согласно резолюции 75/282 Генеральной Ассамблеи, Специальному комитету надлежит представить проект конвенции на семьдесят восьмой сессии Генеральной Ассамблеи. Китай выражает надежду на то, что конструктивное обсуждение данной темы под руководством Председателя позволит в намеченный срок прийти к соглашению о новой конвенции, которая будет носить универсальный и авторитетный характер, будет приемлема для всех сторон и позволит заложить правовую основу для укрепления сотрудничества в борьбе с киберпреступностью во всем мире.

К настоящему времени государствам-членам в рамках соответствующих механизмов Организации Объединенных Наций удалось провести подробное обсуждение темы борьбы с киберпреступностью и согласовать ряд выводов и рекомендаций. Одно из государств-членов также внесло проект всеобъемлющей конвенции, который может послужить полезным ориентиром в переговорах о конвенции. Китай с удовлетворением отмечает, что Председатель старается способствовать активному представлению государствами-членами своих мнений и предложений, и готов оказать ему поддержку в подготовке первоначального проекта конвенции на основе представленных государствами-членами материалов, чтобы как можно скорее приступить к переговорам по тексту конвенции.

Для облегчения работы Председателя и Специального комитета Китай сформулировал нижеследующие замечания относительно сферы применения, целей и структуры (элементов) конвенции и выражает готовность к конструктивным переговорам со всеми сторонами.

I. Цели

a) Содействие принятию и укреплению мер, направленных на эффективное предупреждение использования информационно-коммуникационных

технологий (ИКТ) в преступных целях и борьбу с ним во имя реализации концепции общего будущего в мировом киберпространстве.

b) Поощрение, облегчение и поддержка международного сотрудничества в предупреждении использования ИКТ в преступных целях и борьбе с ним с учетом специфики ИКТ и необходимости бороться со связанными с ними видами преступной деятельности. Международное сотрудничество может вестись по таким направлениям, как согласование оснований уголовной ответственности в разных государствах-членах, разработка инструкций по разрешению коллизий юрисдикций и создание специализированных институциональных механизмов сотрудничества правоохранительных органов, правовой помощи, выдачи и возвращения активов.

c) Укрепление сотрудничества в вопросах развития потенциала и технической помощи и содействие обмену информацией в этой области с учетом интересов и широкого диапазона потребностей развивающихся стран в сфере международного сотрудничества.

II. Сфера применения

Конвенция должна применяться к предупреждению, расследованию и уголовному преследованию за использование ИКТ в преступных целях отдельными лицами или преступными группами, а также к блокировке, замораживанию, аресту, конфискации и возвращению доходов от преступлений в сфере ИКТ.

Использованием ИКТ в преступных целях следует считать, как минимум, преступления, направленные против объектов ИКТ-инфраструктуры, информационных систем и данных, и преступления, совершаемые с использованием ИКТ.

III. Структура (элементы)

Конвенцию можно разделить на семь глав, посвященных следующим темам: общие положения; предупреждение киберпреступности; криминализация и правоохранительная деятельность; международное сотрудничество; техническая помощь и обмен информацией; механизм осуществления; заключительные положения.

Ниже излагаются предварительные соображения относительно элементов содержания соответствующих глав.

1. Общие положения

Помимо целей и сферы применения в данной главе следует оговорить также следующие моменты:

a) *защита суверенитета*. Основополагающей нормой современных международных отношений является принцип суверенного равенства, закрепленный в Уставе Организации Объединенных Наций. Широкой поддержкой у государств-членов пользуется мнение, что принцип суверенитета должен применяться и к киберпространству. В конвенции следует особо оговорить, что государствам-участникам надлежит осуществлять свои обязательства согласно конвенции в соответствии с принципами суверенного равенства, территориальной целостности и невмешательства во внутренние дела других государств;

b) *терминология*. В конвенции будет необходимо дать определения основных используемых в ней понятий, таких как электронные доказательства, персональные данные, критическая информационная инфраструктура, облачное хранилище данных, поставщик сетевых услуг, вредоносное программное обеспечение, бот-сеть, вредная информация и кибератака.

2. Предупреждение киберпреступности

Следует особо упомянуть о важности мероприятий по предупреждению использования ИКТ в преступных целях. Основополагающий принцип должен заключаться в том, что «на первом месте в борьбе с преступностью должна стоять профилактика». Необходимо уточнить, какие обязанности по предупреждению преступности несут на себе государство и частный сектор, а правительствам следует разработать целенаправленные меры предупреждения преступности и поощрять участие общественности в профилактике преступлений и развитие сотрудничества между государством и частным сектором. В конвенции следует оговорить следующие моменты:

a) государствам-членам следует назначить специализированные учреждения, которые будут заниматься разработкой политики в области предупреждения использования ИКТ в преступных целях и проводить регулярную оценку ее эффективности. Государствам-членам следует обеспечить защиту безопасности критической информационной инфраструктуры и создать многоуровневые системы защиты безопасности информационных сетей. Для обеспечения лучшей защиты критической информационной инфраструктуры от атак преступников или преступных групп следует применять разные технологии информационной безопасности и механизмы управления на разных объектах сетевой инфраструктуры. Необходимо также развивать потенциал соответствующих государственных ведомств в области предупреждения преступности;

b) государствам-членам следует принять или усовершенствовать национальное законодательство для уточнения обязанностей частного сектора, включая поставщиков сетевых услуг, по предупреждению использования ИКТ в преступных целях. В такие обязанности должно входить, помимо прочего, принятие профилактических мер безопасности (например, составление аварийных планов на случай инцидентов в сфере сетевой безопасности, своевременное устранение уязвимостей системы и оборудования, обнаружение компьютерных вирусов, сетевых атак или попыток проникновения в сеть, а также принятие мер в режиме реального времени в случае обнаружения вероятности использования услуг таких провайдеров для преступной деятельности) и хранение информации системных журналов (правительствам следует установить стандартные требования к содержанию и срокам хранения информации). При определении обязанностей поставщиков сетевых услуг следует установить дифференцированные требования для каждого уровня в соответствии с принципом соразмерности и с учетом различий в возможностях, имеющихся у поставщиков сетевых услуг разного размера;

c) следует поощрять участие правительственных структур, частного сектора и общественных организаций в различных формах государственно-частного сотрудничества. Необходимо, в частности, прилагать больше усилий к повышению осведомленности населения о важности предупреждения преступности.

3. Криминализация и правоохранительная деятельность

Преступники и преступные сообщества все активнее пользуются ИКТ для совершения преступлений, что привело к формированию целой «теневой производственной цепочки», специализирующейся на разработке ИКТ для преступных целей и совершении операций с использованием таких технологий и соответствующих данных. Конвенция должна заложить более гибкую и перспективную основу для скоординированного решения вопросов криминализации, позволяющую удовлетворить текущие и будущие потребности борьбы с преступностью с учетом развития ИКТ. В конвенции также следует предусмотреть соответствующие механизмы решения вопросов подсудности, правоприменения и электронных доказательств:

a) государствам-членам следует рекомендовать ввести уголовную ответственность за проникновение на объекты ИКТ-инфраструктуры,

в информационные системы, данные или критическую информационную инфраструктуру и их уничтожение. К соответствующим деяниям можно отнести, в частности, получение неправомерного доступа к компьютерной информации, неправомерное воздействие на компьютерные информационные системы, неправомерное приобретение компьютерных данных, неправомерное воздействие на компьютерные данные и посягательство на критическую информационную инфраструктуру;

b) в конвенции можно при необходимости перечислить виды преступных деяний, совершаемых с использованием ИКТ и широко признаваемых в качестве таковых международным сообществом, например кибервымогательство, кибермошенничество, киберпорнография (особенно детская порнография), нарушение авторских и смежных прав с использованием ИКТ, использование интернета для совершения или подстрекательства к совершению террористических актов или распространения вредной информации;

c) что касается других преступлений, совершаемых с использованием ИКТ, то в конвенции следует подчеркнуть, что государства-члены могут принимать меры к предупреждению не перечисленных в конвенции преступлений и борьбе с ними и осуществлять международное сотрудничество как на основании этой конвенции, так и на основании других международных конвенций и применимого национального законодательства государств-членов;

d) ввиду того, что преступления, совершаемые с использованием ИКТ, приобретают все более «промышленный» характер, в сферу уголовной ответственности следует включить участие в «темной производственной цепочке», параллельно ужесточив меры, направленные на пресечение деятельности, связанной с пособничеством совершению или подготовкой к совершению таких преступных деяний, включая разработку, продажу или распространение ИКТ или данных с преступными целями;

e) что касается «электронных доказательств», то в конвенции необходимо установить правила идентификации электронных доказательств в рамках уголовного судопроизводства, в частности порядок проверки их подлинности, целостности, законности и относимости к делу;

f) государствам-членам можно предложить разработать или усовершенствовать национальное законодательство с целью уточнения обязанностей частного сектора, например обязанности поставщиков сетевых услуг сотрудничать с правоохранительными органами в вопросах отслеживания и расследования преступлений и борьбы с ними. В такие обязанности должно входить, в частности, хранение информации системных журналов, обеспечение сохранности данных и доказательств в соответствии с едиными стандартными требованиями к содержанию и срокам хранения и сотрудничество с правоохранительными органами. При определении обязанностей поставщиков сетевых услуг следует установить дифференцированные требования для каждого уровня в соответствии с принципом соразмерности и с учетом различий в возможностях, имеющихся у поставщиков сетевых услуг разного размера. На случай невыполнения поставщиком сетевых услуг возложенных на него обязанностей государствам-членам следует предусмотреть эффективные меры административной и уголовной ответственности в соответствии со своим национальным законодательством;

g) в конвенции необходимо дать указания по разрешению коллизий юрисдикций. С учетом специфики киберпространства и ИКТ необходимо установить стандартный порядок определения подсудности во избежание возникновения коллизий юрисдикций. Подсудность дел следует определять исходя из наличия «реальной и достаточной» связи с соответствующим преступным деянием, при этом приоритетное значение следует придавать таким критериям, как место наступления последствий преступного деяния, место совершения преступного деяния и место нахождения лица или лиц, совершивших преступление. Если сформулировать такие стандарты затруднительно, следует установить критерии отсева; например, можно предусмотреть, что государство не вправе

претендовать на осуществление юрисдикции в отношении того или иного дела, связанного с использованием ИКТ, лишь на том основании, что через его территорию происходила передача данных. В случае возникновения коллизии юрисдикций подсудность дела следует определять путем консультаций исходя из соображений удобства рассмотрения дела и перспектив возвращения активов;

h) в конвенции следует также предусмотреть положения о пособничестве или подстрекательстве к совершению преступления, подготовке преступления, покушении на совершение преступления, совершении преступлений юридическими лицами и т. п.

4. Международное сотрудничество

Использование ИКТ в преступных целях носит транснациональный характер и представляет общую проблему для всего международного сообщества. Анонимность и высокая технологичность преступной деятельности в сфере ИКТ, а также нестабильный и недолговечный характер электронных доказательств значительно затрудняют использование традиционных механизмов международного сотрудничества и взаимной правовой помощи, предусмотренных действующей международно-правовой базой. Государствам-членам следует в максимально возможной мере сотрудничать друг с другом в вопросах предупреждения использования ИКТ в преступных целях и борьбы с ним, придерживаясь принципа взаимности, активно изыскивая инновационные институциональные решения и внедряя новые механизмы для обеспечения более целенаправленного международного сотрудничества:

a) для успешной борьбы с использованием ИКТ в преступных целях государствам-членам нужно осуществлять трансграничный сбор электронных доказательств, однако при этом им следует уважать суверенитет государства, в котором находятся доказательства. Государствам-членам следует также придерживаться надлежащей правовой процедуры, уважать законные права физических и юридических лиц и воздерживаться от применения интрузивных и разрушительных технических средств расследования для трансграничного сбора электронных доказательств. Государствам не следует осуществлять сбор данных, хранящихся у предприятий или физических лиц в иностранных государствах, напрямую или с применением технических средств, позволяющих обойти меры защиты сетевой безопасности, если использование таких средств противоречит законодательству заинтересованного иностранного государства. Государствам-членам следует изучить возможность применения новых институциональных механизмов для сбора электронных доказательств, находящихся в других государствах, которые бы позволяли проверять подлинность электронных доказательств и осуществлять сбор видео- или аудиодоказательств на основе взаимного доверия. Следует стремиться к тому, чтобы такие механизмы образовывали унифицированную и авторитетную основу для трансграничного сбора электронных доказательств и позволяли добиться оптимального баланса в достижении таких разных целей, как защита национального суверенитета и борьба с преступностью;

b) государствам-членам следует разработать механизмы оперативного сотрудничества правоохранительных органов. Для быстрого обмена оперативными сведениями, дачи консультаций по техническим вопросам и осуществления других форм сотрудничества в правоохранительной сфере в случае возникновения такой необходимости государства-члены могут назначить конкретные органы ответственными за обеспечение связи взаимодействия;

c) с целью повышения эффективности взаимной правовой помощи по уголовным делам государства-члены могли бы создать механизм оперативного взаимодействия и реагирования, позволяющий компетентным органам в случае необходимости общаться друг с другом в режиме реального времени. Передача правовых документов и электронных доказательств в рамках трансграничного сбора доказательств может осуществляться в режиме онлайн с применением

технических средств (таких, как электронные подписи) в рамках национальных систем управления безопасностью трансграничной передачи данных. В конвенции можно также предусмотреть порядок оказания взаимной правовой помощи в экстренных ситуациях, предусматривающий ускоренную процедуру сохранения электронных доказательств и их последующего раскрытия и т. п.;

d) с учетом того, что в национальном законодательстве предполагается закрепить обязанность частного сектора, включая поставщиков сетевых услуг, сотрудничать с правоохранительными органами в вопросах отслеживания и выявления противоправной деятельности и борьбы с нею, государствам-членам, особенно обладающим развитой сетевой инфраструктурой, следует и далее укреплять международное сотрудничество в этой области. Если объекты ИКТ-инфраструктуры, информационные системы или сети, принадлежащие поставщику сетевых услуг в государстве A, используются подозреваемым в другом государстве для совершения преступления, то при условии, что соответствующее деяние является уголовно наказуемым в государстве A, это государство должно по собственной инициативе или по просьбе другого государства обратиться к соответствующему поставщику сетевых услуг с требованием отреагировать на противоправную деятельность путем принятия необходимых технических или любых других мер;

e) необходимо ужесточить меры, направленные на предупреждение и блокировку международных переводов доходов от преступной деятельности, и расширять международное сотрудничество в области возвращения активов. Государствам-членам следует придерживаться принципа быстрого и эффективного возвращения активов и не следует оговаривать возвращение активов никакими предварительными условиями помимо соблюдения надлежащих процессуальных требований.

5. Техническая помощь и обмен информацией

Для успешного предупреждения использования ИКТ в преступных целях и борьбы с ним необходимо оказывать техническую помощь развивающимся странам и активнее обмениваться с ними информацией:

a) техническая помощь развивающимся странам должна включать:

i) организацию учебной подготовки для сотрудников правоохранительных органов и органов юстиции;

ii) организацию учебной подготовки для групп специалистов, обладающих как юридическими, так и техническими знаниями;

iii) наращивание потенциала в области сбора электронных доказательств;

iv) предоставление развивающимся странам необходимого оборудования и технологий для укрепления их потенциала в области борьбы с преступностью;

v) привлечение международных организаций, включая Управление Организации Объединенных Наций по наркотикам и преступности, частного сектора, экспертов и ученых к участию в мероприятиях по оказанию технической помощи и наращиванию потенциала;

b) государствам-членам следует делиться друг с другом опытом разработки и применения законов и политических мер и обмениваться данными о предупреждении преступности и борьбе с нею, а также ее динамике и тенденциях.

6. Механизм осуществления

Для содействия осуществлению конвенции следует учредить конференцию государств-участников и соответствующие группы экспертов или рабочие группы, например рабочую группу по технической помощи и рабочую группу по вопросам международного сотрудничества. Совещания таких групп могли бы

служить площадкой для обмена опытом и развития сотрудничества между государствами-участниками.

7. Заключительные положения

На данный момент комментариев нет.

Колумбия

[Подлинный текст на испанском языке]
[5 ноября 2021 года]

В свете принятия резолюции 74/247 Генеральной Ассамблеи Организации Объединенных Наций, согласно которой был учрежден специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, и в ответ на предложение Председателя Специального комитета государствам-членам представить свои мнения относительно сферы применения, целей и структуры будущей конвенции о киберпреступности мы хотели бы представить следующие предварительные замечания со стороны Колумбии:

Сфера применения

Цель новой конвенции должна состоять в том, чтобы предоставить национальным органам власти инструмент международного правового сотрудничества в предупреждении и расследовании киберпреступлений и судебном преследовании и наказании виновных в их совершении, а также решения вопросов, связанных с электронными доказательствами. Поэтому следует избегать обсуждений, не касающихся правовой проблематики киберпреступности и порядка работы с электронными доказательствами.

Следует избегать обсуждения чувствительных в политическом отношении вопросов, которые не имеют прямого отношения к существу обсуждаемой конвенции.

При разработке новой конвенции крайне важно учитывать существующие международные правовые механизмы и инструменты, включая Конвенцию Организации Объединенных Наций против транснациональной организованной преступности, Конвенцию Организации Объединенных Наций против коррупции и Будапештскую конвенцию о киберпреступности, так как национальное законодательство и практика большинства государств приведены в соответствие с существующими соглашениями или основаны на них; следовательно, будущие стандарты должны быть совместимы с этими соглашениями. Кроме того, необходимо обеспечить, чтобы разрабатываемые правила были совместимы с другими международными обязательствами, принятыми на себя государствами, и не противоречили им.

В этой связи конвенция должна носить дополняющий характер, т. е. переговоры следует в принципе проводить с учетом той работы в области противодействия киберпреступности, которая ведется международным сообществом уже несколько лет, и не противоречить соответствующим международным обязательствам, взятым на себя государствами. Поэтому следует использовать потенциал и достижения Конвенции Организации Объединенных Наций против транснациональной организованной преступности с точки зрения устоявшихся принципов и инструментов сотрудничества судебных органов.

Необходимо принять во внимание существующие многосторонние, региональные и двусторонние механизмы оказания взаимной правовой помощи, с тем чтобы избежать потенциальных коллизий в законах и положениях, дополнить существующие международные документы и способствовать их применению, а также не препятствовать их эффективной реализации. Таким образом,

рекомендуется тщательно проанализировать не только многосторонние действующие документы, такие как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция о киберпреступности, но и двусторонние и региональные договоренности, такие как Межамериканская конвенция о взаимной помощи в области уголовного правосудия.

В частности, необходимо принять во внимание Конвенцию о киберпреступности (Будапешт, 2001 год), так как она охватывает концепции, которые широко обсуждались, и отражает 20-летний практический международный опыт. В противном случае возникнет риск вступить на путь, который сведет на нет уже достигнутый прогресс в борьбе с киберпреступностью.

Кроме того, в рамках этого процесса следует учесть результаты работы Группы экспертов для проведения всестороннего исследования проблемы киберпреступности в рамках Организации Объединенных Наций и использовать в качестве основы перечень предварительных выводов и рекомендаций, предложенных государствами-членами в ходе совещаний Группы экспертов.

Мы подчеркиваем, что в целях предотвращения будущих споров важно, чтобы работа над новой конвенцией проводилась на основе всеохватного и прозрачного подхода и — насколько это возможно — на основе консенсуса, как это было сделано ранее, при разработке Организацией Объединенных Наций Конвенции против транснациональной организованной преступности и Конвенции против коррупции.

Цель

Общая цель конвенции должна заключаться в принятии рамочной основы международного сотрудничества судебных органов, в полном объеме обеспечивающей предупреждение, расследование и уголовное преследование в контексте противодействия использованию информационно-коммуникационных технологий в преступных целях — киберпреступности — и позволяющей решать вопросы, связанные с электронными доказательствами.

Структура

- Ключевые определения и стандартизированные технологические концепции, которые сохранят свою актуальность с течением времени.
- Материально-правовые положения (составы преступлений, которые должны быть признаны в национальном законодательстве).

В этой связи в конвенции должна быть установлена уголовная ответственность за целый ряд деяний, затрагивающих компьютерные системы и информацию.

С точки зрения принципов и методов работы представляется логичным сосредоточить внимание исключительно на основных киберпреступлениях, включая преступления, связанные с несанкционированным цифровым доступом к компьютерным сетям или системам путем незаконного получения доступа к компьютерной системе; кибершпионаж, который охватывает все деяния, нарушающие неприкосновенность информации физических и юридических лиц путем перехвата или получения данных, сообщений, файлов или баз данных, хранящихся в компьютерных системах или передаваемых по сетям связи, и включает в себя преступления, связанные с перехватом компьютерных данных, нарушением конфиденциальности персональных данных и созданием фишинговых сайтов в целях получения персональных данных; и компьютерный саботаж, целью которого является нарушение работы, повреждение, приведение в негодность, отключение или вмешательство в работу компьютерных систем, баз данных или процессов обработки, передачи и переноса данных, и который включает в себя преступления, связанные с незаконным нарушением работы компьютерных систем или телекоммуникационных сетей.

Кроме того, этот документ мог бы охватывать ряд деяний, которые в силу их совершения с помощью цифровых средств имеют серьезные и далеко идущие последствия и которые трудно расследовать; это позволит сделать конвенцию достаточно гибкой, чтобы она могла служить инструментом борьбы с незаконной деятельностью, связанной с другими правонарушениями:

- положение об обоюдном признании деяния преступлением: этот механизм важен для содействия оказанию взаимной правовой помощи независимо от того, является ли деяние, послужившее основанием для обращения за такой помощью, наказуемым в соответствии с законодательством запрашиваемого государства; тем самым, среди прочего, киберпреступники лишаются возможности найти убежище в некоторых странах в условиях отсутствия общего стандартного законодательства;

- процессуальные положения, обеспечивающие эффективное правовое сотрудничество: в этой связи необходимо активизировать международное сотрудничество в расследовании преступлений, связанных с киберпреступностью, особенно в вопросах управления цифровыми доказательствами, обеспечения сохранности и передачи доказательств и проведения судебной экспертизы. В первую очередь необходимо уделить внимание вопросам передачи и хранения данных, а также определению механизмов, обеспечивающих оперативное взаимодействие между соответствующими органами власти разных государств с помощью надлежащих и защищенных цифровых каналов;

- отягчающие обстоятельства, применимые к действиям, которые затрагивают законное право на защиту информации и данных, такие как действия, связанные с получением персональных данных в больших масштабах, нарушение прав человека или действия, направленные на критическую инфраструктуру и оказание базовых услуг;

- международное сотрудничество судебных органов: содействие направлению запросов о взаимной правовой помощи по цифровым каналам, их расширение и ускорение рассмотрения, при условии обеспечения соответствующих гарантий и с использованием стандартных форматов;

- определение специальных механизмов расследования для сбора цифровых доказательств, особенно в отношении доказательств, хранящихся в разных юрисдикциях;

- важно, чтобы государства-члены согласовали механизмы, обеспечивающие адекватный уровень защиты персональных данных в ходе обмена информацией посредством международного инструмента, не только ввиду той важной роли, которую защита персональных данных начала играть в цифровой среде, но и чтобы определенные правила, действующие в отдельной стране, не могли стать препятствием для эффективного обмена информацией между государствами;

- содействие оказанию технической помощи, распространению знаний и передового опыта в области расследования преступлений, уголовного преследования и наказания виновных. Кроме того, для преодоления цифрового разрыва необходимо, чтобы конвенция охватывала вопросы наращивания потенциала правоохранительных органов и других национальных судебных органов, особенно в том, что касается программ обучения и подготовки кадров как одной из форм предупреждения киберпреступности;

- содействие техническому сотрудничеству через региональные учебные заведения. С учетом сложности и специфики расследования преступлений, совершенных с помощью цифровых средств, что затрудняет их эффективное расследование, необходимо организованно проводить специализированную подготовку прокуроров и следователей на постоянной основе и с опорой на заранее составленные планы работы с указанием ожидаемых результатов;

- огромное значение имеет развитие прочного доверительного сотрудничества между публичным и частным секторами в области киберпреступности, в связи с чем необходимо выработать общую позицию по данному вопросу и упростить сбор цифровых доказательств субъектами, действующими в цифровой сфере, включая поставщиков интернет-услуг и коммуникационные компании;
- поощрение и облегчение доступа органов власти к совместным платформам для наращивания потенциала и обмена информацией, а также к аналитическим и контекстуальным инструментам расследования киберпреступлений;
- положения, упрощающие доступ к своевременной информации в чрезвычайных ситуациях;
- наконец, в конвенции предлагается предусмотреть создание сети контактных центров, работающих круглосуточно, для реагирования на просьбы о международном правовом сотрудничестве в связи с киберпреступлениями. Кроме того, в дополнение к этой сети можно создать сеть контактных лиц для: a) содействия обмену знаниями и опытом в области киберпреступности и связанных с ней правонарушений; b) внедрения и распространения передовой практики; и c) оптимизации и налаживания международного сотрудничества судебных органов.

Доминиканская Республика

[Подлинный текст на испанском языке]
[5 ноября 2021 года]

Доминиканская Республика приветствует возможность внести свой вклад в коллективную работу, проводимую всеми государствами-членами, и представить свои замечания относительно сферы применения, целей и структуры нового международного документа по киберпреступности, в соответствии с резолюциями 74/247 и 75/282 Генеральной Ассамблеи от 27 декабря 2019 года и 26 мая 2021 года, соответственно.

Киберпреступность является новой и одной из наиболее стремительно распространяющихся форм транснациональной преступности в мире. Рост киберпреступности тесно связан с эволюцией и ускоренным развитием информационно-коммуникационных технологий; ежегодно она затрагивает миллионы граждан и предприятий.

Наш регион, Латинская Америка и Карибский бассейн, особенно подвержен этому явлению. Как правило, развивающиеся страны не обладают необходимым потенциалом для борьбы с киберпреступностью, вследствие чего жертвами подобных преступлений становится множество людей.

Кроме того, на фоне пандемии коронавирусного заболевания (COVID-19) стала очевидной уязвимость международного сообщества к киберпреступности, и эта ситуация подчеркнула важность глобальных мер реагирования на основе взаимодействия и координации, причем не только между государствами-членами, но и между правительствами и неправительственными организациями, гражданским обществом, научными кругами и частным сектором, поскольку сложность и масштабы киберпреступлений настолько велики, что в основе любых эффективных мер реагирования должен лежать междисциплинарный подход.

Доминиканская Республика полностью поддерживает это начинание международного сообщества и подтверждает свою готовность работать вместе со всеми государствами-членами над заключением международного договора, который будет представлять каждого из нас, при неизменном соблюдении принципов прозрачности, беспристрастности и инклюзивности.

Сфера применения

По мнению Доминиканской Республики, основная цель нового международного документа по киберпреступности заключается в том, чтобы предоставить эффективный инструмент для предупреждения, выявления и расследования киберпреступлений и уголовного преследования виновных при условии полного соблюдения принципов неприкосновенности информации, защиты данных, уважения гражданских свобод и прав человека.

В частности, этот документ должен способствовать проведению уголовных расследований, обеспечивая своевременный сбор и последующее использование цифровых доказательств, тем самым снижая уровень безнаказанности в случае подобных преступлений, поскольку такая безнаказанность является одним из основных препятствий, с которыми сталкиваются сотрудники правоохранительных органов на местах.

Кроме того, он должен поощрять и упрощать международное сотрудничество между государствами-членами, а также оказание технической помощи и наращивание потенциала в тех государствах-участниках, которым требуется такая поддержка в связи с киберпреступностью.

Доминиканская Республика также считает, что должно быть четко установлено, что сфера применения нового документа должна ограничиваться вопросами киберпреступности; он не должен затрагивать вопросы, связанные с кибербезопасностью и регулированием интернета, которые обсуждаются на других форумах.

Однако мы понимаем, что необходимо принять во внимание положения существующих международных и региональных документов, чтобы избежать нежелательной несовместимости с правовыми системами государств-членов, которые используют эти документы в качестве основы для своего национального законодательства, или с применением этих документов. Соответственно, важно опираться на опыт, накопленный при применении соответствующих документов, выявляя преимущества и недостатки, которые может устранить новая конвенция. Также должны быть приняты во внимание усилия специализированных групп, таких как Группа экспертов для проведения всестороннего исследования проблемы киберпреступности.

Цели

Новый международный документ по предупреждению киберпреступности и борьбы с ней должен, среди прочего, обеспечивать следующее:

- поощрение и упрощение оперативного, практического и эффективного международного сотрудничества между государствами-участниками;
- охват вопросов предупреждения, выявления и расследования киберпреступлений, на которые распространяется действие документа, а также вопросов уголовного преследования виновных и сбор и обработка цифровых доказательств, связанных с другими преступлениями, при условии предоставления государствам-участникам необходимых инструментов для борьбы с этим видом транснациональной преступности;
- четкое установление видов преступлений, к которым будут применяться положения новой конвенции и которые должны считаться противоправными деяниями в правовых системах всех государств-участников;
- поощрение и облегчение деятельности по наращиванию потенциала в государствах-участниках, которые в этом нуждаются, с целью предотвращения создания убежищ для киберпреступников;
- содействие обмену передовым опытом и извлеченными уроками;

- определение четких правил установления юрисдикции для целей запроса цифровых доказательств у «глобальных» поставщиков интернет-услуг, что в настоящее время является одной из самых больших проблем в плане снижения уровня безнаказанности и оказания поддержки жертвам киберпреступлений;
- установление четких гарантий и системы наказаний за несоблюдение этих гарантий;
- установление достаточных полномочий для расследования соответствующих уголовных преступлений при условии неизменного соблюдения принципа неприкосновенности информации, защиты данных, уважения гражданских свобод и прав человека;
- учитывая быстрое развитие технологий, конвенция должна носить широкий и долгосрочный характер; соответственно, следует использовать технологически нейтральные формулировки, с тем чтобы гарантировать актуальность конвенции с учетом развития технологий с течением времени;
- установление междисциплинарного подхода, обеспечивающего активное сотрудничество между публичным и частным секторами.

Структура

- Определения.
- Уголовные преступления.
- Процессуальные механизмы для проведения расследования.
- Гарантии.
- Международное сотрудничество.
- Доступ к цифровым доказательствам.
- Техническая помощь и наращивание потенциала следственных органов.
- Стандартные рабочие процедуры.
- Меры по предупреждению киберпреступлений.
- Механизм реализации.

Египет

[Подлинный текст на арабском языке]
[28 октября 2021 года]

Стремясь внести конструктивный вклад в международные усилия по разработке всеобъемлющей конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях и руководствуясь своими обязательствами по национальным, региональным и международным договорам и конвенциям, касающимся прав человека и противодействия транснациональной преступности, Арабская Республика Египет подготовила настоящее сообщение, в котором в предварительном порядке сформулированы элементы, предлагаемые к включению в упомянутую конвенцию, в расчете на то, что желаемых целей можно достичь путем укрепления международного сотрудничества и выработки общей политики в отношении преступности, направленной на противодействие всем преступлениям в сфере ИКТ с целью предотвращения угроз, создаваемых этими преступлениями для безопасности и интересов государств и благополучия общества и граждан.

I. Цели

Конвенция должна иметь целью укрепление сотрудничества между государствами — членами Организации Объединенных Наций в противодействии использованию ИКТ в преступных целях, обеспечивая предупреждение любых действий, угрожающих целостности и конфиденциальности ИКТ, криминализацию неправомерного использования ИКТ в незаконных целях и облегчая применение средств расследования соответствующих преступлений и преследования совершающих их лиц. Конвенция должна также предусматривать устранение последствий совершения преступлений в сфере ИКТ, включая приостановление операций, связанных с активами, приобретенными в результате совершения какого-либо противоправного деяния, указанного в конвенции, а также конфискацию и возвращение доходов от таких преступлений, за счет предоставления достаточных полномочий для эффективного противодействия преступлениям в сфере ИКТ посредством заключения договоренностей о международном сотрудничестве, облегчающих выявление и расследование подобных преступлений, преследование за их совершение и выдачу.

II. Сфера применения

1. Если в конвенции не предусмотрено иное, она должна применяться для предупреждения преступлений, указанных в самой конвенции.

2. Каждому государству-участнику следует принимать такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений и иных противоправных деяний, признанных таковыми в соответствии с конвенцией, когда они:

a) совершены на территории этого государства-участника; или

b) совершены на борту судна, которое несет флаг этого государства-участника, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого государства-участника в такой момент; или

c) имеют транснациональный характер и к их совершению причастна организованная преступная группа. Преступление должно считаться транснациональным по сути, если оно совершено: i) более чем в одной стране; ii) в одной стране, но частично подготовлено или спланировано в другой стране, либо руководство им или контроль над ним осуществлялись в другой стране; iii) в одной стране организованной преступной группой, которая осуществляет преступную деятельность в более чем одной стране; или iv) в одной стране, но его совершение приводит к серьезным последствиям в другой стране.

3. Для целей осуществления конвенции, если в ней не предусмотрено иное, не должно являться необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен имущественный вред.

4. Государствам-участникам следует рассмотреть возможность ограничения использования заявления об оговорках, чтобы обеспечить широкое применение вышеупомянутых мер.

III. Защита суверенитета

1. Каждому государству-участнику в соответствии с его внутренним законодательством и конституционными принципами следует выполнять свои обязательства, возникающие в связи с применением конвенции, в соответствии с принципами суверенного равенства государств и невмешательства во внутренние дела других государств.

2. Конвенция не должна наделять компетентные органы государства-участника правом осуществлять на территории другого государства-участника юрисдикцию и функции, которые относятся к исключительной компетенции органов этого другого государства в соответствии с его внутренним законодательством.

IV. Преступления, которые предлагается охватить Конвенцией

1. Каждому государству-участнику следует принимать такие законодательные и иные меры, какие могут потребоваться, с тем чтобы предотвращать совершение преступлений, указанных в конвенции, или любых других преступлений в сфере ИКТ, включая блокирование и удаление контента, связанного с такими преступлениями; выявлять преступления; осуществлять преследование виновных; осуществлять выдачу преступников; упрощать процедуры, необходимые для международного сотрудничества и сбора доказательств.

2. Каждому государству-участнику следует также принимать такие законодательные и другие меры, какие могут потребоваться, с тем чтобы ввести уголовную ответственность за совершение нижеследующих деяний.

Статья 1. Неправомерное использование информационно-коммуникационных услуг и технологий, включая получение неправомерной выгоды или содействие в получении другими лицами неправомерной выгоды от использования телекоммуникационных услуг либо аудио- или видеоканалов, транслируемых с помощью информационных сетей или устройств ИКТ.

Статья 2. Неправомерный доступ и/или превышение прав доступа, включая:

1. использование полученных полномочий на доступ к сайту, личной учетной записи или информационной системе с превышением этих полномочий в том, что касается продолжительности или уровня доступа;

2. неправомерный доступ ко всей информационно-технологической системе или к ее части либо связь со всей системой или ее частью, а также продолжение использования такого доступа или связи;

3. строгость наказания за это преступление должна повышаться в том случае, если подобный доступ или связь:

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

b) обеспечивают доступ к конфиденциальной государственной информации.

Статья 3. Атака на сайт посредством неправомерного повреждения, нарушения работы, замедления, искажения, сокрытия сайта компании, учреждения, объекта или физического лица или изменения оформления сайта.

Статья 4. Преднамеренный и неправомерный перехват потока данных любыми техническими средствами или посредством прерывания передачи или приема данных информационных технологий.

Статья 5. Нарушение целостности данных посредством преднамеренного и неправомерного уничтожения, стирания, препятствования передаче, модификации или блокирования данных информационных технологий.

Статья 6. Противоправное использование информационных технологий посредством производства, продажи, покупки, импортирования, распространения, предоставления или хранения любых спроектированных или адаптированных программных средств или программного обеспечения, паролей или схожей информации, с помощью которых можно получить доступ к информационной системе с намерением использовать ее для совершения одного из преступлений, указанных в конвенции, или создание вредоносных программ, предназначенных для уничтожения, блокирования, модификации, копирования, распространения цифровой информации или

нейтрализации средств ее защиты, за исключением случаев правомерного проведения исследований.

Статья 7. Фальсифицирование с использованием информационных технологий, нацеленное на нарушение достоверности информации с причинением ущерба и осуществляемое с намерением использовать измененную информацию в качестве достоверной.

Статья 8. Мошенничество посредством преднамеренного и неправомерного причинения ущерба бенефициарам и пользователям, осуществляемое с намерением незаконного достижения интересов правонарушителя или других лиц и получения ими выгод, в том числе в форме мошеннических электронных преступлений, связанных с виртуальной валютой (цифровой валютой или криптовалютой).

Статья 9. Угрозы или вымогательство посредством использования ИКТ 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 10. Порнография, при следующих условиях:

1. ИКТ используются для изготовления, показа, распространения, передачи, опубликования, покупки, продажи или импортирования порнографических материалов в непристойных целях;

2. ИКТ используются для изготовления, показа, распространения, передачи, опубликования, покупки, продажи или импортирования материалов детской порнографии или порнографии несовершеннолетних, включая хранение таких материалов или материалов с непристойными изображениями детей или несовершеннолетних в системах ИКТ или на любом носителе ИКТ.

Статья 11. Другие преступления, связанные с порнографией, включая сексуальную эксплуатацию или домогательства, в особенности в отношении женщин, детей или несовершеннолетних.

Статья 12. Побуждение или принуждение к совершению самоубийства, в том числе побуждение или принуждение к совершению самоубийства несовершеннолетних, посредством психологического или иного давления через информационно-коммуникационные сети, включая интернет, как в процессе прямого взаимодействия, так и с помощью популярных технологий или электронных игр.

Статья 13. Использование ИКТ для вовлечения несовершеннолетних в совершение противоправных действий, представляющих опасность для их жизни либо для их физического или психического здоровья.

Статья 14. Использование ИКТ для нарушения права на неприкосновенность частной жизни, в том числе посредством создания адреса электронной почты, сайта или личной учетной записи и их ложной идентификации с каким-либо физическим или юридическим лицом.

Статья 15. Использование информационных технологий для совершения террористических преступлений, включая:

1. распространение идей и принципов террористических групп или оправдание терроризма;

2. финансирование террористических операций или обучения проведению таких операций, содействие коммуникации между террористическим организациями или оказание логистической поддержки лицам, осуществляющим террористические операции;

3. распространение информации о методах изготовления взрывных устройств, особенно предназначенных для использования в террористических операциях;

4. распространение фанатизма, призывов к мятежу, ненависти или расизма;

5. государствам-участникам следует принять необходимые меры для запрещения распространения информации подобного содержания средствами ИКТ, включая блокирование и удаление контента, имеющего отношение к этим преступлениям.

Статья 16. Финансовые преступления, например отмывание денежных средств, в том числе:

1. использование ИКТ для совершения финансовых преступлений или противоправного использования виртуальной валюты (цифровой валюты или криптовалюты);

2. совершение операций по отмыванию денежных средств либо обращение за помощью в отмывании денежных средств, или распространение информации о методах отмывания денежных средств.

Статья 17. Незаконное использование электронных средств платежа, в том числе:

1. подделывание, фальсификация любого электронного средства платежа или создание любым способом какого-либо устройства или материала, позволяющего подделывать или имитировать любое электронное средство платежа;

2. присвоение данных любого средства платежа, использование таких данных, предоставление данных другим лицам или содействие в получении таких данных другими лицами;

3. использование информационных сетей или информационных технологий для получения несанкционированного доступа к коду или данным средства платежа;

4. сознательное принятие поддельного средства платежа.

Статья 18. Совершенные с использованием информационных технологий преступления, имеющие отношение к организованной преступности или транснациональной преступности, в том числе:

1. сбыт или оборот наркотических средств или психотропных веществ;

2. незаконное распространение фальсифицированных лекарственных средств или медицинских изделий;

3. незаконный ввоз мигрантов;

4. торговля людьми;

5. торговля человеческими органами;

6. незаконная торговля оружием;

7. незаконный оборот культурных ценностей.

Статья 19. Преступления, связанные с нарушением авторских и смежных прав, включая нарушение авторских и смежных прав в соответствии с определением, действующим в законодательстве государства-участника, если такие действия совершаются умышленно.

Статья 20. Несанкционированный доступ к критической информационной инфраструктуре, включая:

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, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты;

2. нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой цифровой информации, содержащейся в критической информационной инфраструктуре или информационных системах, или информации, охраняемой в соответствии с внутренним законодательством государства-участника, а также правил эксплуатации коммуникационных сетей, относящихся к критической информационной инфраструктуре, либо нарушение правил доступа к ним, если оно нанесло ущерб критической информационной инфраструктуре.

Статья 21. Подстрекательство к подрывной или вооруженной деятельности или другие преступления, в том числе совершенные с использованием ИКТ призывы к проведению подрывных или вооруженных действий, направленных против правительства другого государства и угрожающих общественной безопасности и стабильности, либо призывы к совершению преступлений, за которые предусмотрено наказание в виде лишения свободы сроком не менее одного года.

Статья 22. Преступления, связанные с экстремистской деятельностью, включая распространение материалов, пропагандирующих или оправдывающих совершение противоправных деяний по политическим, идеологическим, социальным или этническим мотивам либо возбуждающих этническую или религиозную ненависть или вражду в целом; либо обеспечение доступа к таким материалам.

Статья 23. Попытка совершения любого преступления, признанного таковым в соответствии с конвенцией, в том числе участие в качестве пособника в совершении любого правонарушения, признанного таковым в соответствии с конвенцией, и/или организация других лиц либо руководство ими с целью совершения такого преступления.

Статья 24. Иные противоправные деяния

Конвенция не должна являться препятствием для признания государством-участником в качестве преступления любого другого противоправного деяния, совершенного умышленно с использованием ИКТ и повлекшего существенный ущерб.

V. Юридическая ответственность, уголовный процесс, правоохранительная деятельность и международная правовая помощь

Статья 1. Ответственность юридических лиц

Каждому государству-участнику в соответствии со своим внутренним законодательством следует установить для юридических лиц уголовную ответственность за любые преступления, совершенные их представителями или в их интересах, что не должно исключать вынесения наказаний физическим лицам, совершившим данное преступление, например администратору сайта.

Статья 2. Ответственность поставщиков услуг/администраторов сайтов

Без ущерба для положений конвенции поставщики услуг/администраторы сайтов и их подчиненные должны выполнять следующие требования, нарушение которых должно влечь за собой уголовную ответственность:

1. сохранение и хранение файла журнала информационной системы или файла журнала любой информационной технологии в течение периода

времени, который предстоит определить. Сохранять и хранить необходимо в том числе следующие данные:

a) данные, позволяющие идентифицировать пользователей услуг;

b) данные, относящиеся к контенту информационной системы клиента, в тех случаях, когда она находится под контролем поставщика услуг;

c) данные о трафике связи;

d) данные о периферийных устройствах связи;

e) любые другие данные, определенные государством для целей осуществления конвенции;

2. соблюдение конфиденциальности сохраненных и хранимых данных, включая личные данные любого пользователя услуг либо какие бы то ни было 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;

3. обеспечение защиты данных и информации с соблюдением их конфиденциальности и недопущением их утечки и повреждения;

4. поставщик услуг/администратор сайта должен предоставлять пользователям услуг и любому компетентному органу нижеследующие данные и информацию в такой форме и таким образом, чтобы к ним обеспечивался удобный, прямой и непрерывный доступ:

a) название и адрес поставщика услуг;

b) контактная информация поставщика услуг, включая адрес электронной почты;

c) данные лицензии, идентифицирующие поставщика услуг и компетентный орган, осуществляющий надзор за его деятельностью;

5. поставщик услуг/администратор сайта по просьбе компетентных органов, определенных государством, должен предоставлять в их распоряжение все технические средства, позволяющие им осуществлять свои полномочия.

Статья 3. Уголовный процесс

1. Каждое государство-участник принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы утвердить полномочия и процедуры для предупреждения, выявления, обнаружения, расследования преступлений и других противоправных актов и возбуждения дел в связи с ними.

2. Каждому государству-участнику следует применять вышеуказанные полномочия и процедуры в отношении:

a) уголовно наказуемых и других противоправных деяний, предусмотренных в конвенции;

b) других преступлений и иных противоправных деяний, совершенных с использованием ИКТ;

c) электронного сбора доказательств преступлений.

3. Уголовный процесс должен включать:

a) оперативное обеспечение сохранности данных, хранимых с использованием информационных технологий, в том числе технических параметров трафика, хранимых с использованием информационных технологий (в особенности при наличии оснований предполагать, что подобная информация может быть утрачена или изменена), посредством вынесения распоряжения о том, чтобы

соответствующее лицо обеспечивало целостность информации, которая находится в его владении или под его контролем, с тем чтобы компетентные органы могли осуществлять поиск и расследование, при обеспечении конфиденциальности любых мер, принимаемых в этой связи;

b) оперативное обеспечение сохранности и частичное раскрытие данных о технических параметрах трафика независимо от того, передают информацию один или несколько поставщиков услуг, и обеспечение того, чтобы компетентные органы оперативно раскрывали достаточное количество информации в объеме, позволяющем идентифицировать поставщика услуг и определять маршрут передачи информации;

c) вынесение распоряжений о передаче информации, находящейся во владении какого-либо лица на территории того или иного государства-участника и хранимой в информационной системе или на носителе информации, либо находящейся во владении поставщика услуг, предоставляющего услуги на территории государства-участника или под его контролем;

d) изучение информации, хранимой в информационной системе или на носителе информации, или доступ к такой информации;

e) контроль над хранимой информацией, ее копирование и сохранение в целях выполнения процедур поиска информации и получения доступа к ней;

f) сбор технических параметров трафика в режиме реального времени и введение для поставщиков услуг, находящихся в пределах данной юрисдикции, обязанности осуществлять сбор и регистрацию информации и обеспечивать ее конфиденциальность;

g) перехват информационного контента, позволяющий компетентным органам с помощью технических средств собирать и регистрировать в режиме реального времени информацию, передаваемую с использованием ИКТ;

h) каждому государству-участнику следует принять необходимые законодательные и иные меры, позволяющие его компетентным органам останавливать передачу и трансляцию любого контента, являющегося преступным в соответствии с конвенцией.

4. Признание цифровых доказательств

Цифровые доказательства, полученные или извлеченные из устройств, оборудования, электронных носителей информации, информационных систем, компьютерных программ или любых средств ИКТ, должны иметь ценность и доказательную силу вещественных судебных доказательств по уголовным делам при условии, что такие цифровые доказательства отвечают техническим требованиям, установленным в законодательстве государств-участников.

Статья 4. Международное правовое и судебное сотрудничество

1. Государствам-участникам следует развивать сотрудничество друг с другом в соответствии с конвенцией или принципом взаимности для обмена информацией с целью предупреждения совершения преступлений в сфере информационных технологий, оказания помощи в расследовании таких преступлений и отслеживания лиц, которые их совершают.

2. Государствам-участникам следует осуществлять максимально широкое сотрудничество в соответствии с положениями настоящей статьи и путем применения соответствующих международно-правовых документов о международном сотрудничестве по уголовным делам, а также в соответствии с принципом взаимности и применимым внутренним законодательством, в целях предупреждения, пресечения, выявления преступлений в сфере использования ИКТ и преследования за их совершение.

3. Для целей выдачи и взаимной правовой помощи по уголовным делам ни одно из преступлений, указанных в конвенции, не должно рассматриваться как

политическое преступление. В силу этого запрос о выдаче или оказании правовой помощи по уголовным делам в связи с подобными преступлениями не может быть отклонен на том основании, что он касается политического преступления, преступления, связанного с политическим преступлением, или преступления, совершенного по политическим мотивам.

5. Юрисдикция

Каждое государство-участник должно принять необходимые меры для установления своей юрисдикции в отношении вышеупомянутых преступлений, если:

a) преступление совершено или исполнено, полностью или частично, на территории этого государства-участника;

b) преступление совершено или исполнено, полностью или частично, на борту судна, которое несло флаг этого государства-участника;

c) преступление совершено или исполнено, полностью или частично, на борту воздушного судна, которое зарегистрировано в соответствии с законодательством этого государства-участника;

d) преступление совершено или исполнено, полностью или частично, гражданином этого государства-участника в тех случаях, когда за преступление предусмотрено наказание во внутреннем законодательстве в месте его совершения или когда оно совершено вне юрисдикции какого бы то ни было государства;

e) преступление затрагивает какой-либо из высших интересов государства.

6. Выдача

a) Государствам-членам следует производить обмен преступниками, совершившими вышеописанные преступления, при условии, что по их законодательству данные преступления являются уголовно наказуемыми. Государство-участник, если это разрешено его законодательством, может удовлетворить просьбу о выдаче лица, совершившего преступление, указанное в конвенции, но не являющееся уголовно наказуемым согласно его собственному законодательству.

b) Указанные выше преступления должны считаться включенными в любой существующий между государствами-участниками договор о выдаче в качестве преступлений, которые могут повлечь выдачу совершивших их лиц.

c) Если государство-участник, обусловливающее выдачу наличием договора, получает просьбу о выдаче от другого государства-участника, с которым оно не имеет договора о выдаче, оно может рассматривать конвенцию в качестве правового основания для выдачи.

d) Выдача осуществляется в соответствии с условиями, предусматриваемыми законодательством запрашиваемого государства-участника, или условиями, закрепленными в применимых договорах о выдаче, включая условия, касающиеся оснований, на которых государство-участник может отказать в выдаче.

e) Каждое государство-участник может отказаться от выдачи своих граждан, однако в этом случае ему следует, в пределах своей юрисдикции, предъявить обвинение своему гражданину, совершившему в любом другом государстве-участнике преступление, за которое по законодательству обоих государств-участников предусматривается наказание в виде лишения свободы, если другое государство-участник направит ему просьбу о преследовании данного гражданина, к которой будут прилагаться имеющиеся в его распоряжении необходимые материалы, документы, сведения и доказательства. Запрашивающее государство-участник следует информировать о том, какие меры были приняты в отношении его просьбы, а также должно быть вынесено определение

относительно национальности преступника на дату совершения преступления, в отношении которого поступает запрос о выдаче.

f) В отношении любого преступления, к которому применяется настоящая статья, государствам-участникам, при условии соблюдения их внутреннего законодательства, следует прилагать усилия к тому, чтобы ускорить процедуры выдачи и упростить связанные с ней требования о предоставлении доказательств.

g) При условии соблюдения положений своего внутреннего законодательства и договоров о выдаче и по просьбе запрашивающего государства-участника запрашиваемое государство-участник, убедившись в том, что обстоятельства требуют этого и носят неотложный характер, может взять под стражу находящееся на его территории лицо, выдача которого запрашивается, или принять другие надлежащие меры для обеспечения его присутствия в ходе процедуры выдачи.

h) Если запрос о выдаче, направленный с целью исполнения судебного постановления, отклоняется на том основании, что лицо, чья выдача запрашивается, является гражданином запрашиваемого государства-участника, последнему при поступлении соответствующей просьбы запрашивающего государства-участника следует, если это разрешено его внутренним законодательством и в соответствии с ним, рассмотреть вопрос об обеспечении исполнения наказания, предусмотренного внутренним законодательством запрашивающей стороны, или любой еще не исполненной части такого наказания.

i) Любому лицу, по делу которого осуществляется производство в связи с любым преступлением, к которому применяется настоящая статья, должно гарантироваться справедливое обращение на всех стадиях производства, включая осуществление всех прав и гарантий, предусмотренных внутренним законодательством государства-участника, на территории которого находится это лицо.

j) Ничто в конвенции не должно толковаться как устанавливающее обязательство выдачи, если у запрашиваемого государства-участника имеются существенные основания полагать, что просьба о выдаче имеет целью преследование или наказание какого-либо лица по причине его пола, расы, языка, вероисповедания или гражданства или что удовлетворение этой просьбы нанесло бы ущерб положению этого лица по любой из этих причин.

k) Государства-участники не могут отказывать в выполнении запросов о выдаче только на том основании, что преступление, о котором идет речь, связано с финансовыми вопросами.

l) До отказа в выдаче запрашиваемому государству-участнику, в надлежащих случаях, следует провести консультации с запрашивающим государством-участником, с тем чтобы предоставить последнему достаточные возможности для изложения его мнений и представления информации, имеющей отношение к изложенным в его запросе фактам.

m) Необходимо, чтобы каждое государство-участник при сдаче на хранение своей ратификационной грамоты или документа о принятии было обязано сообщать специализированному органу, который предстоит согласовать, контактную информацию органа, ответственного за обработку запросов о выдаче или за процессуальное задержание, и периодически обновлять эту информацию.

7. Взаимная помощь

a) Всем государствам-участникам следует в максимально возможном объеме оказывать взаимную правовую помощь для целей расследований, выполнения процедур, связанных с преступлениями в сфере информации и информационных технологий, или сбора электронных доказательств преступлений.

b) Запрос о помощи на двусторонней основе и все связанные с ними сообщения должны направляться в письменном виде. В чрезвычайных ситуациях

каждое государство-участник может направить срочный запрос, в том числе по электронной почте, при условии, что подобные сообщения защищены (в том числе с применением шифрования) и адресованы надлежащим образом, а их получение подтверждается по просьбе государства-участника.

c) За исключением случаев, предусмотренных в конвенции, оказание помощи на двусторонней основе должно производиться на условиях, оговоренных в законодательстве запрашиваемого государства или в договорах об оказании взаимной помощи, включая условия, касающиеся оснований, на которых запрашиваемое государство может отказаться от сотрудничества.

d) В тех случаях, когда государство-участник, которому направлен запрос о взаимной помощи, может оказать такую помощь только при условии, что конкретное деяние признается преступлением обеими государствами, это условие должно считаться выполненным независимо от того, отнесено ли соответствующее преступление в законодательстве государства-участника к той же категории, что и в запрашивающем государстве-участнике.

8. Информация, предоставляемая в инициативном порядке

Государство-участник может с соблюдением норм своего внутреннего законодательства направить без предварительного запроса другого государства-участника информацию, полученную в рамках своего расследования, когда, по его мнению, раскрытие такой информации могло бы помочь другому государству-участнику начать или провести расследование преступлений, признанных таковыми в соответствии с конвенцией, или могло бы повлечь за собой направление этим государством-участником запроса о сотрудничестве.

9. Процедуры, связанные с запросами о сотрудничестве и взаимной помощи

a) Подпункты настоящего пункта должны применяться при отсутствии между запрашивающим и запрашиваемым государствами-участниками договора или соглашения о взаимной помощи и сотрудничестве, заключенных на основе действующего законодательства. При наличии подобного договора или соглашения указанные подпункты на применяются, за исключением тех случаев, когда соответствующие стороны соглашаются применять их в полном объеме или частично.

b) Каждому государству-участнику следует назначить центральный орган, который будет передавать, принимать и выполнять запросы о взаимной правовой помощи или направлять их компетентному органу. Контактная информация центрального органа должна периодически обновляться.

c) Предусмотренные в настоящей статье запросы о взаимной помощи должны исполняться в соответствии с процессуальными нормами, указанными запрашивающим государством-участником, если они не противоречат законодательству запрашиваемого государства-участника.

d) Запрашиваемое государство-участник может отложить принятие мер по запросу, если такие меры могут влиять на уголовные расследования, проводимые его компетентными органами.

e) Прежде чем отказать в предоставлении помощи или отсрочить ее оказание, запрашиваемому государству-участнику после консультаций с запрашивающим государством-участником следует определить, необходимо ли удовлетворить запрос частично или на таких условиях, какие оно сочтет необходимыми.

f) Запрашиваемому государству-участнику следует информировать запрашивающее государство-участник о результатах выполнения запроса. Необходимо, чтобы в случае отказа в выполнении запроса или отсрочки его окончательного выполнения запрашиваемое государство-участник было обязано сообщать запрашивающему государству-участнику причины такого отказа или существенной отсрочки.

g) Запрашивающее государство-участник может просить запрашиваемое государство-участник сохранять конфиденциальность запроса, но лишь в той степени, которая согласуется с его выполнением. Если запрашиваемое государство-участник не может выполнить просьбу о конфиденциальности, ему следует сообщить об этом запрашивающему государству-участнику. В этом случае запрашивающее государство-участник принимает решение о том, в какой степени может быть выполнен запрос.

h) В неотложных случаях запросы о взаимной помощи могут направляться напрямую судебным органам в запрашиваемом государстве-участнике от аналогичных органов в запрашивающем государстве-участнике. В таких случаях копия запроса должна направляться одновременно центральным органом запрашивающего государства-участника в центральный орган запрашиваемого государства-участника.

i) Сообщения и запросы, о которых идет речь в предыдущем подпункте, могут направляться через Международную организацию уголовной полиции (Интерпол).

10. Отказ в оказании помощи

a) Запрашиваемое государство-участник помимо отказа в помощи на основаниях, изложенных в предыдущих пунктах, может отказать в оказании помощи, если оно считает, что выполнение запроса нарушит его суверенитет, безопасность, порядок или основные интересы.

b) В выполнении запроса об оказании правовой помощи по делам о преступлениях, указанных в конвенции, не может быть отказано на основании того, что преступления носят политический или схожий характер.

11. Конфиденциальность и ограничения на использование информации

В случае отсутствия между запрашивающим и запрашиваемым государствами-участниками договора или соглашения о взаимной помощи, опирающихся на действующее законодательство, применяются положения настоящей статьи. При наличии такого договора или соглашения настоящая статья не применяется, если только заинтересованные государства-участники не соглашаются применять все ее положения или их часть.

12. Оперативное обеспечение сохранности информации, хранимой в информационных системах

a) Любое государство-участник может просить другое государство-участник безотлагательно обеспечить сохранность информации, которая хранится с использованием информационных технологий на территории этого государства-участника и в отношении которой запрашивающее государство-участник намеревается в рамках взаимной правовой помощи направить запрос об оказании взаимной помощи с целью поиска сведений среди этой информации, ее выемки, защиты или раскрытия.

b) Запрашиваемое государство-участник может отказать в исполнении запроса об обеспечении сохранности информации, если оно полагает, что исполнение такого запроса может угрожать его суверенитету, безопасности, порядку или интересам.

13. Если в ходе исполнения запроса об обеспечении сохранности технических параметров трафика, относящихся к передаче определенной информации, запрашиваемому государству-участнику станет известно, что в передаче информации участвовал поставщик услуг с территории иного государства, оно раскрывает в порядке, установленном национальным законодательством, запрашивающему государству-участнику технические параметры трафика в объеме, позволяющем идентифицировать этого поставщика услуг и определить маршрут передачи информации, сохранение которой запрашивается.

14. Двустороннее сотрудничество и помощь, связанные с доступом к хранимым данным информационных технологий

a) Любое государство-участник может просить другое государство-участник произвести поиск данных информационных технологий, хранимых и находящихся на территории запрашиваемого государства-участника, включая сохраненную информацию, предоставить доступ к таким данным, изъять их, обеспечить их защиту или раскрыть такие данные.

b) Необходимо, чтобы запрашиваемое государство-участник было обязано выполнить просьбу запрашивающего государства-участника в соответствии с положениями конвенции.

c) Если необходимая информация может быть утеряна или изменена, реагирование на запрос должно производиться безотлагательно.

15. Трансграничный доступ к данным информационных технологий

Любое государство-участник может без получения разрешения другого государства-участника воспользоваться данными информационных технологий, находящимися в открытом доступе (с открытым кодом), независимо от географического местонахождения этой информации.

16. Двустороннее сотрудничество и помощь по сбору технических параметров трафика в режиме реального времени

a) Государствам-участникам следует на двусторонней основе оказывать друг другу помощь в сборе в режиме реального времени технических параметров трафика, связанных с передачей определенной информации на их территории и передаваемых с помощью информационных технологий.

b) Каждому государству-участнику следует оказывать такую помощь по меньшей мере в делах о преступлениях, аналогичных тем, для которых внутреннее законодательство позволяет осуществлять сбор технических параметров трафика в режиме реального времени.

17. Двустороннее сотрудничество и помощь в отношении содержания информации

Необходимо, чтобы государства-участники были обязаны оказывать друг другу двустороннюю помощь, связанную со сбором в режиме реального времени данных о содержании определенной информации, передаваемой с помощью информационных технологий, в той степени, в которой это позволяют применимые договоры и национальное законодательство.

18. Специализированное учреждение

a) Каждому государству-участнику в соответствии с основополагающими принципами его правовой системы следует обеспечить наличие специализированного учреждения, которое круглосуточно и без выходных будет отвечать исключительно за оказание экстренной помощи в проведении расследований или выполнении процессуальных действий, связанных с преступлениями в сфере информационных технологий, или сборе доказательств в электронной форме по конкретному преступлению. Подобная помощь должна включать содействие выполнению либо непосредственно выполнение следующих действий:

i) оказание технической консультативной помощи;

ii) обеспечение сохранности информации согласно соответствующим статьям;

iii) сбор доказательств, предоставление правовой информации и установление местонахождения подозреваемых.

b) Специализированное учреждение в каждом государстве-участнике должно располагать возможностями для экстренной связи с аналогичными учреждениями в других государствах-участниках.

c) Если специализированное учреждение, назначенное тем или иным государством-участником, не входит в состав ведомств данного государства-участника, отвечающих за оказание международной помощи на двусторонней основе, то специализированное учреждение должно иметь возможность оперативно взаимодействовать с этими ведомствами.

d) Каждому государству-участнику следует обеспечить укомплектование вышеупомянутого учреждения квалифицированными кадрами.

VI. Техническая помощь и подготовка кадров

1. Общие принципы технической помощи

a) Государствам-участникам следует рассмотреть вопрос о предоставлении друг другу широкой технической помощи, особенно в интересах развивающихся стран, в связи с их планами и программами по борьбе с преступлениями в сфере ИКТ, включая материальную поддержку и подготовку кадров в областях, указанных в конвенции, а также подготовку кадров, оказание помощи, передачу технологий и знаний и обмен соответствующим передовым опытом и специальными знаниями, что будет способствовать международному сотрудничеству между государствами-участниками по вопросам выдачи и взаимной правовой помощи.

b) Государствам-участникам необходимо активизировать усилия, направленные на максимальное повышение эффективности практических и учебных мероприятий в международных и региональных организациях и в рамках соответствующих двусторонних и многосторонних соглашений или договоренностей.

c) Государствам-участникам следует рассмотреть возможность оказания друг другу содействия, по просьбе, в проведении оценок, исследований и разработок, касающихся видов, причин и последствий преступлений, совершаемых в сфере ИКТ в их странах, с целью разработки, с участием компетентных органов и основных субъектов, стратегий и планов действий по борьбе с этими видами преступлений.

d) Государствам-участникам следует рассмотреть вопрос о создании механизмов финансирования, позволяющих по линии программ и проектов технической помощи оказывать развивающимся странам помощь в их деятельности.

e) Государствам-участникам следует рассмотреть возможность обмена информацией о правовых, политических или технологических нововведениях, касающихся борьбы с киберпреступностью и сбора доказательств в электронной форме.

2. Подготовка кадров и наращивание потенциала

a) Каждому государству-участнику следует по мере необходимости разрабатывать, осуществлять или совершенствовать конкретные программы подготовки своего персонала, несущего ответственность за предупреждение преступлений в сфере ИКТ и борьбу с ними. Такие программы подготовки кадров могут затрагивать следующие области:

i) эффективные меры по предупреждению, выявлению и расследованию преступлений в сфере ИКТ, а также наказанию за их совершение и борьбе с ними, включая методы сбора и использования доказательств в электронной форме и расследования;

ii) предупреждение перевода доходов от преступлений, признанных таковыми в соответствии с конвенцией, а также изъятие таких доходов;

iii) выявление и приостановление операций по переводу доходов от преступлений, признанных таковыми в соответствии с конвенцией; отслеживание перемещения доходов от преступлений, признанных таковыми в

соответствии с конвенцией; отслеживание методов, используемых для перевода, сокрытия или утаивания таких доходов;

iv) создание надлежащих и действенных правовых и административных механизмов и методов, способствующих изъятию и конфискации доходов от преступлений, признанных таковыми в соответствии с конвенцией;

v) методы, используемые в защите потерпевших и свидетелей, которые сотрудничают с судебными и правоохранительными органами;

vi) разработка и планирование стратегической политики противодействия преступлениям в сфере ИКТ. Странам следует вкладывать средства в создание и наращивание потенциала в области цифровой криминалистики, включая подготовку кадров и повышение квалификации в сфере безопасности, а также в системы управления информационной безопасностью для содействия успешному судебному преследованию по делам, связанным с киберпреступностью, посредством проверки электронных устройств с целью сбора доказательств надежным образом;

vii) составление запросов о взаимной правовой помощи, удовлетворяющих условиям, предусмотренным в конвенции;

viii) расследование киберпреступлений, обращение с электронными доказательствами, обеспечение хранения и передачи доказательств и проведение судебной экспертизы;

ix) организация языковой и профессиональной подготовки по всем направлениям деятельности, связанной с противодействием преступлениям в сфере ИКТ, а также с защитой и упрощением коммуникации со специализированными учреждениями с целью выявления соответствующих преступлений и осуществления контроля за ними.

b) Государства-участники, обладающие более развитым потенциалом и инфраструктурой в области борьбы с киберпреступностью, должны брать на себя соразмерную этому потенциалу ответственность при оказании правовой помощи другим государствам, в особенности развивающимся странам, равно как и ответственность за оказание им поддержки, консультативных услуг и передачу знаний в сфере противодействия киберпреступности.

Европейский союз и его государства-члены

[Подлинный текст на английском языке]
[2 ноября 2021 года]

Настоящий документ отражает мнения и позицию Европейского союза и его государств-членов[1], связанные со сферой применения, целями и структурой (элементами), которые следует принять во внимание при разработке новой конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях и которые призваны содействовать подготовке первой сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, учрежденного с этой целью в соответствии с резолюцией 74/247 Генеральной Ассамблеи.

Настоящий документ не предопределяет будущие позиции, которые Европейский союз и его государства-члены могут занять в ходе дальнейших

[1] Австрия, Бельгия, Болгария, Венгрия, Германия, Греция, Дания, Ирландия, Испания, Италия, Кипр, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Соединенное Королевство Великобритании и Северной Ирландии, Финляндия, Франция, Хорватия, Чехия, Швеция и Эстония.

переговоров о сфере применения, целях и структуре будущей конвенции Организации Объединенных Наций.

I. Цели

Европейский союз и его государства-члены подчеркивают, что будущая конвенция Организации Объединенных Наций должна стать практическим инструментом для правоохранительных и судебных органов в борьбе с киберпреступностью на глобальном уровне в целях повышения эффективности международного сотрудничества. Как отмечено в резолюциях 74/247 и 75/282 Генеральной Ассамблеи, при разработке будущей конвенции Организации Объединенных Наций следует в полной мере учитывать существующие концепции хорошо зарекомендовавших себя международных и региональных документов по борьбе с организованной преступностью и киберпреступностью. Соответственно, любая новая конвенция должна носить дополняющий характер и ни в коей мере не мешать применению действующих документов или присоединению к ним новых государств, а также, насколько это возможно, не допускать дублирования.

Будущая конвенция Организации Объединенных Наций должна предусматривать защиту прав человека и основных свобод, которые действуют как в интернете, так и за его пределами, и быть совместимой с соответствующими документами в этой области.

Будущая конвенция Организации Объединенных Наций, как подтверждено Генеральной Ассамблеей в ее резолюции 75/282, должна в полной мере учитывать работу[2] и итоги работы[3] Межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности.

II. Сфера применения

В связи с этим Европейский союз и его государства-члены считают, что сфера применения будущей конвенции Организации Объединенных Наций должна в основном касаться материального уголовного права и уголовно-процессуального права, а также соответствующих механизмов сотрудничества. Также конвенция должна соответствовать международным правозащитным стандартам и быть направлена на борьбу с киберпреступностью наиболее эффективным образом, обеспечивая тем самым защиту жертв.

Европейский союз и его государства-члены считают, что в этом новом документе следует дать точное определение используемых в нем терминов и отдать предпочтение понятиям, уже согласованным в действующих международных текстах.

Европейский союз и его государства-члены рекомендуют обеспечить компактность содержания этой конвенции и уделить основное внимание ключевым элементам уголовного правосудия, максимально исключив, таким образом, любые вспомогательные элементы.

С учетом изложенных выше принципов Европейский союз и его государства-члены считают, что в будущую конвенцию Организации Объединенных Наций должны быть включены следующие элементы:

1. **Положения материального уголовного права**, связанные с киберпреступлениями, в отношении которых всем государствам — участникам будущей конвенции Организации Объединенных Наций следует установить уголовную ответственность. В целом такие положения должны касаться только высокотехнологичных преступлений и киберзависимых преступлений, таких как

[2] См. www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.
[3] См. UNODC/CCPCJ/EG.4/2021/2.

незаконное получение доступа к компьютерным данным и системам, перехват компьютерных данных и вмешательство в работу компьютерных систем[4].

Положения материального уголовного права должны быть четко и узко определены и полностью соответствовать международным стандартам в области прав человека, а также принципам глобального, открытого, свободного, стабильного и безопасного киберпространства. В случае криминализации в рамках будущей конвенции Организации Объединенных Наций или других универсальных правовых инструментов видов действий, которые определены недостаточно четко, может возникнуть риск неоправданного и несоразмерного вмешательства в права человека и основные свободы, включая право на свободу слова и выражения, и правовая неопределенность.

Положения материального уголовного права следует, насколько это возможно, изложить в технически нейтральных формулировках, чтобы охватить технические достижения будущего[5]. В то же время следует поощрять обмен мнениями и информацией о новых вызовах, возникающих вследствие дальнейшего технологического развития.

Необходимо избегать несовместимости с другими международными конвенциями, в частности в тех случаях, когда определенные преступления, такие как незаконный оборот оружия или незаконное распространение наркотических средств, уже широко охвачены действующими положениями международных конвенций, вследствие чего включение этих видов действий в конвенцию о киберпреступности не принесет дополнительной пользы.

В целом при разработке будущей конвенции Организации Объединенных Наций следует воздержаться от установления (минимальных) стандартов в отношении санкций или наказаний за конкретные правонарушения сверх предусмотренного в действующих моделях, например в пункте 1 статьи 11 Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

Что касается правил установления юрисдикции, то при разработке будущей конвенции Организации Объединенных Наций в качестве модели следует использовать подход, изложенный в действующих правовых инструментах, например в статье 15 Конвенции об организованной преступности.

2. Надлежащие материальные и процессуальные условия и гарантии для обеспечения совместимости с принципами соблюдения прав человека и основных свобод, включая принципы законности, необходимости и соразмерности действий правоохранительных органов, и конкретные материальные и процессуальные гарантии, обеспечивающие, в частности, право на неприкосновенность частной жизни и защиту персональных данных, право на свободу выражения мнений и информации и право на справедливое судебное разбирательство. Такие гарантии должны основываться на гарантиях, предусмотренных в других соответствующих международно-правовых документах, и находиться, как минимум, на том же уровне.

3. Процессуальные меры и уголовно-процессуальные положения, касающиеся механизмов сотрудничества между сторонами будущей конвенции Организации Объединенных Наций, включая сотрудничество в проведении расследований и других судебных разбирательств, а также в получении электронных доказательств, по мере необходимости и целесообразности, при условии, что они могут быть собраны, сохранены, аутентифицированы и

[4] В соответствии с рекомендацией 5 о криминализации, принятой Группой экспертов для проведения всестороннего исследования проблемы киберпреступности на ее совещании в Вене 6–8 апреля 2021 года (см. UNODC/CCPCJ/EG.4/2021/2, приложение, рекомендация 5).

[5] См. UNODC/CCPCJ/EG.4/2021/2, приложение, рекомендация 1 о законодательстве и правовой основе.

использованы в уголовном производстве[6]. Такие меры и положения должны соответствовать моделям, предусмотренным в других соответствующих международно-правовых документах, и основываться на них, а также быть дополнены надлежащими гарантиями, включая гарантии сотрудничества в чрезвычайных ситуациях.

4. Элементы, соответствующие принципам соблюдения прав человека и касающиеся **наращивания потенциала, обмена передовым опытом и извлеченными уроками, а также оказания технической помощи**, в том числе с учетом важной роли Управления Организации Объединенных Наций по наркотикам и преступности в этих областях.

Европейский союз и его государства-члены считают, что из сферы применения будущей конвенции Организации Объединенных Наций должно быть исключено следующее:

- вопросы, связанные с национальной безопасностью или поведением государства либо регулирующие эти аспекты;
- вопросы, связанные с регулированием интернета или касающиеся установления правил в этой области, которые уже решаются в рамках предметно-ориентированных многосторонних стратегий и форумов.

Наконец, при разработке будущей конвенции Организации Объединенных Наций, как межправительственного документа, следует воздержаться от прямого установления обязанностей для неправительственных организаций, включая организации частного сектора, такие как поставщики интернет-услуг.

III. Структура

С учетом изложенного выше будущая конвенция Организации Объединенных Наций могла бы включать следующие отдельные главы:

Преамбула (сфера применения и цели будущей конвенции Организации Объединенных Наций)

I. Виды и точные определения состава преступлений

II. Внутренние процессуальные правила и основополагающие принципы, которые должны соблюдаться в этой связи, например уважение прав человека, включая право на неприкосновенность частной жизни и защиту персональных данных, принципы необходимости и соразмерности

III. Международное сотрудничество

IV. Техническая помощь, обучение и наращивание потенциала, а также роль Управления Организации Объединенных Наций по наркотикам и преступности в этом отношении.

Индонезия

[Подлинный текст на английском языке]
[28 октября 2021 года]

Общая справочная информация и цели

Индонезия, как один из крупнейших в мире пользователей интернета, признает важность информационно-коммуникационных технологий (ИКТ) для общества. Однако успехи в области ИКТ используются для совершения безответственных действий, в частности киберпреступлений и актов кибертерроризма,

[6] Там же, рекомендация 16, касающаяся электронных доказательств и уголовного правосудия.

что подрывает использование ИКТ для политического и социально-экономического развития.

Киберпреступность, как и другие виды транснациональной преступности, затрагивает международное сообщество в силу уникального и трансграничного характера технологий и киберпространства. Поэтому международное сотрудничество играет решающую роль. Индонезия приветствует принятие резолюции 74/247 Генеральной Ассамблеи, в которой Ассамблея постановила учредить специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Индонезия считает своевременным и важным проведение предметного обсуждения конвенции о киберпреступности в рамках Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и надеется, что государства смогут воспользоваться этой возможностью, чтобы обсудить и согласовать международный документ, способный обеспечить реагирование на вызовы, связанные с киберпреступностью, на инклюзивной и прозрачной основе.

За последнее десятилетие достигнут значительный прогресс в обсуждении и разработке международных документов, направленных на определение наиболее эффективных методов предотвращения киберпреступности. Поэтому при обсуждении будущего документа по киберпреступности государствам следует учитывать все существующие платформы и рамочные механизмы, включая результаты работы межправительственной Группы экспертов для проведения всестороннего исследования проблемы киберпреступности и Конвенцию Организации Объединенных Наций против транснациональной организованной преступности.

Обсуждение конвенции о киберпреступности должно быть направлено, в первую очередь, на укрепление и развитие международного сотрудничества в поддержку национальных, региональных и международных усилий по борьбе с использованием ИКТ в преступных целях, в том числе путем предоставления технической помощи для совершенствования национального законодательства и правовых рамок государств-членов и наращивания потенциала национальных органов в целях противодействия таким преступлениям.

Кроме того, конвенция должна предусматривать надлежащие и эффективные меры, которые будут приниматься государствами на двусторонней и многосторонней основе, а также, по мере целесообразности, в сотрудничестве с соответствующими международными и региональными организациями.

Принципы

Как и в случае многих международных конвенций, наше обсуждение должно проводиться с учетом обязательств государств-членов в соответствии с принципами суверенного равенства и территориальной неприкосновенности государств, а также невмешательства во внутренние дела других государств. Кроме того, государства должны уважать суверенные права других государств при разработке политики и законодательства по борьбе с киберпреступностью в соответствии с собственными национальными условиями и потребностями.

В рамках будущего документа должно быть признано, что использование ИКТ в преступных целях влияет на безопасность и имеет социально-экономические и гуманитарные последствия. В то же время конвенция должна предусматривать, чтобы меры по борьбе с киберпреступностью были направлены на борьбу с преступным поведением и не препятствовали развитию ИКТ, включая исследования, разработки и передачу технологий.

Поощрение использования ИКТ в мирных целях отвечает всеобщим интересам и жизненно необходимо для общего блага. В рамках этих усилий центральное место по-прежнему занимает уважение суверенитета, прав человека и основных свобод, а также устойчивое и цифровое развитие.

Индонезия также считает целесообразным обеспечить установление, осуществление и применение уголовно-процессуальных норм в соответствии с внутренним законодательством каждого государства, признавая при этом необходимость решения задач, возникающих из-за различий в уголовно-процессуальных нормах государств и в обязательствах каждого государства согласно соответствующим международным документам, таким как Конвенция против транснациональной организованной преступности, международные договоры о правах человека и правах интеллектуальной собственности, а также двусторонние договоры о выдаче и взаимной правовой помощи.

Кроме того, государства-члены должны подчеркнуть необходимость обеспечения открытого и прозрачного многостороннего процесса, позволяющего всем государствам-членам добросовестно вести переговоры для выработки обоснованных, консенсусных и реалистичных решений.

Сфера применения

Сфера применения конвенции должна быть определена таким образом, чтобы учесть текущие и будущие вызовы, связанные с недобросовестным использованием ИКТ в преступных целях, обеспечить защиту пользователей ИКТ, а также смягчение и предупреждение ущерба, наносимого людям, данным, системам, услугам и инфраструктуре.

Конвенция должна быть также в состоянии обеспечить способность государств-членов принять законодательные и другие меры, которые могут потребоваться, с тем чтобы признать в качестве уголовно наказуемых деяний совершение действий, запрещенных конвенцией, в частности компьютерных преступлений и преступлений, связанных с использованием компьютеров, а также других противоправных действий.

Индонезия считает, что будущая конвенция должна охватывать весь спектр основных киберпреступлений. К ним относятся, в частности:

a) незаконное получение доступа к компьютерным системам или их взлом;

b) незаконный перехват компьютерных и системных данных;

c) мошенничество;

d) противоправное использование компьютерных данных и систем в преступных целях;

e) нарушение авторских и смежных прав;

f) манипулирование компьютерными данными и системами;

g) распространение и передача незаконного контента и материалов, например порнографии, детской порнографии, дезинформации, заговорческой информации, мистификаций и материалов, которые вызывают враждебность на расовой, национальной, религиозной или политической почве.

Государствам-членам следует рассмотреть вопрос о принятии мер, необходимых для осуществления уголовного судопроизводства, предусмотренного конвенцией, включая следующие меры, но не ограничиваясь ими:

a) обеспечение сохранности данных и систем и сохранности данных о трафике, хранящихся у одного или нескольких поставщиков услуг, при том понимании, что сроки хранения данных и классификация хранящихся на собственной территории данных регулируются национальным и внутренним законодательством;

b) предоставление или передача сохраненных компьютерных данных физическими или юридическими лицами, а также принятие адекватных мер к тому, чтобы обязать поставщиков онлайновых системных услуг предоставлять или передавать сохраненные компьютерные данные, включая данные, касающиеся типа оказанных услуг;

c) поиск и изъятие данных и компьютерных систем, создание и обеспечение сохранности копий компьютерных данных, а также изменение и передача сохраненных данных;

d) сбор и запись данных о трафике в режиме реального времени, а также получение данных о трафике от поставщиков онлайновых услуг и/или систем.

С учетом изложенного выше государствам-членам следует обеспечивать проведение расследований киберпреступлений в соответствии с принципами защиты неприкосновенности частной жизни, конфиденциальности, устойчивости государственных услуг, поддержания непрерывности оказания государственных услуг и соблюдения общественных интересов, а также интеграции данных.

Сотрудничество

Расследование киберпреступлений и преступлений, совершаемых с помощью ИКТ, должно проводиться эффективно на национальном и транснациональном уровнях. Поэтому разрабатываемый документ должен стать эффективным механизмом международного сотрудничества в борьбе с использованием ИКТ в преступных целях. Такое сотрудничество должно осуществляться на основе взаимной выгоды и принципа взаимности в соответствии с национальным законодательством и с учетом существующих инструментов и действующих механизмов и рамок.

Учитывая важность многосторонних подходов к предупреждению, выявлению и искоренению киберпреступности, обсуждение также должно быть нацелено на развитие тесного сотрудничества субъектов, имеющих дело с киберпреступностью, включая сотрудничество между правоохранительными органами и поставщиками услуг ИКТ. В этом контексте сотрудничество между частными предприятиями с опорой, в соответствующих случаях, на публично-частные партнерства имеет решающее значение для повышения уровня знаний и более эффективного противодействия киберпреступности. Государствам-членам следует также прилагать усилия в целях повышения осведомленности о киберпреступности в публичном и частном секторах.

В рамках наших обсуждений следует также обратить внимание на меры, позволяющие органам власти проводить расследования, в ходе которых производится сбор и конфискация данных через механизмы взаимной правовой помощи, при этом государства-члены, возможно, пожелают рассмотреть возможность использования своих существующих правовых основ в этой связи.

Что касается взаимной правовой помощи, то в ходе обсуждений следует в максимально возможной степени учитывать соответствующие законы, договоры и соглашения, касающиеся расследований, уголовного преследования и судопроизводства. Государствам-членам рекомендуется, в частности, обсудить договоренности об ускорении сбора электронных доказательств или механизмы обмена информацией между компетентными органами.

Положения о международном сотрудничестве в этой конвенции должны обеспечить необходимую правовую основу для решения процессуальных проблем, устранения пробелов и совершенствования неадекватных механизмов международного сотрудничества, особенно в отношении расследований, обмена информацией, сбора данных и электронных доказательств и судебного преследования, а также содействия выдаче. Государствам-членам также рекомендуется назначить координаторов или органы для ускорения выполнения положений конвенции о международном сотрудничестве.

Кроме того, государства-члены, возможно, пожелают рассмотреть вопрос об укреплении своего национального потенциала в области выявления, расследования и реагирования на использование ИКТ в преступных целях посредством принятия мер по наращиванию потенциала и оказанию технической помощи, которые способствуют повышению устойчивости государств-членов. Эти меры по наращиванию потенциала должны основываться на взаимном доверии, быть обусловлены спросом, который соответствует выявленным на национальном уровне потребностям, и осуществляться при полном признании принципа национальной ответственности.

Поскольку сотрудничество в области предупреждения и искоренения киберпреступности остается приоритетом в наших обсуждениях, будущий документ должен, как минимум, включать перечень мероприятий по повышению эффективности сотрудничества посредством следующих мер:

a) обмен информацией об угрозах киберпреступности;

b) содействие укреплению сотрудничества и координации между правоохранительными органами, прокуратурой и судебными органами;

c) обмен передовой практикой и опытом в отношении трансграничных расследований киберпреступлений;

d) взаимодействие с поставщиками услуг в рамках публично-частных партнерств с целью установления форм сотрудничества в правоохранительной сфере, расследовании киберпреступлений и сборе доказательств;

e) разработка руководящих принципов для поставщиков услуг с целью содействия правоохранительным органам в расследовании киберпреступлений, в том числе в отношении формата и сроков обеспечения сохранности электронных доказательств и информации;

f) подготовка квалифицированных кадров и развитие людских ресурсов в рамках политики, позволяющей государствам-членам повысить адаптивность к цифровым технологиям;

g) укрепление технического и правового потенциала правоохранительных и судебных органов и прокуратуры с помощью программ по наращиванию потенциала и повышению квалификации.

С помощью этого механизма государствам-членам следует также продолжать повышать эффективность внутренней межведомственной координации и взаимодействия, включая обмен информацией и сотрудничество с региональными организациями, частным сектором, центрами реагирования на компьютерные инциденты и инциденты информационной безопасности, организациями гражданского общества и другими заинтересованными сторонами в целях содействия эффективному международному сотрудничеству.

Обсуждение должно также охватывать вопросы, связанные с механизмом обзора применения или выполнения всех обязательств и обязанностей по будущему документу.

Ямайка

[Подлинный текст на английском языке]
[29 октября 2021 года]

Ниже приводится мнение Ямайки относительно сферы применения, целей и структуры международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, представленное по просьбе секретариата Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Ямайка надеется на сотрудничество с другими государствами-членами в целях содействия разработке проекта конвенции о киберпреступности. Ямайка ожидает заключения конвенции, которая станет для мирового сообщества средством защиты граждан от киберугроз и других преступлений и которая будет принята и ратифицирована всеми. Ямайка приветствует привлечение экспертов гражданского общества в этой области с целью информационного обеспечения наших обсуждений.

Ямайка считает процесс разработки конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях важным шагом в рамках глобальных мер реагирования на проблемы, с которыми сталкиваются государства в связи с этой угрозой. Цель этой конвенции была четко сформулирована в выпущенном в 2015 году консенсусном докладе Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, где в подпункте (d) пункта 13 было предусмотрено, что государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам[7].

Главной целью конвенции должно стать сотрудничество в целях обмена информацией для содействия борьбе государств с использованием ИКТ в преступных целях и уголовному преследованию виновных. Для этого необходимо, чтобы государства стали лучше понимать различные точки зрения на киберпреступность. Можно надеяться, что это приведет к гармонизации подходов и созданию международной рамочной основы, которая будет работать во всеобщих интересах. Однако успех в достижении этой цели зависит от того, чтобы позиции всех государств, включая малые островные развивающиеся страны, были учтены в рамках сбалансированного, справедливого, прозрачного и инклюзивного процесса.

Необходимо принять во внимание и другие процессы, которые могут способствовать прогрессу в подготовке конвенции, не вызывая при этом неоправданных задержек. Следует уложиться в согласованные сроки проведения переговоров и завершения работы над проектом конвенции, что будет свидетельствовать о нашем серьезном отношении к борьбе с киберпреступностью.

Очевидно, что отправной точкой переговоров является определение терминов. Термины определяют сферу применения конвенции и важны для достижения общих целей участников. Поэтому определения должны быть четкими, ясными и тщательно сформулированными; они не должны быть неоправданно ограничительными или широкими, а должны соответствовать контексту и целям конвенции.

Противодействие использованию ИКТ в преступных целях — это широкая задача. Поэтому составы преступлений должны быть определены с перспективой на будущее. Они должны быть сформулированы таким образом, чтобы не ограничиваться существующими технологиями, а, напротив, допускать достаточную интерпретацию, чтобы обеспечить охват будущих технологий и постоянно развивающейся среды ИКТ.

В конвенцию должны быть включены такие составы преступлений, чтобы обеспечить укрепление инструментария, доступного странам для борьбы с киберпреступностью, и чтобы не нарушать основополагающие права и свободы человека, но способствовать соблюдению и уважению этих прав. Соответственно, необходимо учесть международные договоры в области прав человека.

В вопросах уголовного производства, правоприменения и международного сотрудничества необходимо, чтобы положения новой конвенции должным

[7] A/70/174.

образом учитывали принцип государственного суверенитета и другие принципы, изложенные в Уставе Организации Объединенных Наций и международно-правовых документах.

Ямайка считает, что в конвенции необходимо уделить должное внимание международному сотрудничеству, поскольку это будет способствовать более активному взаимодействию в глобальной борьбе с киберпреступностью. В случаях, когда между государствами не существует договора о взаимной правовой помощи, конвенция должна служить руководством для направления соответствующих просьб и ответа на них. Должны быть охвачены такие вопросы, как ответственность за покрытие издержек.

При разработке конвенции необходимо учитывать различия в возможностях государств, которые, в свою очередь, влияют на их способность сотрудничать настолько широко, насколько это необходимо для достижения оптимальных результатов. Поэтому чрезвычайно важно предоставлять техническую помощь для наращивания потенциала государств, чтобы они могли вносить больший вклад в глобальную систему борьбы с киберпреступностью. В этой связи наращивание потенциала должно быть устойчивым, иметь четкую цель, соответствовать внутренним потребностям и отвечать задаче развития людских ресурсов в этой особой области. Следует также рассмотреть вопрос о создании механизма финансирования для содействия наращиванию потенциала в целях осуществления конвенции о киберпреступности.

Япония

[Подлинный текст на английском языке]
[29 октября 2021 года]

Япония, как государство, которое придает большое значение разработке будущей конвенции Организации Объединенных Наций по киберпреступности на основе инклюзивного, прозрачного и справедливого процесса, с удовлетворением представляет свои предложения по новой конвенции до начала ее официальной разработки и высоко оценивает инициативу Председателя предоставить эту возможность.

Хотя разные государства сталкиваются с разными проблемами, связанными с киберпреступностью, Япония считает киберпреступность постоянно меняющейся серьезной угрозой, общей для всех государств-членов. Поскольку киберпреступность легко преодолевает национальные границы, для борьбы с ней крайне важно обеспечить сотрудничество между всеми государствами-членами. Поэтому Япония считает, что следует стремиться к обеспечению свободного, справедливого и безопасного киберпространства и укреплению наших возможностей по предупреждению киберпреступности и борьбе с ней во всем мире, а для этого необходимо сделать содержание новой международной конвенции универсальным и приемлемым для всех государств-членов.

Ниже изложена точка зрения Японии относительно сферы применения, целей и структуры новой конвенции, с тем чтобы способствовать обсуждению в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, который был учрежден в соответствии с резолюцией 74/247 Генеральной Ассамблеи.

Сфера применения

В целях укрепления глобальных мер по борьбе с киберпреступностью и создания универсальных международно-правовых рамок международному сообществу следует, прежде всего, заложить прочную основу, сосредоточив внимание на базовых и ключевых положениях об уголовных преступлениях и

уголовном производстве, а также на вопросах взаимной правовой помощи и другого международного сотрудничества в этой области.

Деяния, криминализация которых будет предусмотрена новой конвенцией, должны быть ограничены сферой киберпреступности; преступления, признанные таковыми в новой конвенции, должны в основном включать киберзависимые преступления, а преступления, совершаемые с помощью кибертехнологий, должны быть охвачены только при необходимости и при наличии широкого консенсуса среди государств-членов.

В основе новой конвенции должны лежать результаты предыдущих и проводимых обсуждений в рамках существующих структур для борьбы с киберпреступностью, при этом следует учитывать обсуждения и работу в рамках других форумов, где обсуждаются вопросы киберпреступности, с тем чтобы избежать дублирования работы или негативного воздействия на нее.

Для того чтобы создать универсальную международно-правовую основу, которая будет в целом применима к любому виду использования информационно-коммуникационных технологий, независимо от различий между государствами, и учесть будущее развитие технологий, при разработке новой конвенции следует использовать технически нейтральные формулировки.

Борьба с киберпреступностью важна, однако меры противодействия киберпреступности не должны нарушать принцип надлежащей правовой процедуры или налагать неоправданные ограничения на права человека. Такие гарантии являются предпосылкой для успешного международного сотрудничества, и поэтому новая конвенция должна включать конкретные положения по обеспечению надлежащей правовой процедуры и соблюдению прав человека.

Цель

Основной целью новой конвенции должно стать содействие обеспечению безопасности и защите интересов всех, кто связан с информационно-коммуникационными технологиями, которые требуют защиты. Для этого необходимо на глобальном уровне активизировать принятие мер по борьбе с киберпреступностью посредством создания универсальной международно-правовой основы с наиболее широким охватом киберпреступности в ее различных транснациональных формах и содействия эффективному двустороннему или многостороннему сотрудничеству в области уголовных расследований и уголовного преследования.

Для достижения этой цели в новой конвенции следует предусмотреть базовые и ключевые положения, которые могут быть соблюдены и реализованы как можно большим числом государств-членов, что позволит повысить общий уровень принимаемых в мире мер по противодействию киберпреступности и укрепить существующие правовые рамки.

Структура

По мнению Японии, в новую конвенцию следует включить следующие базовые элементы, хотя в ходе предстоящих переговоров Япония готова придерживаться гибкого подхода в отношении более детальной структуры:

a) определение терминов;

b) перечень национальных мер, которые должны принять государства-члены:

i) криминализация:

a. правонарушения, относящиеся к категории киберзависимых преступлений;

b. правонарушения, которые должны быть криминализированы в качестве преступлений, совершаемых с помощью кибертехнологий;

ii) процедурные положения, касающиеся обеспечения сохранности, раскрытия и предоставления данных;

iii) гарантии обеспечения прав человека и других интересов;

c) международное сотрудничество в области выдачи, взаимной помощи и другие формы сотрудничества;

d) заключительные положения.

Иордания

[Подлинный текст на арабском языке]
[28 октября 2021 года]

Сфера применения

Конвенция должна охватывать преступления, связанные с:

- конфиденциальностью, надежностью и доступностью электронных услуг;
- несанкционированным доступом к информационной сети, информационной системе или любой их части;
- нарушением функционирования критически важной инфраструктуры;
- намерением вывести из строя информационные сети или информационные системы;
- слежением за потоком данных в информационной сети или информационной системе;
- мошенничеством, фальсификацией и маскировкой под законного пользователя;
- перехватом данных или информации финансовых систем;
- нарушением неприкосновенности частной жизни и прав интеллектуальной собственности;
- аппаратными средствами, дешифрующим программным обеспечением и кодами доступа;
- мошенничеством с интернет-адресами;
- порнографией;
- эксплуатацией детей и жестоким обращением с ними;
- распространением ложных новостей;
- расовой дискриминацией;
- эксплуатацией женщин и жестоким обращением с ними;
- призывами к мятежу, подстрекательством или распространением ненавистнической риторики;
- незаконной торговлей через информационные сети или веб-сайты;
- распространением, поддержкой или пропагандой террористической идеологии;
- использованием ИКТ для террористических целей;
- оскорблением религий, стран и символов;
- производственно-сбытовыми цепочками;
- программами-вымогателями;

- электронным фишингом;
- нарушением авторских прав на программное обеспечение;
- несанкционированным использованием данных поставщиками услуг.

Цели

Конвенция должна иметь следующие цели:

- укрепление международного сотрудничества и взаимодействия для противодействия использованию ИКТ в преступных целях;
- разработка норм международного права для противодействия использованию ИКТ в преступных целях;
- акцентирование необходимости защиты критически важной инфраструктуры посредством противодействия использованию ИКТ в преступных целях;
- пропаганда необходимости создания и развития национального и международного потенциала и повышение уровня осведомленности населения о противодействии использованию ИКТ в преступных целях.

Структура

- Введение.
- Определения.
- Цели.
- Сфера применения.
- Обязанности и ответственность.
- Международное сотрудничество.
- Наращивание потенциала и информирование.
- Механизм осуществления.
- Непрерывное обновление конвенции с учетом новых обстоятельств.

Конвенция должна иметь широкую сферу применения и насчитывать максимально возможное количество стран-участниц, прежде всего стран, занимающих ведущие позиции в разработке новых технологий.

В ней должны использоваться согласованные на международном уровне понятия, связанные с преступлениями в сфере информационных технологий, совершаемыми против людей или с целью хищения денежных средств.

Основное внимание следует уделить созданию для правоохранительных органов государств-участников возможностей для обмена информацией друг с другом, а также внедрению механизмов отслеживания средств, полученных в результате электронного мошенничества, и цифровой идентификации лиц, совершающих подобные преступления, в соответствии с внутренним законодательством государств и с уважением права на неприкосновенность частной жизни.

В государствах-участниках необходимо назначить постоянных контактных лиц для незамедлительного реагирования на такие преступления, как терроризм, сексуальная эксплуатация детей и другие преступления. Следует также создать механизмы для содействия развитию сотрудничества с международными компаниями — операторами социальных сетей с целью получения необходимой технической информации для противодействия преступлениям этого типа.

Необходимо развивать международное сотрудничество для повышения квалификации сотрудников подразделений по борьбе с киберпреступностью в

государствах-участниках, в рамках которого проводить учебные курсы, практикумы и мероприятия по обмену опытом.

Кувейт

[Подлинный текст на арабском языке]
[17 сентября 2021 года]

1. При изложении текста проекта конвенции необходимо делать акцент на том, что конвенция предназначена для расширения и укрепления сотрудничества, направленного на противодействие преступлениям в сфере информационных технологий и снижение связанных с ними рисков и опирающегося на принципы суверенного равенства государств и невмешательства в их внутренние дела, включая процедуры, связанные с осуществлением юрисдикции, уважением верховенства права, поддержанием общественного порядка и безопасности и уважением общественных ценностей.

2. Сфера применения конвенции должна охватывать преступления, совершаемые более чем в одной стране; преступления, которые готовятся и планируются в других странах и руководство и контроль над которыми осуществляются из других стран; преступления, совершаемые в других странах; преступления, совершаемые в одной стране, но вызывающие серьезные последствия в другой стране; при этом следует принимать во внимание международно-правовые документы по предотвращению террористических актов и Конвенцию Организации Объединенных Наций против транснациональной организованной преступности и протоколы к ней.

3. Определять, за какие деяния конвенция должна устанавливать уголовную ответственность, необходимо с учетом недавно зародившихся форм преступности в сфере ИКТ, которые фигурируют в качестве основных правонарушений во внутреннем законодательстве государств-участников; особое внимание следует уделять преступлениям, связанным с контентом, ненавистнической риторикой и насилием.

4. Необходимо сформулировать общие принципы для правового и судебного сотрудничества; выдачи преступников; обмена информацией; допустимости предоставления информации без предварительной просьбы в тех случаях, когда государство-участник полагает, что раскрытие такой информации способно помочь начать расследование преступления; сотрудничества в вопросах срочного раскрытия и обеспечения сохранности информации, хранимой с помощью информационных технологий; доступа к трансграничным информационным технологиям; двустороннего сотрудничества и помощи в сборе технических параметров трафика в режиме реального времени; положений о конфиденциальности; ограничений на использование данных, являющихся предметом взаимной помощи.

5. Кроме того, следует установить общие принципы оценки осуществления конвенции в соответствии с механизмами, применяемыми государствами-участниками. Следует назначить соответствующие учреждения и контактных лиц в государствах-участниках и использовать преимущества уже существующих информационных сетей Управления Организации Объединенных Наций по наркотикам и преступности.

Лихтенштейн

[Подлинный текст на английском языке]
[28 октября 2021 года]

Лихтенштейн благодарит секретариат Специального комитета по разработке всеобъемлющей международной конвенции о противодействии

использованию информационно-коммуникационных технологий в преступных целях и его председателя Е. П. г-жу Фаузию Бумайзу за стремление ознакомиться с мнениями государств-членов относительно сферы применения, целей и структуры (элементов) новой конвенции. Общая позиция Лихтенштейна заключается в следующем.

Для Лихтенштейна одной из главных целей является обеспечить согласование новой конвенции о киберпреступности с действующими международными и региональными правовыми документами, включая Конвенцию Организации Объединенных Наций против транснациональной организованной преступности и Конвенцию Совета Европы о киберпреступности, и использование в качестве основы новой конвенции норм международного права, в том числе в области прав человека.

В этой связи Лихтенштейн рассчитывает на разработку краткой функциональной конвенции, охватывающей такие характерные для киберпространства преступления, как противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий и преступления, связанные с нарушением авторского права и детской порнографией. Широкое введение уголовной ответственности за совершение преступлений других типов, не относящихся непосредственно к преступлениям в киберпространстве, должно быть предметом других конвенций и форумов и поэтому не заслуживает рассмотрения. Кроме того, Лихтенштейн выступает против дублирования мер в отношении преступлений, уже охваченных другими отдельными договорами.

Ввиду быстрого изменения обстановки в киберпространстве Лихтенштейн предпочитает, чтобы в конвенции использовались технически нейтральные формулировки — это позволит применять составы преступлений как к текущим, так и к будущим технологиям, имеющим отношение к данной проблематике. Пространные технические определения конкретных типов киберпреступлений с большой долей вероятности утратят свою актуальность в будущем, поэтому в конвенции их следует избегать.

Принципиальное значение для Лихтенштейна имеют также положения о защите данных и права человека, которые должны занимать видное место в конвенции. Крайне важно в полной мере обеспечить защиту данных и соблюдение норм о правах человека.

Более подробно Лихтенштейн представит свою позицию на переговорах по новой конвенции о киберпреступности.

Мексика

[Подлинный текст на испанском языке]
[21 октября 2021 года]

Для правительства Мексики информационно-коммуникационные технологии, цифровые платформы и киберпространство открывают широкие возможности для активизации развития, преодоления неравенства и поддержки единения общества, обеспечения благосостояния, справедливости и соблюдения прав.

Вместе с тем Мексика признает, что использование этих технологий для совершения преступлений и расширения нелегального рынка все более тревожит правительства, коммерческие организации, организации гражданского общества и население в целом.

Поэтому сейчас, как никогда, необходимы международное сотрудничество и механизмы оказания правовой помощи и обмена информацией. Мексика решительно поддерживает многосторонний подход и в особенности роль

Организации Объединенных Наций в выработке всеобъемлющих и эффективных мер противодействия этой глобальной угрозе.

Мексика считает, что поручение Генеральной Ассамблеи о разработке всеобъемлющей конвенции о противодействии использованию информационных технологий в преступных целях — превосходная возможность наладить предметный, ответственный, многосторонний, инклюзивный и прозрачный рабочий процесс с учетом опыта, накопленного в ходе другой работы в рамках Организации Объединенных Наций, связанной с данной проблематикой, и другого опыта региональной деятельности в этой области.

Правительство Мексики рассчитывает, что участники процесса проработки и определения содержания будущей конвенции будут руководствоваться нижеследующими соображениями.

Подход, сфера применения и тип конвенции

Конвенция должна представлять собой всеобъемлющий юридически обязательный правовой документ, который будет охватывать вопросы существа и процессуальные вопросы и служить основой для международного сотрудничества и обмена информацией, опытом, специальными знаниями и примерами передовой практики.

Ожидается, что конвенция поможет расширить применение стандартов, способствующих совершенствованию расследований, минимизации последствий и преследования, и что конвенция будет служить своего рода образцом согласованного рамочного документа, который позволяет повысить эффективность преследования за совершение киберпреступлений и при этом не препятствует заключению других международных договоров по этой же проблематике.

Она должна включать следующие элементы:

- общие определения, базовую типологию и описание компетентных органов;
- основные процессуальные меры, которые должны применяться в государствах для надлежащего расследования киберпреступлений и преследования за их совершение;
- описание основных преступлений, которые следует принимать во внимание национальным законодательным органам;
- механизмы доступа к информации и содействия эффективному сотрудничеству.

Кроме того, будущая конвенция должна содержать положения о формулировании оговорок и заявлений о толковании, а также предусматривать гибкую процедуру внесения поправок, облегчающую ее обновление, и механизмы урегулирования споров. Желательно, чтобы конвенция вступала в силу после того, как будут сданы на хранение 50 документов о ратификации.

После определения содержания конвенции целесообразно согласовать эффективный, универсальный и не обременительный для государств механизм обзора хода ее осуществления, основанный на проведении обзора самими участниками.

Актуальность других международно-правовых документов

Для правительства Мексики важно, чтобы основополагающим для конвенция являлся постулат о том, что к киберпространству применимы нормы международного права, и поэтому необходимо принимать во внимание такие действующие международно-правовые документы, как:

- Конвенция Организации Объединенных Наций против транснациональной организованной преступности и три протокола к ней;

- Статут Международного суда;
- Конвенция Совета Европы о киберпреступности;
- договоры о защите и трансграничном перемещении личных данных;
- международные договоры о правах человека и договоры, гарантирующие права участников судебного процесса;
- договоры, применимые к интеллектуальной собственности;
- двусторонние договоры о выдаче, взаимной правовой помощи в уголовно-правовых вопросах и других формах международного правового сотрудничества.

Помимо этого, в процессе переговоров целесообразно руководствоваться документами, принятыми в системе Организации Объединенных Наций и на других соответствующих международных форумах, главным образом следующими из них:

- «Компиляция всех предварительных выводов и рекомендаций, предложенных государствами-членами в ходе совещаний Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенных в 2018, 2019 и 2020 годах»;
- заключительный доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве за 2019–2021 годы и предыдущие доклады за 2013 и 2015 годы;
- заключительный доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности;
- проект руководящих принципов использования Глобальной программы кибербезопасности, разработанной Международным союзом электросвязи;
- резолюции Генеральной Ассамблеи о праве на неприкосновенность частной жизни в цифровую эпоху;
- резолюции Совета по правам человека о поощрении, защите и осуществлении прав человека в интернете.

Киберпреступления/преступное поведение, которые необходимо охватить конвенцией

Правительство Мексики считает, что в конвенции должны фигурировать деяния, признаваемые незаконными в международном праве (в соответствии с терминологией других договоров, принятых в рамках системы Организации Объединенных Наций) и совершаемые электронными средствами.

Хотя не следует ожидать, что конвенция будет содержать исчерпывающий перечень преступлений или что используемая типология будет совместима с различными правовыми системами, желательно, чтобы процесс разработки проекта предусматривал диалог для рассмотрения следующих понятий:

- кража и фишинг;
- мошенничество и вымогательство;
- использование программ-вымогателей;
- вредоносное программное обеспечение и преступное поведение, связанное с изготовлением, хранением, распространением, продажей и выполнением вредоносного кода;
- раскрытие личной или корпоративной информации в ущерб ее владельцам;
- преступления, связанные с торговлей людьми, детской порнографией и нарушением права на конфиденциальность сексуальной жизни;

- груминг и кибербуллинг;
- цифровое насилие, включая насилие по признаку пола и насилие на основе ненависти, расы, национальности, религии или политической вражды;
- методы атаки (фишинг, вишинг, смишинг, фарминг);
- преступления против национального суверенитета, например, терроризм, диверсия, шпионаж и проникновение в системы, содержащие информацию, которая отнесена к секретной по соображениям национальной безопасности;
- преступные действия, направленные против критической информационной инфраструктуры и конфиденциальности, целостности и доступности информации;
- преступления в отношении детей и подростков;
- нарушение свободы выражения мнений;
- преступления против интеллектуальной собственности;
- преступления против финансовой системы;
- противозаконная продажа оружия, животных, контролируемых лекарственных средств и лекарственных препаратов, которые не являются зарегистрированной медицинской продукцией;
- изготовление фальшивых денег и фальсификация официальных документов;
- использование криптовалют и активов двойного назначения в преступных целях;
- незаконное модифицирование веб-сайтов (искажение внешнего вида);
- ответственность юридических лиц.

Кроме того, при подготовке проекта конвенции целесообразно обсудить возможность установления наказаний за попытки совершения преступлений и возможность определения отягчающих обстоятельств, повышающих строгость наказания.

Аспекты, связанные с суверенитетом и юрисдикцией

- Подтверждение уважения национального суверенитета и принципа невмешательства во внутренние дела других государств.
- Установление общих правил определения юрисдикции с использованием в качестве основы схожих положений в других правовых документах и процессах.
- Формулирование общих мер, применяемых для получения технических параметров трафика и содержания информации и в то же время исключающих незаконное блокирование или перехват данных.
- Разработка механизмов, обеспечивающих определенность в отношении получения, удержания, сохранения и представления цифровых доказательств.
- Разъяснение таких стадий следствия, как вызов в суд или арест.
- Разработка положений, регламентирующих представление технических данных и содержания информации в уголовных расследованиях и оперативное раскрытие компьютерных данных.
- Рассмотрение вопроса о введении для операторов технологий, поставщиков услуг и поставщиков интернет-контента правового обязательства независимо от их физического местоположения предоставлять информацию компетентным органам в ходе расследований.

Аспекты, связанные с обменом информацией и международным сотрудничеством

Правительство Мексики считает, что одна из основных целей конвенции должна заключаться в обеспечении определенности в отношении обмена информацией и международного сотрудничества и установлении процедур для их эффективного осуществления. Ожидается, что помимо прочего будут рассмотрены следующие аспекты:

- взаимная правовая помощь;
- выдача;
- общие механизмы запроса информации для целей расследований и оперативно-розыскной деятельности, реагирования на запросы, получения такой информации и обмена ею;
- процедуры судебного надзора, обеспечивающие оперативное и эффективное сотрудничество в ходе расследований;
- сотрудничество в проведении полицейских расследований и получении свидетельских показаний для их использования в судебном процессе с рассмотрением возможности использования информационно-коммуникационных технологий;
- разработка рекомендаций, стандартов, методологий и передовой практики для предупреждения и расследования киберпреступлений;
- налаживание сотрудничества между национальными группами реагирования на компьютерные инциденты или группами реагирования на инциденты в сфере компьютерной безопасности с целью предупреждения киберпреступности;
- координация расследований;
- подготовка рекомендации относительно минимальных общих принципов обеспечения прозрачности и защиты информации, с тем чтобы независимо от различий в национальной политике государств имелась возможность передачи данных расследований и судебных разбирательств;
- установление минимального периода времени для хранения данных и сохранения цифровых доказательств;
- подготовка рекомендаций относительно правил и условий перехвата частных сообщений и геолокации в режиме реального времени;
- установление общих критериев соблюдения и регулирования политики конфиденциальности;
- содействие согласованию местных, региональных и глобальных статистических данных.

Аспекты, связанные с защитой и осуществлением прав человека

Все меры, которые будут применяться в соответствии с будущей конвенцией, должны согласовываться с обязательствами, закрепленными в международно-правовых документах о правах человека. Ожидается, что ее положения также будут соответствовать нормам, относящимся к свободе выражения мнений.

Правительство Мексики рассчитывает, что при разработке конвенции будут рассмотрены следующие аспекты:

- концепции и нововведения, касающиеся предпринимательской деятельности и прав человека;

- акцент на расследованиях, преследовании и наказании за гендерное насилие и преступления в отношении детей и подростков, совершаемые с помощью интернета;
- поощрение расследований, преследования и наказания за расистское поведение, подстрекающее к насилию или преследующее цель вызвать изоляцию или сегрегацию;
- минимальные общие элементы нейтральности сети;
- рекомендация относительно механизмов защиты информации компаниями — поставщиками интернет-услуг.

Элементы, касающиеся наращивания потенциала и оказания технической помощи

Правительство Мексики считает, что для эффективного осуществления будущей конвенции необходимо включить в нее положения, стимулирующие наращивание потенциала в области предупреждения киберпреступлений и преследования за их совершение. В этой связи желательно:

- стимулировать деятельность, связанную с обучением, оказанием технической помощи и применением передовой практики, а также стандартизацией порядка проведения компьютерно-технической экспертизы и получения достоверных цифровых доказательств;
- поощрять реализацию образовательных инициатив, ориентированных на предупреждение киберпреступности, и проведение тиражируемых информационных кампаний;
- стимулировать также создание или укрепление групп реагирования на компьютерные инциденты в различных секторах, например в финансовой сфере, образовании, торговле и энергетике;
- разрабатывать руководства, руководящие принципы и рекомендации, способствующие внедрению передовой практики;
- расширять диапазон учебных мероприятий, ориентированных на различных участников: следователей, прокуроров, судей, дипломатов, работников законодательных органов и представителей негосударственных субъектов.

Аспекты, связанные с участием соответствующих негосударственных субъектов (гражданское общество, частный сектор, научная общественность)

Правительство Мексики считает целесообразным в процессе работы над проектом рассмотреть возможные механизмы обеспечения участия в осуществлении конвенции организаций гражданского общества, частного сектора, поставщиков услуг, научной общественности и исследовательских центров, а также получения от них необходимых материалов. Желательно рассмотреть следующие вопросы:

- возможность вовлечения этих субъектов в деятельность, направленную на предупреждение и противодействие киберпреступности;
- содействие формированию условий, благоприятствующих сотрудничеству с частными группами реагирования на компьютерные инциденты, поставщиками коммуникационных услуг и различными телекоммуникационными компаниями;
- диалог с частными предприятиями, эксплуатирующими критическую информационную инфраструктуру или работающими в стратегических секторах, и с компаниями, предоставляющими такие бесплатные интернет-услуги, как электронная почта, мгновенная передача сообщений, микроблоги и онлайновые транспортные услуги;

- поддержка саморегулирования, информирование общественности о концепции предпринимательской деятельности и прав человека и пропаганда этой концепции.

Новая Зеландия

[Подлинный текст на английском языке]
[29 октября 2021 года]

Новая Зеландия с удовлетворением откликается на предложение Председателя Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях представить свои мнения относительно сферы применения, целей и структуры новой конвенции, которое было направлено государствам-членам во исполнение резолюций 74/247 и 75/282 Генеральной Ассамблеи. Новая Зеландия приветствует возможность поделиться своим мнением, рассчитывает на вклад других государств и с нетерпением ждет обсуждения дальнейших действий по совместной подготовке новой конвенции на основе транспарентного, инклюзивного подхода.

Проблема киберпреступности носит трансграничный характер. Следовательно, эффективно противодействовать этой растущей угрозе международное сообщество может лишь в рамках глобального сотрудничества на основе инклюзивного и многостороннего подхода. Международное сотрудничество по вопросам, касающимся киберпреступности, требует согласующихся между собой, действенных законов о киберпреступности, которые позволяют вести трансграничное расследование киберпреступлений и осуществлять судебное преследование за их совершение. Как никогда важно оказывать содействие этому сотрудничеству. С перемещением работы, исследовательской деятельности и социального взаимодействия в интернет, в том числе в ходе пандемии коронавирусного заболевания (COVID-19), поле деятельности киберпреступников расширилось, а киберпреступления происходят чаще и становятся все опаснее.

Международное сотрудничество в области борьбы с киберпреступностью особенно важно для малых островных развивающихся государств, и необходимо, чтобы эти страны могли принимать конструктивное участие в работе Специального комитета. Новая Зеландия прилагает все усилия к тому, чтобы тихоокеанские островные страны имели возможность конструктивно участвовать в работе Специального комитета. Мы поддерживаем смешанное (очное и в режиме онлайн) участие в сессиях Специального комитета и подчеркиваем важность предоставления времени для надлежащей подготовки и обеспечения участия небольших делегаций.

Сфера применения

Новая конвенция по киберпреступности должна дополнять существующие документы, а не противоречить им. Все государства-члены согласились с тем, что международное право применимо к киберпространству, а это значит, что новая конвенция будет существовать не в вакууме. Наиболее эффективной она будет в том случае, если дополнит и укрепит существующие документы и действующий правовой режим, включающий такие инструменты борьбы с киберпреступностью, как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Совета Европы о киберпреступности. Это соответствует мандату, предусмотренному резолюцией 74/247 Генеральной Ассамблеи, в которой Ассамблея призвала к тому, чтобы в рамках работы Специального комитета в полной мере учитывались существующие международные документы и предпринимаемые на национальном, региональном и международном уровнях усилия.

Для Новой Зеландии важно, чтобы любой разрабатываемый документ защищал права человека и обеспечивал свободное и открытое киберпространство, которое управляется множеством субъектов. Поэтому конвенция о киберпреступности должна согласовываться с обязательствами государств по защите и соблюдению в киберпространстве прав человека, в том числе права на свободу выражения мнений и права не подвергаться произвольному и незаконному вмешательству в частную жизнь. Меры борьбы с киберпреступностью должны согласовываться с международным правом прав человека.

Чтобы действительно укрепить сотрудничество в борьбе с угрозой, которую киберпреступность представляет для частных лиц, промышленности и правительств, нужно, чтобы этот договор был четко сфокусирован на основных вопросах киберпреступности. Мы считаем, что в договоре следует охватить киберзависимые преступления, а также преступления, совершаемые с помощью кибертехнологий, но только те, в которых сфера охвата, скорость совершения и масштаб преступления увеличиваются за счет использования информационно-коммуникационных технологий. Мы считаем, что есть два явных кандидата на вхождение в эту категорию преступлений: сексуальная эксплуатация детей и сексуальные надругательства над ними в интернете, а также мошенничество и кражи с использованием кибертехнологий, в том числе вирусов-вымогателей.

По мнению Новой Зеландии, нет необходимости в точности повторять такие составы преступлений, как коррупция, торговля людьми или терроризм, которые охватываются другими правовыми инструментами, только потому, что они могут совершаться с использованием информационно-коммуникационных технологий. Такой подход чреват возникновением противоречий и путаницы и не позволит подготовить конкретно ориентированный, практически применимый документ, способный укрепить нашу коллективную способность бороться с киберпреступностью.

В поручении, касающемся этого процесса, четко указано, что нам следует сосредоточиться на разработке инструмента уголовного правосудия для повышения эффективности международной борьбы с киберпреступностью посредством принятия соответствующих мер национальными правоохранительными органами. Для этого нужно дать определение преступного поведения в киберпространстве и определить соответствующие санкции, а государствам необходимо внедрить надлежащие процессы и законодательные инструменты, позволяющие ведомствам получать доступ к цифровым доказательствам и обмениваться ими для эффективного пресечения преступной деятельности в киберпространстве и наказании за нее. Для этого не требуется определять нормы непреступной деятельности в интернете. Мы считаем, что стоит учесть опыт других успешных договоров в области уголовного правосудия в том, что касается их ориентированности на основные вопросы уголовного права, наряду с широко сформулированными положениями о международном сотрудничестве и поддержкой усилий по наращиванию потенциала во всех государствах-членах.

В итоговой конвенции должны использоваться как можно более практичные, технически нейтральные и ориентированные на будущее формулировки, чтобы гарантировать, что она выдержит испытание временем и не потребует постоянного пересмотра. Это значит, что нам будет нужно сосредоточиться на самом деянии, а не на конкретных формах или методах, используемых для совершения этого деяния.

На данном этапе было бы преждевременно определять, какие требования могут возникнуть в плане механизма осуществления конвенции. Имеется широкий спектр моделей для рассмотрения, но изучение этого аспекта договора может быть отложено до тех пор, пока сфера применения и цели документа не будут определены более четко.

Цели

Новый документ прежде всего должен быть направлен на предоставление государствам гармонизированной, современной и эффективной глобальной основы для сотрудничества и координации усилий по борьбе с растущей угрозой, которую киберпреступность представляет для частных лиц, бизнеса, ключевой инфраструктуры и правительств. Следует предусмотреть в нем оказание поддержки и технической помощи, дабы все государства могли развивать потенциал и возможности для борьбы с этими угрозами. Таким образом повысится способность государств принимать эффективные меры противодействия киберпреступности на национальном, региональном и международном уровнях.

Иными словами, необходимо, чтобы договор содействовал сотрудничеству между национальными правоохранительными органами, прокуратурой и судебными органами на двусторонней или многосторонней основе в предотвращении, расследовании и преследовании за совершение преступлений, указанных в договоре. Этот элемент крайне важен для борьбы с киберпреступностью, поскольку в силу ее трансграничного характера преступники и жертвы зачастую находятся в разных юрисдикциях. Для этого будет полезно обеспечить общее понимание состава уголовных преступлений в контексте киберпространства и того, какие преступления должны быть наказуемы в национальных юрисдикциях, особенно если это понимание будет дополнено согласованными механизмами доступа к цифровым доказательствам и обмена ими с международными партнерами с соответствующими гарантиями.

Полномочия на проведение расследований указанных в договоре преступлений и на судебное преследование за них должны осуществляться при соблюдении эффективных гарантий в отношении прав человека и основных свобод, изложенных в действующих международных договорах. Кроме того, должны существовать гарантии, обеспечивающие справедливое и надлежащее применение полномочий осуществлять взаимодействие и позволяющие государствам отказываться от сотрудничества при несоблюдении определенных стандартов. Кроме того, Новая Зеландия считает, что договор должен признавать независимость национальных правоохранительных органов и органов прокуратуры и что решение о том, следует ли действовать, принимают исключительно эти органы в соответствующих государствах-членах.

Наилучшим средством обеспечить эффективное международное сотрудничество является широкая поддержка договора. Новая Зеландия считает, что для этого переговоры по договору должны быть инклюзивными и транспарентными и что необходимо приложить максимальные усилия для достижения консенсуса, чтобы обеспечить как можно более широкий мандат для конвенции. Следует предоставить всем государствам-членам возможность выразить свое мнение и принять конструктивное участие в переговорах и подкреплять свои позиции опытом и мнением гражданского общества, промышленных кругов и других соответствующих заинтересованных сторон. Следует учитывать мнение коренных народов, включая маори в Новой Зеландии (которая на языке маори называется Аотероа) и другие группы меньшинств, а также возможное влияние киберпреступности и борьбы с ней на такие группы.

Международное сотрудничество в борьбе с киберпреступностью не столь эффективно, каким бы оно могло быть. Это связано не с отсутствием воли у государств-членов, а, скорее, с отсутствием потенциала или опыта. Важнейшим требованием является оказание технической помощи и наращивание потенциала правоохранительных органов, и конвенция должна поддерживать развитие потенциала и возможностей во всем мире.

Структура

Нам интересно, какие мнения относительно сферы применения и целей конвенции выскажут другие государства в рамках этого процесса и на первой

переговорной сессии в январе 2022 года. Мы ожидаем, что после этого будет быстро и четко определено направление дальнейшей работы в этом отношении.

Нигерия

[Подлинный текст на английском языке]
[5 ноября 2021 года]

Нигерия считает, что для эффективного реагирования на быстроразвивающиеся угрозы, которые несет киберпреступность, необходимо срочно определить и ввести санкции за преступную деятельность в киберпространстве, улучшить взаимодействие между органами охраны правопорядка в разных странах, усовершенствовать процессуальные механизмы и реформировать и/или укрепить международное сотрудничество, соблюдая при этом права человека. Таким образом, при разработке конвенции Организации Объединенных Наций по данному вопросу в настоящее время необходимо сосредоточиться на борьбе с киберпреступностью и не пытаться охватить кибербезопасность и другие вопросы, связанные с киберпространством, которые подвержены влиянию политических факторов и которые лучше рассматривать на других форумах Организации Объединенных Наций. Необходимо, чтобы процесс переговоров по новой конвенции был транспарентным, инклюзивным и основанным на консенсусе и обеспечил более широкую приемлемость и/или принятие итоговой конвенции.

Сфера применения

Новая конвенция по киберпреступности должна создать правовую и институциональную основу для противодействия киберпреступности, включающую следующие элементы:

a) криминализация основных киберпреступлений: определение и установление санкций за совершение киберзависимых преступлений, объектами которых являются компьютеры или данные, и некоторых преступлений, совершаемых с использованием кибертехнологий, а также установление санкций за отмывание доходов от киберпреступлений;

b) предоставление процессуальных полномочий для расследования и преследования установленных киберпреступлений, а также для получения электронных доказательств по другим уголовным преступлениям и обмена ими;

c) положения или меры по устойчивому наращиванию потенциала и оказанию технической помощи;

d) положения или меры по возвращению доходов от киберпреступлений и возмещению ущерба;

e) положения или меры по улучшению сотрудничества и координации между правоохранительными органами и частным сектором;

f) положения или меры по расширению международного сотрудничества в связи с вышеуказанными вопросами, включая прямое сотрудничество с поставщиками интернет-услуг; и

g) положения или меры по предотвращению киберпреступлений и повышению осведомленности, включая работу с организациями гражданского общества, частным сектором, поставщиками услуг, научными и исследовательскими центрами.

Цели

Новая конвенция должна быть направлена на достижение следующих целей:

a) достижение единого понимания базовых характеристик основных киберпреступлений, процессуальных полномочий и международного сотрудничества в борьбе с киберпреступностью;

b) содействие криминализации преступлений на основе технически нейтрально сформулированных положений об основных преступлениях, чтобы они могли быть применимы не только к современным, но и к будущим технологиям и методам совершения преступлений;

c) создание органов и возможностей для сбора и получения электронных доказательств киберпреступлений и других правонарушений и обмена ими при соблюдении надлежащей правовой процедуры и обеспечении защиты прав человека и основных свобод;

d) поощрение и облегчение международного сотрудничества в борьбе с киберпреступностью и лишение лиц, совершающих киберпреступления, возможности скрыться в месте, недоступном для правосудия;

e) содействие наращиванию потенциала и оказанию технической помощи для укрепления способности правоохранительных органов бороться с киберпреступностью, а также использованию существующих институциональных возможностей, таких как базы данных Международной организации уголовной полиции (Интерпола);

f) поощрение использования государствами-членами многосторонних документов, которые уже доказали свою полезность в борьбе с киберпреступностью, таких как Конвенция Совета Европы о киберпреступности, и связи с существующими договорами Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в частности Конвенцией Организации Объединенных Наций против транснациональной организованной преступности и Конвенцией Организации Объединенных Наций против коррупции;

g) поощрение межправительственных и многосторонних процессов доверительного обмена информацией на уровне специалистов с целью определения грядущих тенденций, угроз и мер противодействия киберпреступности; и

h) создание механизма для мониторинга и/или поддержки эффективного применения и осуществления конвенции, обмена информацией и рассмотрения целесообразности какого-либо пересмотра и/или внесения поправок в будущем.

Структура

Важно, чтобы структура новой конвенции помимо преамбулы, четких определений и надлежащих заключительных положений включала следующие элементы:

a) общие положения и/или цели и описание сферы их применения;

b) меры по предупреждению киберпреступности, аналогичные изложенным в Конвенции об организованной преступности и Конвенции против коррупции, например положения о повышении информированности и образовательных инициативах;

c) основные киберпреступления и наказания;

d) нормы процессуального права и общие следственные полномочия;

e) гарантии, обеспечивающие соблюдение международных норм в области прав человека при осуществлении правоохранительной деятельности;

f) международное сотрудничество в борьбе с киберпреступностью, включая как официальное, так и неофициальное международное сотрудничество, направленное на выявление и расследование киберпреступлений и осуществление преследования за их совершение, а также на получение электронных доказательств в отношении других уголовных преступлений;

g) положения о наращивании потенциала и технической помощи для повышения квалификации специалистов-практиков и укрепления способности противодействовать киберпреступности;

h) положения о многостороннем сотрудничестве на уровне специалистов-практиков для доверительного обмена информацией и опытом с соответствующими заинтересованными сторонами;

i) положения о создании механизма для мониторинга и/или поддержки эффективного применения и осуществления конвенции, обмена информацией и рассмотрения целесообразности какого-либо пересмотра и/или внесения поправок в будущем.

Норвегия

[Подлинный текст на английском языке]
[3 ноября 2021 года]

Правительство Королевства Норвегия в рамках осуществления резолюций 74/247 и 75/282 Генеральной Ассамблеи с удовлетворением отвечает на адресованное государствам-членам предложение изложить свои мнения о сфере применения, целях и структуре новой конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Международное сотрудничество имеет решающее значение для противодействия непрерывно меняющейся угрозе киберпреступности, и правительство Норвегии с интересом ожидает участия в переговорах по всеобъемлющей конвенции по данной проблематике.

Сфера применения

В резолюции 74/247 Генеральная Ассамблея постановила учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Поскольку объектом данной резолюции определенно является преступное поведение, центральное место в конвенции должна занимать криминализация киберпреступлений.

Вопросы, касающиеся кибербезопасности и управления киберпространством, выходят за пределы поручения Генеральной Ассамблеи и не должны затрагиваться в конвенции. Эти вопросы обсуждаются на других форумах и в рамках других процессов Организации Объединенных Наций. Попытки включить в конвенцию положения о кибербезопасности и управлении киберпространством затруднят задачу разработки документа, способного получить широкую поддержку.

Угроза киберпреступности существует уже несколько десятков лет, и одна из нерешенных проблем заключается в том, что преступники во многих случаях на один шаг опережают национальные правоохранительные органы. Киберпреступления завтра будут отличаться от нынешних киберпреступлений, поэтому продолжающаяся цифровая революция существенно затрудняет задачу международного сообщества. В этой связи принципиально важно попытаться включить в конвенцию современный актуализированный перечень преступлений, способный выдержать испытание временем.

Несмотря на то, что киберпреступность меняется с каждым днем, национальные и международные учреждения смогли выявить основные повторяющиеся типы 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 или с помощью компьютерных технологий:

a) незаконный доступ, т. е. осуществление несанкционированного доступа к компьютеру или компьютерной системе;

b) незаконный перехват, т. е. неправомерный перехват в режиме реального времени содержания передаваемой информации или технических параметров трафика, относящихся к передаче информации;

c) воздействие на данные или систему, т. е. использование вредоносного программного обеспечения, атак типа «отказ в обслуживании», программ-вымогателей и удаление либо изменение данных;

d) противоправное использование устройств, т. е. незаконная торговля данными о кредите, паролями и личной информацией, которые позволяют получить доступ к ресурсам, или их незаконное использование;

e) преступления, связанные с материалами о сексуальных надругательствах над детьми;

f) преступления, связанные с компьютерным мошенничеством, т. е. манипулирование компьютерными системами или данными в мошеннических целях, например фишинг, взлом деловой переписки по электронной почте и мошенничество на аукционах;

g) преступления, связанные с нарушением авторских и смежных прав.

Кроме того, в конвенцию следует включить положения о попытке, пособничестве, подстрекательстве и сговоре, об отмывании доходов от киберпреступлений и об ответственности корпораций и других юридических лиц.

Поскольку киберпреступность непрерывно эволюционирует, важно, чтобы Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях внимательно изучал обновляемые отчеты национальных правоохранительных органов и аналогичные доклады региональных и международных организаций. Существенную ценность представляет проведенное Управлением Организации Объединенных Наций по наркотикам и преступности всестороннее исследование проблемы киберпреступности. Правительство Королевства Норвегия желает обратить внимание еще на один важный источник информации о наиболее распространенных типах киберпреступлений — ежегодную публикацию Агентства Европейского союза по сотрудничеству правоохранительных органов (Европол) “Internet Organised Crime Threat Assessment” («Оценка угрозы со стороны организованной преступности в интернете»).

Помимо положений о криминализации, в конвенции должны также присутствовать положения о процессуальных полномочиях, в частности положения о сборе и передаче электронных доказательств. Необходимо, чтобы эти положения согласовывались с надлежащими правовыми процедурами и принципами защиты прав человека и основных свобод.

Поскольку конвенция предназначена для борьбы с угрозой современной киберпреступности, она должна обязывать государства-члены добавлять во внутреннее законодательство положения, непосредственно касающиеся электронных доказательств, например правила оперативного обеспечения сохранности накопленных компьютерных данных, поиска и изъятия накопленных компьютерных данных и сбора технических параметров компьютерного трафика и

содержания информации в режиме реального времени в делах о серьезных преступлениях. Далее, конвенция должна позволять осуществлять сотрудничество в вопросах сбора и получения электронных доказательств в отношении преступлений любых типов, а не только киберпреступлений.

В частности, Специальному комитету следует обсудить положения о получении так называемых «облачных» электронных доказательств. В последнее десятилетие хранение компьютерных данных в облаке неоднократно создавало проблемы для национальных правоохранительных органов, в том числе проблемы, связанные с юрисдикцией и зависимостью в этом вопросе от других государств. Поэтому в современной и актуализированной конвенции о киберпреступности должен освещаться вопрос о том, каким образом государства-члены могут сотрудничать друг с другом в целях получения доказательств, хранящихся в облаке в других государствах.

Необходимо также, чтобы в конвенции присутствовали положения о международном сотрудничестве. В этой связи Специальному комитету следует обратиться к опыту осуществления действующих договоров, в особенности Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Конвенции Организации Объединенных Наций против коррупции. Необходимо принять во внимание положения о выдаче и взаимной помощи.

Важно также, чтобы в конвенции учитывались неодинаковые возможности государств-членов соблюдать предложенные положения, в частности положения о технической инфраструктуре и средствах. В связи с этим в конвенции должны быть предусмотрены инструментарий для создания потенциала и способы обращения за подобной помощью для государств-членов.

Наконец, в конвенции должны предусматриваться возможности сотрудничества граждан, субъектов предпринимательской деятельности, организаций и других заинтересованных сторон с правительствами в целях защиты себя и общества от киберпреступлений. Несмотря на то, что конвенция не затрагивает проблематику кибербезопасности, вопросы предупреждения киберпреступности естественным образом относятся к сфере ее применения и поэтому должны быть рассмотрены.

Цели

Специальный комитет должен стремиться к выработке действенной конвенции, обязывающей государства-члены принимать национальные законы, которые повышают эффективность предупреждения и противодействия киберпреступности на глобальном уровне. Особое значение будут иметь внутренние положения о криминализации определенных типов киберпреступлений и положения о процессуальных полномочиях и международном сотрудничестве.

Целью предстоящей работы над проектом конвенции должно стать создание правового документа, способного выдержать испытание временем и учитывающего не только все современные формы киберпреступности, но и наиболее вероятные будущие тенденции. Кроме того, проект конвенции должен представлять собой амбициозный документ, который поможет эффективно бороться с главными угрозами киберпреступности. В то же время принципиально важно придерживаться подхода, основанного на достижении консенсуса.

Правительство Королевства Норвегия желает также вновь указать на необходимость сохранения открытого, инклюзивного, прозрачного и многостороннего характера процесса работы, чтобы государства-члены могли вести переговоры в духе доброй воли с целью выработки обоснованных практических решений, которые, по нашему мнению, являются залогом присоединения к новой конвенции большого количества государств.

Структура

Содержание основных частей конвенции предопределено предлагаемой сферой ее применения и целями. Вместе с тем Специальному комитету и государствам-членам в вопросе о структуре конвенции целесообразно сохранять открытость новым идеям. Даже при том, что центральное место в конвенции должны занимать положения о криминализации, процессуальных полномочиях и международном сотрудничестве, на окончательную структуру документа могут повлиять и другие соображения. Правительство Королевства Норвегия рекомендует в вопросе о структуре конвенции придерживаться открытого подхода.

Права человека

Международное право прав человека применяется к деятельности в киберпространстве точно так же, как и к любой другой деятельности. В киберпространстве государства должны выполнять свои обязательства в области прав человека так же, как и в физическом мире. Государства должны уважать и защищать права человека, включая право на свободу выражения мнений и право на неприкосновенность частной жизни, равно как и другие имеющие отношение к данному вопросу принципы защиты данных.

Самоочевидно, что нормы о правах человека, закрепленные в Международном пакте о гражданских и политических правах, составляют важную основу для любых новых положений о киберпреступности. Тем не менее правительство Королевства Норвегия желает вновь заявить о важном значении прав человека для предстоящих переговоров, в особенности при обсуждении положений, требующих наличия внутреннего законодательства о процессуальных полномочиях.

Оман

[Подлинный текст на арабском языке]
[18 октября 2021 года]

За нападения на гражданские объекты, особенно на критически важные объекты инфраструктуры, включая сети электро- и водоснабжения, финансовые учреждения и транспортный сектор, должна предусматриваться уголовная ответственность. Такие объекты не должны становиться ареной для конфликтов между странами и использоваться для сведения счетов.

Панама

[Подлинный текст на испанском языке]
[28 октября 2021 года]

Непрерывное развитие технологий требует от государств разработки механизмов для предупреждения новых форм преступности и борьбы с ними. Пандемия COVID-19 лишь усугубила проблему, которая и до этого приобретала все более очевидный характер: мы недостаточно подготовлены к борьбе с киберпреступностью и преступлениями, совершаемыми с помощью технических средств.

Готовность к этой борьбе требует, помимо прочего, осознания того, что расследования киберпреступлений и преступлений, совершаемых с помощью цифровых средств, неизбежно имеют международную составляющую. Деятельность преступников, нашедших в транснационализации благодатную почву для достижения своих целей и ухода от ответственности, наносит ущерб всем государствам.

С учетом вышеизложенных соображений всеобъемлющая международная конвенция о противодействии использованию информационно-коммуникационных технологий в преступных целях призвана служить инструментом,

содействующим расследованию государствами данных преступлений. Для этого необходимо, чтобы конвенция охватывала не только деяния, непосредственно затрагивающие информацию, компьютерные системы и сами технологии, но и деяния, совершаемые с помощью технических средств, независимо от наличия соответствующего охраняемого законом права.

Мы считаем, что этот новый инструмент должен предусматривать принятие мер для совершенствования систем официальной и неофициальной коммуникации между государствами, что позволит повысить эффективность расследований с учетом недолговечности информации.

Наряду с укреплением системы коммуникации необходимо установить правовые рамки для таких следственных действий, как изъятие данных и переписки, сохранение данных и обращение с электронными доказательствами.

Мы осознаем, что по определенным вопросам позиции будут расходиться, однако цель должна быть прежней: создать правовой документ, способствующий противодействию использованию информационно-коммуникационных технологий в преступных целях.

Российская Федерация

Примечание Секретариата. Сообщение Российской Федерации содержится в документе A/75/980 «Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря» и в приложении к этому письму «Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях», которые были представлены Генеральной Ассамблее на ее семьдесят пятой сессии. Это сообщение передается Специальному комитету по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях вместе с сообщениями, которые отражают мнения государств-членов относительно сферы применения, целей и структуры (элементов) новой конвенции и были представлены в ответ на предложение Председателя Специального комитета.

Швейцария

[Подлинный текст на английском языке]
[28 октября 2021 года]

Информационно-коммуникационные технологии (ИКТ) оказывают сильное влияние на жизнь общества: с одной стороны, они открывают возможности для социального, культурного и экономического развития, с другой — служат основой для преступной деятельности в киберпространстве. По мере распространения в нашем мире цифровых технологий растут и показатели киберпреступности. В резолюции 74/247 Генеральная Ассамблея учредила специальный межправительственный комитет открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В настоящем сообщении излагается мнение Швейцарии о целях, сфере применения и структуре данного правового документа.

Цели

С точки зрения Швейцарии, общая цель конвенции Организации Объединенных Наций о противодействии использованию ИКТ в преступных целях должна заключаться в защите пользователей ИКТ, чтобы они могли свободно пользоваться всеми преимуществами ИКТ. В силу своего глобального и

открытого характера ИКТ выступают одним из факторов, ускоряющих прогресс в области социально-экономического развития. В связи с этим конвенция должна иметь целью обеспечение безопасности пользователей, что не должно ограничивать их свободу в использовании ИКТ. Пользователи должны иметь возможность осуществлять свои права человека и основные свободы онлайн, тем самым в полной мере реализуя потенциал открытого цифрового мира. Поэтому принятие конвенции должно стать еще одним шагом к обеспечению свободы, надежности и безопасности ИКТ.

Именно конвенция Организации Объединенных Наций способна помочь нам достичь этой общей цели. Для этого конвенция должна предусматривать скоординированный подход к борьбе с киберпреступностью. В силу транснационального характера ИКТ лица, совершающие киберпреступления, и потерпевшие могут находиться в нескольких государствах. В этой связи определяющее значение для обеспечения наивысшего уровня защиты от киберпреступлений имеет международное сотрудничество. Конвенция должна обеспечить формирование единого представления о том, что представляют собой уголовно наказуемые преступления в сфере ИКТ и за какие преступления следует предусматривать наказания в национальном законодательстве. Это будет первый шаг на пути к любого рода сотрудничеству. Закрепляя это единое представление и вводя единую терминологию, конвенция должна служить основой для эффективного международного сотрудничества в целях защиты пользователей ИКТ и обеспечения правосудия для потерпевших от киберпреступлений.

Применение скоординированного подхода к борьбе с киберпреступностью на глобальном уровне возможно лишь на основе открытого для всеобщего участия процесса. Все государства-члены должны иметь возможность внести полноценный вклад в общее дело, а именно — изложить свои мнения по поводу конвенции и обсудить мнения других государств-членов в ходе основных совещаний Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Специальный комитет должен прилагать усилия к достижению консенсуса при каждой возможности.

Киберпреступность — транснациональное явление, которое по своей сути также связано с деятельностью негосударственных субъектов. Чтобы конвенция соответствовала своему назначению, в процессе работы над ее проектом должны быть учтены все мнения. Участие всех заинтересованных сторон, включая соответствующие неправительственные организации, организации гражданского общества, научные учреждения и частный сектор, на каждом скоординированном этапе разработки конвенции принципиально важно для того, чтобы конвенция отвечала поставленным перед ней задачам[8].

Сфера применения

Нормы международного права действуют и в киберпространстве. С одной стороны, будущая конвенция не будет существовать отдельно от заключенных ранее международных соглашений, с другой стороны, она не должна лишать их смысла. Швейцария убеждена, что конвенция должна и опираться на существующий правовой режим, и усиливать его. Она должна быть рассчитана на то, чтобы дополнять уже предпринятые международным сообществом инициативы и использовать преимущества синергетического взаимодействия для эффективной борьбы с киберпреступностью.

Поскольку конвенция будет международным договором в области уголовного права, она должна опираться на нормы международного уголовного права и соответствовать им. В мире уже существует инструментарий для борьбы с проблемой киберпреступности. Помимо Конвенции Организации Объединенных Наций против транснациональной организованной преступности одним из

[8] В соответствии с пунктами 9–10 резолюции 75/282 Генеральной Ассамблеи.

стандартов, на основе которого многие страны мира, включая Швейцарию, модернизируют свое законодательство по борьбе с киберпреступностью, является Конвенция Совета Европы о киберпреступности. Она представляет собой также важный ориентир для международного сотрудничества в эпоху интернета. При разработке конвенции Организации Объединенных Наций необходимо учитывать этот опыт. Специальному комитету в своей работе следует руководствоваться результатами работы других групп и форумов, в том числе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности.

В конвенции должны быть надлежащим образом учтены, гарантированы и усилены нормы международного права прав человека. Поскольку киберпреступность представляет угрозу для соблюдения прав человека, борьба с ней должна предусматривать защиту этих прав, а не нарушать их. Те права, которыми человек обладает в повседневной жизни, должны быть гарантированы ему и при пользовании интернетом. Принимаемые меры по борьбе с киберпреступностью должны согласовываться с международным правом прав человека.

Структура

Швейцария считает, что одним из перспективных и действенных подходов к конкретизации вышеописанных целей может стать повторение структуры уже существующих международно-правовых документов в области уголовного права, переговоры по которым проходили под эгидой Организации Объединенных Наций. В связи с этим конвенция могла бы иметь следующую структуру:

a) общие положения;

b) меры предупреждения;

c) криминализация и правоохранительная деятельность;

d) международное сотрудничество;

e) техническая помощь и обмен информацией;

f) механизмы осуществления;

g) заключительные положения.

Швейцария считает, что дублировать преступления, которые уже охвачены имеющимися договорами (например, коррупцию, незаконный оборот и терроризм), не имеет смысла хотя бы потому, что они (также) могут совершаться с помощью ИКТ. Вместо этого в конвенции следует уделить внимание преступлениям, характерным исключительно для киберпространства. Составление широкого перечня преступлений, даже если каждое из них может быть совершено с помощью компьютерных систем, чревато возникновением противоречий, поэтому такой путь избирать не следует.

Включение преступлений, связанных с содержанием информации, следует свести к минимуму, и во всех случаях необходимо оценивать, насколько это целесообразно.

Швейцария подчеркивает, что необходимо и важно предусмотреть процессуальные гарантии, обеспечивающие как законность и справедливость судебного разбирательства, так и соблюдение прав участвующих в нем лиц, в частности применительно к оказанию взаимной правовой помощи, обмену информацией и выдаче на условиях, установленных соответствующими государствами. Должно быть полностью гарантировано право на неприкосновенность частной жизни. Необходимо обеспечить надлежащий уровень защиты личных данных.

Следует рассмотреть и ввести надлежащие условия и гарантии защиты прав, в частности касающиеся соблюдения и укрепления прав человека, в том числе принцип недискриминации.

Турция

[Подлинный текст на английском языке]
[4 ноября 2021 года]

Турция придает принципиальное значение свободному, открытому и безопасному использованию информационно-коммуникационных технологий во всем мире.

Развитие этих технологий повышает риск злоупотребления ими в преступных целях. Устранение этих рисков и угроз для безопасности объектов критически важной инфраструктуры и для соблюдения основополагающих прав и свобод должно быть одной из приоритетных задач в международной повестке дня. В силу транснационального характера киберпространства совершаемые в нем атаки могут иметь глобальные последствия. Уменьшить ущерб от таких атак возможно лишь с помощью эффективного сотрудничества на глобальном уровне.

Поэтому Турция придает первостепенное значение эффективному международному сотрудничеству, направленному на повышение стабильности и безопасности киберпространства на международном уровне. В этой связи Турция готова участвовать в работе Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и оказывать ему поддержку. С учетом вышесказанного мы хотели бы поделиться предварительными соображениями относительно сферы применения, целей и структуры конвенции.

В контексте разработки конвенции необходимо рассмотреть следующие вопросы:

a) создание каналов эффективного сотрудничества между государствами;

b) ясное определение вопросов, связанных с преступным использованием информационно-коммуникационных технологий;

c) создание каналов экстренной коммуникации между государствами;

d) совершенствование ресурсов для сбора и получения оперативной информации о киберугрозах;

e) налаживание обмена оперативной информацией между соответствующими органами государств;

f) предоставление информации по делам, связанным с преступным использованием информационно-коммуникационных технологий.

Помимо этого, в конвенции следует предусмотреть эффективные меры предотвращения внутренней коммуникации между преступниками и террористами и их пропагандистской деятельности.

В связи с пандемией коронавирусного заболевания (COVID-19) существенно расширилось использование дистанционной связи, поэтому в ходе переговоров по конвенции необходимо также учитывать то, как пандемия влияет на преступное использование информационно-коммуникационных технологий.

Кроме того, целесообразно в рамках сферы применения конвенции рассмотреть вопрос о безопасном использовании в борьбе с преступностью и кибератаками технологий нового поколения, например облачных вычислений, 5G, блокчейна, интернета вещей и искусственного интеллекта.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[28 октября 2021 года]

Сфера применения

Соединенное Королевство считает, что новая международная конвенция о киберпреступности должна быть предназначена для укрепления сотрудничества в борьбе с растущей угрозой, которую преступная деятельность несет для населения, предпринимателей и правительств.

Некоторые существующие региональные и международные договоры о киберпреступности уже внесли существенный вклад в борьбу с этим явлением. Необходимо использовать успешный опыт осуществления этих документов и учитывать соответствующие положения таких договоров в области уголовного правосудия, как Конвенция Организации Объединенных Наций против коррупции и Конвенция Организации Объединенных Наций против транснациональной организованной преступности.

Сфера применения будущего договора должна включать: a) расследование преступлений, указанных в договоре, и преследование за их совершение; b) развитие потенциала и расширение возможностей государств-членов для борьбы с этими преступлениями; c) утверждение форума экспертов, с помощью которого можно выявлять новые и зарождающиеся угрозы.

Международный договор Организации Объединенных Наций о киберпреступности должен охватывать преступления, совершаемые в виртуальном пространстве, и преступления, которые могут совершаться с использованием информационно-коммуникационных технологий, при этом в обоих случаях использование компьютера должно увеличивать масштаб, сферу охвата и скорость преступления. Сотрудничество эффективно в тех случаях, когда указанные в договоре преступления одинаково классифицируются и признаются преступлениями во всех правовых системах.

Определения преступлений в договоре не должны ограничивать осуществление права на свободу слова и убеждений.

Поскольку это будет договор в области уголовного права, внимание в нем должно быть сосредоточено на деятельности, которую следует осуществлять национальным правительствам. Кроме того, в нем следует предусмотреть возможности сотрудничества в рамках многостороннего подхода между гражданами, неправительственными организациями, организациями гражданского общества, научными учреждениями и частным сектором для защиты от киберпреступности.

Любой договор должен предусматривать эффективные гарантии защиты прав, включающие уважение права на неприкосновенность частной жизни и других прав человека, закрепленных в нормах международного права прав человека и признанных в соответствующих резолюциях Генеральной Ассамблеи и Совета по правам человека.

Договор должен разрабатываться на инклюзивной и прозрачной основе с учетом мнений всех государств-членов и при активном участии широкого круга заинтересованных сторон, включая неправительственные организации, организации гражданского общества, научные учреждениям и частный сектор. Более того, положения договора, например положения о его осуществлении и создании потенциала, должны стимулировать также применение инклюзивного и прозрачного подхода к борьбе с киберпреступностью.

Формулировки должны носить технически нейтральный характер, чтобы договор со временем не утратил актуальности и не требовал постоянного обновления.

Договор не должен дублировать уже проделанную работу или работу, которую уместно выполнять в рамках других форумов. Договор не должен затрагивать вопросы кибербезопасности, которыми уже занимается Первый комитет Генеральной Ассамблеи, или вопросы регулирования интернета, которые уже рассматриваются на специализированных многосторонних форумах.

Цели

Главная цель договора должна заключаться в поддержке эффективного двустороннего или многостороннего сотрудничества национальных правоохранительных органов и органов прокуратуры в вопросах расследования преступлений, указанных в договоре, и преследования за их совершение. Обеспечить максимально широкое международное сотрудничество способен лишь договор, пользующийся широкой поддержкой.

Для содействия эффективному сотрудничеству должны быть предусмотрены возможности отказа в сотрудничестве на основании принципа обоюдного признания соответствующего деяния преступлением, отказа в отношении политических преступлений, особенно в случаях, когда предполагаемое преступление касается осуществления права на свободу слова, и отказа в выполнении запроса, направленного с целью наказания или преследования какого-либо лица по признаку расы, религии, пола или по другим подлежащим защите признакам. Целесообразно установить минимальные требования к запросам, выполнение которых должен обеспечить запрашивающий орган, например требования относительно необходимости запроса, его соразмерности, ограниченности по времени и санкционирования на конкретном уровне.

Использование полномочий на расследование указанных в договоре преступлений или преследование за их совершение, в том числе полномочий, применяемых в двусторонних или многосторонних делах, должно сопровождаться применением эффективных гарантий защиты прав человека и основных свобод, провозглашенных в нормах международного права прав человека.

В договоре должна признаваться независимость оперативной деятельности национальных органов следствия и прокуратуры и их исключительное право принимать решение о том, следует ли предпринимать какие-либо действия.

Договор должен поддерживать подготовку кадров на глобальном уровне и деятельность по созданию потенциала.

Угрозы, создаваемые преступной деятельностью в киберпространстве, со временем будут меняться, и в договоре должен быть прописан межправительственный и многосторонний процесс определения будущих угроз, который при этом не обязательно должен являться частью договора.

Учитывая, что киберпреступность затрагивает представителей разных полов в неодинаковой степени, в договоре должен приниматься во внимание гендерный фактор, что поможет более эффективно бороться с киберпреступностью. Разработка договора о киберпреступности, в положениях которого учтены гендерные соображения, побудит большее число женщин участвовать на всех уровнях во всех процессах, связанных с договором. Это приведет к выработке более разнообразных, содержательных и в конечном итоге более эффективных решений. На состоявшемся в апреле 2021 года совещании межправительственной Группы экспертов для проведения всестороннего исследования проблемы киберпреступности все государства-члены согласились с тем, что необходимо, в частности, стимулировать участие в работе экспертов из числа женщин.

Договор должен поощрять участие в борьбе с киберпреступностью всего общества и побуждать государства-члены взаимодействовать с лицами, не

работающими в правительственных структурах, например с экспертами, представителями промышленности и общественности, в таких областях, как информационная работа, совершенствование образования, обучение по вопросам взаимосвязи гендера и киберпреступности и оказание поддержки потерпевшим от преступлений.

Структура

Соединенное Королевство считает, что эффективным способом организации текста договора будет использование следующей структуры:

a) Общие положения

Общие положения должны включать обоснование и назначение договора и определения терминов, которые будут употребляться в тексте. В отношении определений должно быть достигнуто взаимопонимание и согласие всех сторон, они должны быть технически нейтральными, и при их формулировании необходимо учитывать терминологию, согласованную на широкой основе в региональных правовых документах и используемую в нормативно-правовой базе различных стран.

b) Основные преступления

В число охватываемых договором преступлений должны входить преступления, совершаемые в виртуальном пространстве (например, незаконный доступ); описания и определения таких преступлений должны быть приемлемыми для всех сторон. Что касается преступлений, которые могут совершаться с использованием информационно-коммуникационных технологий (например, сексуальная эксплуатация детей и сексуальные надругательства над ними или мошенничество), то в договор их следует включать при условии, что преступление главным образом совершается онлайн, компьютеры меняют масштаб и скорость совершения преступления и определение преступления одинаково понимается всеми сторонами.

c) Права человека и гарантии защиты прав

При применении и осуществлении договора должны использоваться эффективные процессуальные гарантии защиты прав и строгие меры защиты прав человека, а также учитываться базовые нормы международного права прав человека.

d) Меры предупреждения

Подобно Конвенции против коррупции и Конвенции об организованной преступности, договор должен включать положения, стимулирующие государства принимать меры для предупреждения киберпреступности, в том числе путем взаимодействия со всеми заинтересованными сторонами.

e) Положения процессуального права

В отношении внутренних и международных расследований полномочия по содействию расследованию и преследованию должны позволять соответствующим органам сохранять, искать и изымать электронные доказательства в случае с любым преступлением, совершенным с помощью компьютера, или в тех случаях, когда доказательства совершения преступления имеют электронную форму.

f) Международное сотрудничество

Положения о международном сотрудничестве должны охватывать оказание взаимной правовой помощи и экстренной помощи и включать требование об учреждении в странах контактных центров, функционирующих круглосуточно. Рекомендации, вынесенные Группой экспертов в апреле 2021 года, ясно указывают на то, что помимо практического обмена доказательствами государства-члены желают продолжать обмен опытом и

информацией о передовой практике, а также информацией о новых и растущих угрозах.

g) Техническая помощь и создание потенциала

Создание потенциала необходимо стимулировать, и существенная роль в этой деятельности должна отводиться Управлению Организации Объединенных Наций по наркотикам и преступности, при этом координировать работу в этой области следует силами существующих структур, таких как Глобальный форум по обмену опытом в области компьютерных технологий. Соединенное Королевство отмечает, что в апреле 2021 года Группа экспертов согласовала большое количество рекомендаций по созданию потенциала, включая организацию для специалистов-практиков специализированного и отвечающего современным требованиям обучения по вопросам расследования киберпреступлений, обращения с электронными доказательствами, обеспечения хранения и передачи доказательств и проведения судебной экспертизы.

h) Осуществление

Должен быть разработан ясный план осуществления договора.

Соединенные Штаты Америки

[Подлинный текст на английском языке]
[28 октября 2021 года]

Правительство Соединенных Штатов Америки с удовлетворением откликается на предложение государствам-членам изложить свои мнения относительно сферы применения, целей и структуры (элементов) новой конвенции во исполнение резолюций 74/247 и 75/282 Генеральной Ассамблеи. Соединенные Штаты надеются на совместную работу с другими государствами-членами и заинтересованными сторонами над проектом глобального документа, направленного на улучшение расследования и судебного преследования киберпреступности, в соответствии с существующими правами и обязательствами и на их основе. Соединенные Штаты вновь заявляют о важности того, чтобы процесс был открытым, инклюзивным, прозрачным и многосторонним, что позволит всем государствам-членам добросовестно вести переговоры с целью выработки продуманных и основанных на консенсусе практических решений, которые, по нашему мнению, будут способствовать широкому присоединению к новому глобальному документу по борьбе с киберпреступностью.

Предлагаемые сроки завершения работы считались бы жесткими даже в обычных обстоятельствах, а теперь работа будет проходить еще и на фоне глобальной пандемии. Поэтому тем более важно, чтобы наши усилия по выработке глобального документа по борьбе с киберпреступностью были целенаправленными и эффективными. К сожалению, пока бóльшая часть мира борется с пандемией коронавирусного заболевания (COVID-19), киберпреступники используют произошедший глобальный переход на цифровые технологии и зависимость от них. Киберпреступность представляет собой прямую угрозу безопасности и благополучию общества и людей во всем мире. Уже длительное время имеет место сотрудничество по укреплению коллективной способности бороться с этой деятельностью, и мы можем продолжать развивать успешные результаты, тщательно продумывая практические решения. Учитывая актуальность угрозы киберпреступности, тем более важно прилагать целенаправленные и взвешенные усилия с целью согласования глобального документа по борьбе с киберпреступностью.

Этот документ должен быть направлен на укрепление международного сотрудничества и предоставление национальным правоохранительным органам практических инструментов для борьбы с киберпреступностью, как это

обеспечили другие документы Организации Объединенных Наций в отношении других форм транснациональной преступности, включая коррупцию, оборот наркотиков, торговлю людьми и незаконный ввоз мигрантов. Этот документ должен также обеспечить национальным органам возможность собирать и получать электронные доказательства, относящиеся к любым составам преступлений, а не только к киберзависимым преступлениям, и способствовать международному сотрудничеству по таким делам. Как и в любом другом документе Организации Объединенных Наций по борьбе с преступностью, эти инструменты должны включать в себя соответствующие ограничения и гарантии, в контексте существующей национальной нормативной базы, для учета принципа неприкосновенности частной жизни и гражданских свобод при полном соблюдении прав человека. Документ по борьбе с киберпреступностью должен также учитывать растущую потребность в технической помощи и предоставлять государствам-членам возможности для обращения за такой помощью.

В связи с тем, что государства-члены начинают процесс подготовки проекта, необходимо сознавать, что они делают это не в вакууме. Насколько важно определить, что должен охватывать этот документ, настолько же важно понять, что выходит за рамки собственно его сферы применения. В настоящее время в Организации Объединенных Наций и других межправительственных и многосторонних форумах ведется полезная работа по другим связанным с киберпространством вопросам, выходящим за рамки киберпреступности. Важно не дублировать и не подрывать эту работу как во избежание коллизии обязанностей, так и для того, чтобы не отвлекаться от задачи разработать конкретно ориентированный практический инструмент для борьбы с киберпреступностью. Попытка охватить в этом инструменте уголовного правосудия все вопросы, связанные с киберпространством, рискует превратить переговорный процесс в аморфные и неконкретные дебаты, которые мало чем помогут борьбе с киберпреступностью и только замедлят работу по подготовке полезного документа.

В частности, государствам-членам не следует углубляться в широкомасштабные темы управления киберпространством или кибербезопасности в документе по вопросам преступности, посвященном борьбе с киберпреступностью. Борьба с киберпреступностью и кибербезопасность нередко рассматриваются как две стороны одной медали, однако противодействие киберпреступности по сути является прерогативой государства, а обеспечение кибербезопасности — обязанностью целого ряда государственных и частных структур. Мандат Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях прежде всего предусматривает разработку инструмента уголовного правосудия по уголовно-правовым вопросам, чтобы содействовать международным мерам противодействия киберпреступности, которые включают определение и применение санкций за преступное поведение в киберпространстве. Специальный комитет не уполномочен предписывать общемировые нормы некриминального поведения в интернете. Включение концепций управления киберпространством и кибербезопасности в договор о киберпреступности не отвечает цели разработки четкого и эффективного документа, который будет пользоваться широкой поддержкой государств-членов.

Как подтверждено в резолюции 75/282 Генеральной Ассамблеи, жизненно важно, чтобы переговоры с целью разработки нового документа по борьбе с киберпреступностью не препятствовали существующим механизмам, включая многонациональные и региональные инструменты, которые уже предоставляют целый ряд средств для эффективной борьбы с киберпреступностью. Наилучший способ добиться консенсуса в отношении этого нового документа и избежать политических и вызывающих разногласия вопросов — это опереться на существующие документы, доказавшие свою эффективность. Нам следует ориентироваться на достижения в осуществлении других договоров Организации Объединенных Наций в области уголовного правосудия, таких как Конвенция Организации Объединенных Наций против транснациональной организованной

преступности. Эта Конвенция оказалась чрезвычайно полезной, поскольку направлена против основных видов организованной преступной деятельности и при этом включает широкие положения о международном сотрудничестве, которые могут применяться к любому виду серьезных преступлений, совершаемых с целью получения дохода тремя или более лицами. В результате Конвенция об организованной преступности тысячи раз успешно использовалась ее участниками, в том числе для борьбы с такими преступлениями, как использование программ-вымогателей и сексуальная эксплуатация детей.

Соединенные Штаты еще раз заявляют о важности обеспечения того, чтобы процесс был открытым, инклюзивным и прозрачным, что позволит всем государствам-членам и заинтересованным сторонам добросовестно вести переговоры с целью выработки продуманных и основанных на консенсусе практических решений, что, по нашему мнению, лучше всего будет стимулировать широкое присоединение к новому глобальному документу по борьбе с киберпреступностью.

Криминализация основных киберпреступлений

Прежде всего, любой новый документ должен обеспечивать национальным органам возможность собирать и получать электронные доказательства в отношении любого вида преступлений. Такие полномочия необходимы для того, чтобы страны могли эффективно расследовать и в судебном порядке преследовать практически все виды преступлений, поскольку лишь очень немногие современные преступления совершаются полностью вне цифровой сферы. Этот документ должен также способствовать международному сотрудничеству для обмена электронными доказательствами по любому виду преступлений с учетом гибкого применения положения об обоюдном признании соответствующего деяния преступлением, содержащегося в Конвенции об организованной преступности и Конвенции Организации Объединенных Наций против коррупции[9].

Кроме того, для эффективного международного сотрудничества требуется, чтобы у государств-членов имелось адекватное внутреннее законодательство, предусматривающее уголовную ответственность за основные киберпреступления. Дабы не допускать создания безопасных убежищ для киберпреступников, необходимо, чтобы у государств-членов было общее понимание основных преступлений и имелись сопутствующие процессуальные полномочия. Исследования Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) показывают, что страны в целом согласны с тем, какие основные линии поведения следует признавать уголовно наказуемыми в конкретных законах о киберпреступности, при этом общие положения содержатся во многих многонациональных соглашениях и уголовном законодательстве многих стран. Сложилось также и международное понимание законных видов процессуальных полномочий для поддержки эффективного расследования киберпреступлений. В результате специалистами-практиками накоплен двадцатилетний разнообразный опыт расследования киберпреступлений, что свидетельствует о неизменной востребованности общепринятых типов основных и процессуальных полномочий для расследования киберпреступлений.

Новый документ по борьбе с киберпреступностью должен содержать определение и применяться в отношении киберзависимых преступлений, т. е. преступлений, в которых объектом преступной деятельности являются компьютеры или данные, а также определенных преступлений, совершаемых посредством кибертехнологий, т. е. преступлений, для облегчения совершения которых

[9] См. пункт 9 статьи 18 Конвенции Организации Объединенных Наций против транснациональной организованной преступности и пункт 9 статьи 46 Конвенции Организации Объединенных Наций против коррупции. Хотя положения этих двух конвенций несколько отличаются, обе предоставляют запрашиваемым государствам-участникам значительную свободу действий при предоставлении помощи, особенно в отношении применения принудительных мер.

используется компьютер. К этой первой и доминирующей категории преступлений, которая должна быть определена в новом документе, относятся те, которые невозможно совершить без противозаконного использования компьютеров или сетевых систем и которые, следовательно, не существовали как преступления до появления компьютерных систем. Киберзависимые преступления могут происходить полностью в цифровой сфере. Для основных уголовных киберзависимых преступлений, таких как атаки типа «отказ в обслуживании» или повреждение компьютеров и данных, требуются законы, непосредственно касающиеся кибертехнологий, поскольку в большинстве юрисдикций уголовные законы толкуются строго, а традиционные законы, охватывающие такие привычные понятия, как незаконное проникновение и вандализм, часто не подходят для применения к киберпреступности. Более того, некоторые положения уголовного кодекса, применимые к преступлениям, совершаемым вне компьютерной сети, нелегко применить к действиям, совершаемым с использованием компьютеров.

Напротив, мы должны проявлять осмотрительность и не рассматривать традиционные преступления как «киберпреступления» только потому, что при их планировании или совершении использовался компьютер. Несмотря на противозаконное использование компьютера для совершения преступления, некоторые виновные деяния могут подпадать под действие общих законов, поскольку в самом использовании компьютерной системы при таком деянии нет ничего особенного или уникального. Напротив, некоторые преступления, совершаемые посредством кибертехнологий, уместно рассматривать на основе документа по борьбе с киберпреступностью, например, когда использование компьютера:

a) увеличивает масштаб преступления, например число пострадавших исчисляется тысячами или украдены миллионы записей платежных данных;

b) повышает скорость атаки, поскольку компьютер многократно увеличивает возможность совершения преступления;

c) увеличивает размер ущерба или вреда, причиненного жертвам; или

d) повышает степень анонимности преступника.

Если применять эти понятия, то некоторые традиционные составы преступлений, такие как мошенничество и эксплуатация детей, также могут быть обоснованно отнесены к предмету этих переговоров. Однако государствам-членам следует рассудительно подойти к определению круга преступлений с использованием кибертехнологий, с которыми мы намерены бороться, чтобы не исказить давно устоявшиеся концепции уголовного правосудия. Давно действующие положения и инструменты уголовного законодательства не теряют своей применимости только потому, что преступление включает в себя некий «цифровой элемент».

В глобальном документе по борьбе с киберпреступностью должен также содержаться призыв к его сторонам принять законодательство, в технически нейтральных формулировках предусматривающее уголовную ответственность за основные киберпреступления, обеспечивая при этом процессуальные гарантии. Формулирование положений о криминализации в технически нейтральных терминах (т. е. криминализация деятельности, нарушающей конфиденциальность, целостность и доступность компьютерных данных, а не криминализация используемых конкретных форм или методов, таких как фишинг или программы-вымогатели) станет гарантией того, что основные положения об уголовной ответственности будут применимы не только к нынешним, но и к будущим технологиям и методам совершения преступлений. Иллюстрацией стремительного развития технологий служит проект Всестороннего исследования проблемы киберпреступности 2013 года, которое явно стремилось быть всеобъемлющим, но не сдержит подробного описания технологий или методов, которые широко не использовались или только появлялись во время исследования, включая программы-вымогатели, интернет вещей, криптовалюту, а также быстрое

развитие и преобладание мобильных технологий. Отражением этой озабоченности стало согласование государствами-членами на совещании Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, в частности, вывода и рекомендации о том, что государствам-членам следует обеспечить, чтобы их законодательные положения отвечали требованиям времени с учетом технического прогресса посредством принятия законодательства, содержащего технически нейтральные формулировки и предусматривающего уголовную ответственность за деятельность, признаваемую незаконной, а не за использование технических средств[10]. Это особенно важно, поскольку мы пытаемся разработать сохраняющий актуальность документ, способный должным образом учитывать технологии завтрашнего дня и удовлетворять потребности сотрудников правоохранительных органов и в настоящее время и в будущем.

С учетом этих принципов глобальный документ по борьбе с киберпреступностью должен предусматривать криминализацию следующих действий:

a) неправомерный доступ, т. е. доступ к компьютеру или компьютерной системе без разрешения;

b) незаконный перехват, т. е. противоправный перехват в режиме реального времени содержания сообщений или данных трафика, связанных с сообщениями;

c) вмешательство в данные или системы, т. е. распространение вредоносных программ, атаки типа «отказ в обслуживании», распространение вирусов-вымогателей и уничтожение или модификация данных;

d) неправомерное использование устройств, т. е. незаконный оборот или использование данных кредитных карт, паролей и личной информации, позволяющих получить доступ к ресурсам;

e) преступления, связанные с материалами о сексуальном насилии над детьми;

f) преступления, связанные с мошенничеством с использованием компьютеров, т. е. манипуляции с компьютерными системами или данными в мошеннических целях, такие как фишинг, взлом деловой электронной почты и мошенничество на аукционах;

g) преступления, связанные с нарушением авторского права и смежных прав; и

h) положения, касающиеся покушения, пособничества и подстрекательства, а также заговора.

Кроме того, за отмывание доходов от киберпреступлений также следует установить уголовную ответственность. Наконец, для юридических лиц в случае их участия в запрещенных в этом документе киберпреступлениях должны быть предусмотрены уголовные или гражданско-правовые и административные санкции.

Процессуальные полномочия в отношении сбора электронных доказательств и обмена ими

Помимо криминализации основных преступлений в глобальном документе по борьбе с киберпреступностью должна быть также отражена необходимость сбора, обеспечения сохранности и обмена электронными доказательствами национальными судебными инстанциями в соответствии с надлежащей правовой процедурой и при обеспечении защиты прав человека и основных свобод. Некоторые государства-члены отметили, что в соответствии с их внутренним

[10] См. Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, прошедшего в Вене 6–8 апреля 2021 года (UNODC/CCPCJ/EG.4/2021/2).

законодательством традиционные источники процессуальных полномочий могут быть неприменимы к неосязаемым данным или не позволяют достаточно быстро собирать неустойчивые электронные доказательства. Как всегда, устаревших законов будет недостаточно для решения многих задач, связанных с расследованием электронных преступлений, включая работу с новыми технологиями, такими как широко распространенное шифрование и сервисы облачных вычислений. Поэтому требуются специализированные источники процессуальных полномочий в отношении сбора электронных доказательств. При разработке таких законов следует учитывать применимые технические концепции, а также практические потребности следователей по уголовным делам. В частности, эти источники процессуальных полномочий должны предоставлять возможности для:

a) оперативного обеспечения сохранности информации, хранимой в электронной форме;

b) выдачи распоряжений о предоставлении компьютерных данных;

c) производства обыска и выемки информации, хранимой в электронной форме;

d) сбора в режиме реального времени информации о компьютерном трафике; и

e) сбора в режиме реального времени данных о контенте в случае серьезных преступлений.

Кроме того, новый документ должен предусматривать возможность сотрудничества в целях сбора и получения электронных доказательств по любому виду преступлений, а не только по киберпреступлениям. Практически все значительные уголовные преступления связаны с электронными доказательствами, будь то информация с мобильного телефона, электронная почта, данные транзакций или другие данные, которые имеют значение для расследования преступлений и судебного преследования за них. Что касается внутригосударственных задач, то государствам-членам требуется современная нормативно-правовая база для работы с доказательствами, которая позволяет считать допустимыми электронные доказательства при проведении уголовных расследований и осуществлении уголовного преследования, включая обмен электронными доказательствами с правоохранительными органами-партнерами на международном уровне.

Международное сотрудничество

Основой эффективного международного сотрудничества в борьбе с киберпреступностью помимо внутреннего законодательства являются официальные договоры о сотрудничестве, например о взаимной правовой помощи, и другие механизмы, такие как традиционное сотрудничество на уровне уполномоченных органов полиции. В новом документе по борьбе с киберпреступностью следует учесть эффективные средства для расширения международного сотрудничества, предусмотренные в действующих договорах, и при этом следует обеспечить, чтобы он не помешал применению существующих документов и текущему международному сотрудничеству в глобальной борьбе с киберпреступностью. Положения документа по борьбе с киберпреступностью, касающиеся международного сотрудничества, в том числе по вопросам взаимной правовой помощи, выдачи, передачи судебного преследования, конфискации доходов от преступлений, в том числе в виртуальных валютах, и возвращения конфискованных активов пострадавшим, а также обоюдного признания соответствующего деяния преступлением, и сотрудничества правоохранительных органов, должны строго соответствовать положениям Конвенции об организованной преступности и Конвенции против коррупции, включая предусмотренные в них соответствующие гарантии и меры правовой защиты, которые успешно применяются подавляющим большинством государств-членов. Кроме того, положение о взаимной правовой помощи должно предусматривать оказание широкой помощи в

получении электронных доказательств, относящихся к уголовному преступлению, независимо от того, было ли оно совершено с использованием или без использования компьютерной системы.

Техническая помощь и наращивание потенциала

Согласно исследованиям УНП ООН, более 75 процентов стран имеют в своих правоохранительных органах специальные подразделения по борьбе с киберпреступностью, а около 15 процентов имеют отдельный специальный орган по киберпреступности. Это указывает на особый характер расследований киберпреступлений, включая необходимость специальной подготовки. Кроме того, киберпреступления и традиционные преступления с электронным или цифровым элементом стали значительно сложнее, что выдвигает дополнительные требования к обучению и переподготовке высококвалифицированных следователей и технических экспертов.

Нехватка внутренних ресурсов — наиболее распространенная причина, по которой страны не имеют возможности эффективно сотрудничать на международном уровне. Неспособность большинства стран осуществлять международное сотрудничество обусловлена не отсутствием воли, а недостатками внутреннего законодательства или нехваткой опыта правоохранительных органов. Во многих государствах-членах недостаточная оснащенность правоохранительных органов не позволяет бороться с киберпреступностью или работать с электронными доказательствами. Так, в свете существующих национальных приоритетов, некоторые государства-члены сталкиваются с трудностями в подготовке и удержании квалифицированных следователей и экспертов-криминалистов и в решении проблемы нехватки компьютерных и программных средств. Соответственно, существует широкий международный консенсус в отношении того, что для эффективного международного противодействия киберпреступности по-прежнему существует острая необходимость в оказании правоохранительным ведомствам, включая следственные органы, прокуратуру и суды, технической помощи и помощи в наращивании потенциала. Более того, поскольку электронные доказательства становятся компонентом почти всех видов преступлений, даже не имеющим специальной подготовки сотрудникам правоохранительных органов потребуется некоторое базовое понимание расследований, связанных с использованием компьютеров.

Положения документа по борьбе с киберпреступностью, касающиеся технической помощи и наращивания потенциала, должны предусматривать:

a) принятие государствами-членами мер по инициированию, разработке или совершенствованию программ обучения сотрудников, ответственных за предупреждение и противодействие киберпреступности;

b) рассмотрение государствами-членами, с учетом своих возможностей, вопроса о предоставлении друг другу самой широкой технической помощи, особенно в интересах развивающихся стран и стран, для которых могут быть несоразмерно высоки угрозы киберпреступности, в рамках своих соответствующих планов и программ борьбы с киберпреступностью;

c) создание механизмов, с помощью которых добровольные финансовые взносы государств-членов могли бы содействовать выполнению положений документа по борьбе с киберпреступностью;

d) рассмотрение государствами-членами вопроса о внесении добровольных взносов для поддержки Глобальной программы борьбы с киберпреступностью УНП ООН и связанных с ней усилий по наращиванию потенциала в области уголовного правосудия.

Участие общества, субъектов и организаций

Противодействие киберпреступности, учитывая сложность и многогранность этой проблемы, не может осуществляться в отрыве от остальных усилий.

В документе по борьбе с киберпреступностью следует отразить важность активного участия в предупреждении киберпреступности отдельных лиц и групп, при должном учете требования гендерного паритета, включая неправительственные организации, организации гражданского общества, академические учреждения и частный сектор. Такое участие может способствовать повышению осведомленности населения об угрозах киберпреступности, обеспечению прозрачности работы государств-членов и решению важных вопросов, касающихся неприкосновенности частной жизни, гражданских свобод и прав человека. Кроме того, эффективность документа зависит от вклада физических лиц и структур, обладающих опытом в сфере борьбы с киберпреступностью. Для того чтобы документ по борьбе с киберпреступностью был реально действующим и эффективным, требуется деятельное участие специалистов в этой области.

Механизмы осуществления

На данном этапе слишком рано определять, нужен ли отдельный процесс для анализа реализации документа в будущем, и если нужен, то в какой форме. Существуют разные успешные модели, которые можно рассмотреть. Ввиду дефицита ресурсов, выделяемых на техническую помощь, следует уделить внимание методам, основанным на низкозатратных вариантах, чтобы максимально увеличить взносы доноров на техническую помощь. Один из таких методов мог бы заключаться в том, чтобы предоставить Комиссии по предупреждению преступности и уголовному правосудию, учрежденной резолюцией 1992/1 Экономического и Социального Совета, полномочия рассматривать все вопросы, относящиеся к целям документа по борьбе с киберпреступностью. Существует успешный прецедент выполнения таких функций — деятельность Комиссии по наркотическим средствам, которая осуществляет надзор за тремя международными договорами о контроле над наркотиками. Как указано в предыдущем разделе, посвященном участию общества, субъектов и организаций, важно, чтобы деятельное участие общественности, субъектов и организаций принималось во внимание при реализации любого направления деятельности, рекомендованного в документе. Однако обсуждение механизмов осуществления следует отложить до дальнейшего определения сферы применения документа.