Distr.: General
21 February 2017
Russian
Original: English

Группа экспертов для проведения всестороннего исследования проблемы киберпреступности
Вена, 10-13 апреля 2017 года

Ход обсуждений на первом совещании Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 17-21 января 2011 года

Резюме Докладчика

I. Введение

1. В своей резолюции 65/230 Генеральная Ассамблея просила Комиссию по предупреждению преступности и уголовному правосудию учредить в соответствии с пунктом 42 Салвадорской декларации о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развития в изменяющемся мире, межправительственную группу экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

2. Первое совещание Группы экспертов для проведения всестороннего исследования проблемы киберпреступности было проведено в Вене 17-21 января 2011 года. (Доклад о работе этого совещания см. UNODC/CCPCJ/EG.4/2011/3.) Совещанию были представлены проект предварительной повестки дня (UNODC/CCPCJ/EG.4/2011/1) и проекты тем для рассмотрения в рамках всестороннего исследования проблемы киберпреступности и ответных мер (UNODC/CCPCJ/EG.4/2011/2), подготовленные Секретариатом. Группа экспертов рассмотрела и приняла краткий доклад по процедурным вопросам, сборник основных тем для рассмотрения в рамках исследования и методологию и примерные сроки проведения исследования, которые были доведены до сведения Комиссии по предупреждению преступности и уголовному правосудию на ее двадцатой сессии (см. E/CN.15/2011/19, приложения I и II).

3. Работа по составлению резюме хода обсуждения вопросов существа была начата, но не доведена до конца из-за недостатка средств. В своей резолюции 22/7 от 26 апреля 2013 года Комиссия предложила группе экспертов за-

вершить подготовку кратких докладов о работе ее первого и второго совещаний, проведенных в Вене соответственно 17-21 января 2011 года и 25-28 февраля 2013 года. На заседании расширенного бюро Группы экспертов, проведенного 1 декабря 2016 года, Председатель просил Докладчика завершить подготовку кратких докладов к концу января 2017 года и информировать Секретариат и Председателя о ходе этой работы. Соответственно Докладчик Кристофер Д. Рэм (Канада) рассмотрел первоначальные комментарии и элементы проекта резюме и отчеты заседаний сессии для подготовки и окончательной доработки настоящего резюме.

4. Обсуждения Группы экспертов были основаны на принятой повестке дня, проекте перечня основных тем и предложенной методологии исследования, которая была разработана в ходе сессии. Настоящее резюме хода обсуждений дополняет решения, касающиеся сферы охвата или методологии исследования, на основе рассмотрения как затронутых вопросов существа, так и информации, представленной экспертами на первом совещании. Оно включает мнения, высказанные межправительственными и другими экспертами по целому ряду вопросов, включая вопросы существа, вызывающие обеспокоенность государств-членов, проект перечня основных тем и других тем, предложенных для включения в исследование, и процедурные и методологические вопросы, касающиеся проведения самого исследования. Оно отражает повестку дня совещания, однако в связи с тем, что многие вопросы были затронуты неоднократно, оно, насколько это возможно, основано на тематическом подходе.

II. Резюме хода обсуждений

A. Проблема киберпреступности (пункт 2 повестки дня)

5. Эксперты обсудили масштабы использования и роль информационно-коммуникационных технологий в их странах и вопрос о том, как эти факторы связаны с киберпреступностью. Большинство экспертов отметили растущие масштабы киберпреступности. Они также отметили, что существуют конкретные и сложные связи между a) распространенностью и использованием технологий как в государствах-членах, так и на региональном уровне, и b) развитием киберпреступности. Было признано, что проблема киберпреступности носит универсальный, но не обязательно единообразный характер. Многие выступавшие согласились с тем, что эта проблема вызывает обеспокоенность во всем мире. Ряд экспертов отметили, что сложные формы преступности и виктимизации и потоки данных и доходы от преступлений, помимо других факторов, имеют разные последствия в разных странах. Было отмечено, что распространение технологий и связанная с этим проблема киберпреступности также затрагивают вопросы, связанные с национальным суверенитетом, независимостью, управлением, правами человека и культурой. Ряд экспертов упомянули о необходимости уважения суверенной независимости и культурного разнообразия как при разработке определений киберпреступности, так и при рассмотрении внутренних, транснациональных и глобальных мер реагирования на нее.

6. В ходе сессии неоднократно рассматривались следующие несколько аспектов проблемы киберпреступности:

a) *информационные технологии и компьютерные сети*. Эксперты отметили, что информационные технологии и компьютерные сети представляют собой как возможность, так и цель внутренних и международных усилий в области развития, а также рассматриваются в качестве средства обеспечения и максимального повышения эффективности помощи в целях развития и технического содействия. С этой точки зрения киберпреступность рассматривается также как один из факторов, способных поставить под угрозу возможности в области развития. В этой связи пути и средства решения этой проблемы имеют важное значение для всех государств-членов. Эксперты также отметили, что,

хотя киберпреступность и связанная с ней деятельность могут иметь разные последствия для развитых и развивающихся стран, все государства-члены имеют общие стимулы для содействия процессу развития и его защиты от киберпреступности. В более общем плане они отметили, что, поскольку компьютерные сети позволяют правонарушителям в одном государстве использовать инфраструктуру и причинять ущерб потерпевшим в другом государстве, и то, и другое государство заинтересованы в предупреждении киберпреступности и борьбе с ней вне контекста развития;

b) *скорость и масштабы развития как технологий, так и киберпреступности*. Эти факторы создают проблемы для законодателей, правоохранительных органов и систем уголовного правосудия, особенно в развивающихся странах. Была выражена обеспокоенность по поводу необходимости обеспечения того, чтобы внутренние законы, международные договоры и программы технической помощи были актуальны и чтобы техническая помощь оказывалась на постоянной основе;

c) *транснациональный характер компьютерных сетей и киберпреступности*. Эксперты отметили, что ограничения, связанные с суверенитетом, международной вежливостью и территориальной юрисдикцией распространяются на официальные органы, отвечающие за борьбу с киберпреступностью и защиту потерпевших и инфраструктуры, но не распространяются на самих правонарушителей. Этот вопрос часто затрагивался не только в контексте правоохранительной деятельности и международного сотрудничества, но и в связи с более общими политическими областями, воздействием прав человека на формы криминализации киберпреступности и национальным и глобальным регулированием технологий по причинам, необязательно связанным с преступностью;

d) *сложный характер киберпреступлений, скорость, с которой они совершаются, и проблемы, которые эти факторы создают для уголовных расследований и судебного преследования с точки зрения как внутренних возможностей следствия, так и правовых и иных механизмов международного сотрудничества*. Было отмечено, что необходимость создания оперативных или ускоренных следственных полномочий и их согласования с гарантиями обеспечения верховенства права создает проблемы для национальных законодателей и следователей;

e) *проблемы, создаваемые скоростью совершения киберпреступлений и их транснациональным характером*. Эти факторы во все большей мере создают проблемы с точки зрения оперативности решения вопросов, связанных с киберпреступностью. При рассмотрении дел транснационального характера требуется быстрый доступ к данным. Вместе с тем необходимость использования официальных каналов оказания взаимной правовой помощи и гарантий соблюдения принципа верховенства права во всех заинтересованных государствах существенно увеличивает время, требуемое для получения данных;

f) *растущая распространенность технологий и увеличение числа проблем, создаваемых этими технологиями почти во всех областях жизни*. Широкое распространение технологий оказывает воздействие на всех уровнях – от самой маленькой деревни до самого высокого уровня глобальных стратегических и международных отношений как в государственном, так и в частном секторе. Эксперты рассказали о работе правительств своих стран и усилиях, предпринимаемых на региональном и субрегиональном уровнях. Они также приветствовали принятие ответных глобальных мер, а также подчеркнули их необходимость и потребность в участии Организации Объединенных Наций в разработке и координации таких мер.

7. В отношении противодействия киберпреступности были затронуты два общих вопроса:

a) *необходимость надежных и всеобъемлющих глобальных данных о характере и масштабах проблемы*. Этот вопрос был отражен в мандате на проведение исследования и согласованных материалах по основным темам и методологии исследования, утвержденных на первом совещании Группы экспертов. К числу серьезных трудностей в этой области относятся очень широкий охват проблемы, большое количество источников информации, подлежащих рассмотрению, необходимость постоянного обновления и анализа данных для отражения их динамичного развития;

b) *вопрос о правовых или иных механизмах регулирования и координации международного противодействия киберпреступности*. Были высказаны разные мнения. Одни эксперты указывали на необходимость нового и всеобъемлющего универсального международно-правового документа по киберпреступности для нахождения глобального консенсуса в отношении эффективных ответных мер и обеспечения четкой международно-правовой основы для их применения. Другие эксперты утверждали, что более эффективным средством будет использование существующих внутренних и международных правовых режимов и более специализированных подходов к сотрудничеству и оказанию технической помощи в каждом конкретном случае.

8. В отношении значения термина «киберпреступность» ряд экспертов подчеркнули, что единое юридическое определение не представляется возможным. Вместе с тем было достигнуто общее согласие в отношении необходимости описательного или типологического подхода в качестве основы для рассматриваемого исследования и других исследовательских работ и основы для эффективного международного сотрудничества. Большинство экспертов согласились с тем, что типология, разработанная в 1990-х годах и отраженная в Конвенции Совета Европы о киберпреступности, является хорошим отправным пунктом независимо от того, поддерживают ли они саму Конвенцию в качестве эффективного правового документа. Эта типология включает рассмотрение новых видов преступлений, совершение которых возможно только с помощью новых технологий; использование технологий для совершения известных ранее или аналогичных преступлений, иногда с применением новых методов; и тот факт, что технологии также часто используются организованными преступными группами, террористическими группами или другими лицами для облегчения совершения преступлений, недопущения обнаружения или сокрытия улик или доходов от преступлений.

9. Ряд экспертов отметили, что потенциал использования технологий для совершения уже известных преступлений является весьма широким, в силу чего составление какого-либо перечня преступлений не представляется возможным ни в исследовании, ни в других прикладных программах. Вместе с тем было также отмечено, что с течением времени перечень конкретных преступлений фактически сформировался в тех областях, в которых был достигнут консенсус в отношении того, что новые формы преступлений, связанных с использованием технологий, представляют собой серьезную или особую проблему и могут потребовать международного сотрудничества и скоординированных международных мер реагирования. В этой связи самыми часто приводимыми примерами были создание и распространение детской порнографии и новые или расширенные виды мошенничества с использованием средств массовых коммуникаций.

10. Был также указан ряд стратегических или политических проблем, препятствующих возможному достижению консенсуса в отношении сферы охвата киберпреступности как глобальной проблемы. Одной из таких проблем является растущая зависимость государств-членов от технологий и сетей как формы важнейшей инфраструктуры и, как следствие, возникновение киберпреступности и других угроз как проблемы национальной безопасности или кибербезопасности. Было отмечено, что вопросы киберпреступности и кибербезопасности неизбежно взаимосвязаны друг с другом. Еще одной упомянутой проблемой был тот факт, что, несмотря на отсутствие международного консенсуса в

отношении точного определения или сферы охвата термина «терроризм», весьма очевидным является то, что террористические организации могут использовать и действительно используют технологии и сети. Этот факт создает проблемы в отношении как сферы охвата исследования, так и усилий, направленных на предупреждение и пресечение киберпреступности и терроризма в целом. Большинство экспертов согласились с тем, что проблемы, связанные с кибербезопасностью и терроризмом, существуют и требуют ответных мер, хотя мнения разошлись по вопросу о том, будет ли целесообразна или осуществима разработка мер противодействия этим угрозам в рамках мандата и работы Группы экспертов.

11. Были также рассмотрены проблемы, касающиеся измерения и оценки темпов роста киберпреступности и тенденций в этой области. Было достигнуто согласие с необходимостью наличия точной национальной и глобальной информации для использования фактологической базы для будущей деятельности как в исследовании, так и в более общем плане, а также был затронут ряд конкретных проблем. Несколько экспертов отметили, что после сбора статистической информации обычно составляются отчеты и возбуждается уголовное преследование на основе правовых определений преступлений. Было отмечено, что это не касается ситуаций, в которых использование технологий является фактическим элементом, а не требованием закона, а также дел, которые не были успешно расследованы или не привели к уголовному преследованию и которые необязательно отражают разные подходы государств-членов к вопросам криминализации. Было также отмечено, что серьезную проблему представляют собой «темные» или незарегистрированные преступления, поскольку многие случаи киберпреступлений никогда не выявляются и в некоторых случаях потерпевшие не сообщают о них. Важным источником информации в этой области являются, как было признано, поставщики услуг и другие субъекты частного сектора, поскольку сообщение о преступлениях иногда получают они, а не государственные органы, и поскольку наличие или распространенность некоторых видов преступлений можно оценить при помощи технических средств. Был также затронут вопрос об отсутствии статистического потенциала и соответствующей структуры в развивающихся странах с точки зрения как наличия проблемы, так и возможного направления усилий в области оказания помощи в целях развития и технического содействия. Было также отмечено, что быстрое распространение технологий, которые преобразуют многие виды деятельности в области управления и социально-экономического развития, создает более широкие трудности для оценки издержек и общей серьезности проблемы, а также для статистических сопоставлений во временной перспективе.

B. Меры по противодействию киберпреступности, принимаемые государствами-членами, международным сообществом и частным сектором, и возможные пути укрепления существующих и выработки предложений в отношении новых национальных и международных правовых и других мер по противодействию киберпреступности (пункты 3 и 4 повестки дня)

12. В отношении существующих внутренних правовых и иных мер противодействия многие эксперты представили краткую информацию о законодательных мерах в их странах, некоторые из которых принимаются на протяжении нескольких десятилетий по мере расширения масштабов киберпреступности и появления ее новых форм. Большинство экспертов отметили, что их страны признают серьезность проблемы и что для борьбы с ней принимаются законодательные и иные ответные меры. Были упомянуты различные подходы, однако было отмечено, что эти подходы в целом отражают определенное сочетание изменения или актуализации существующих положений о криминализации в соответствии с национальным законодательством и следственными полномо-

чиями и принятия, в необходимых случаях, абсолютно новых положений. Большинство экспертов согласились с тем, что существует необходимость защищать неприкосновенность компьютерных сетей и их пользователей от новых и конкретных преступных угроз, таких как вредоносные программы, ботнеты и получение доступа к сохраненным данным или находящимся в процессе передачи сообщениям, таким образом, который нарушает частный характер данных или национальный суверенитет. Было также достигнуто согласие в отношении необходимости установления или актуализации состава преступлений для обеспечения решения таких конкретных проблем, как мошенничество или жестокое обращение с детьми. В числе неоднократно затронутых вопросов в отношении законодательных мер противодействия были вопросы о том, следует ли уделять основное внимание внесению изменений в существовавшие ранее преступления и полномочия или использованию совершенно новых подходов, а также необходимости разработки «технически нейтральных» проектов законодательных положений, с тем чтобы они не устарели или не стали неприменимыми по мере развития технологий.

13. Многие эксперты отметили, что необходима определенная степень согласования или использования общих подходов к криминализации для обеспечения основы для международного сотрудничества, хотя некоторые эксперты указали также на то, что достижение консенсуса по каждому возможному преступлению необязательно, и подчеркнули необходимость уважения национального суверенитета и культурного разнообразия. Были высказаны разные мнения по вопросу о том, является ли наилучшим подходом к согласованию и международному сотрудничеству открытая разработка нового международно-правового документа, использование Конвенции Совета Европы о киберпреступности в качестве правовой базы или «мягких правовых» руководящих принципов, использование других существующих документов или руководящих принципов или более специализированного подхода к сотрудничеству, обмену информацией и технической помощи в каждом конкретном случае. Вместе с тем ряд экспертов отметили, что существуют границы согласования, поскольку во многих государствах уже приняты свои законы, и что будет необходимо обмениваться информацией, с тем чтобы каждое государство могло выбрать самый подходящий для себя подход.

14. Несколько экспертов указали на то, что согласование уголовных преступлений и законов о расследованиях будет также в определенной степени связано с теми законами о правах человека, которые затрагивают доступ к технологиям и сетям и их использование и состав преступлений, и теми законами, которые относятся к другим областям, таким как применение разных подходов к регулированию использования технологий в некриминальных целях, поставщики услуг и установление технических стандартов. Например, было отмечено, что некоторые формы онлайнового контента считаются уголовными преступлениями в одних правовых системах, тогда как в других на них по закону распространяется защита свободы информации или свободы выражения мнений. Некоторые эксперты указали на расхождения в определении общих преступлений или конкретных киберпреступлений, такие как различия в возрасте потерпевших, который используется в качестве основания для признания преступлений в отношении детей. В качестве проблемы для законодателей и следователей были также названы различия между фактическим совершением преступлений и введением понятия «распределенные преступления», когда сложные преступления совершаются группой лиц, находящихся в разных местах.

15. Ряд экспертов кратко информировали о своих национальных законодательных схемах, касающихся расследования киберпреступлений. В большинстве случаев следственные полномочия включают общие полномочия, регулирующие такие методы, как обыск и изъятие, перехват сообщений, правила и практика судебной экспертизы и сбор доказательств. Были также упомянуты более специальные положения или варианты, разработанные специально для решения проблем в области расследования киберпреступлений. К числу таких

проблем и мер относятся юридические обязанности поставщиков услуг сохранять данные и оказывать помощь следователям в извлечении и получении соответствующих данных из сложных систем и ускоренные следственные полномочия с учетом скорости, с которой могут совершаться преступления и с которой могут переноситься или стираться цифровые доказательства, если преступникам станет известно о проведении расследования. Было отмечено, что ряд существовавших ранее следственных методов был приспособлен для использования при определении местонахождения, изъятия и сохранения цифровых доказательств в устройствах и сетях. Ряд экспертов указали также на проблему, связанную с недопущением отставания от постоянного развития технологий и методов, которые используют преступники, с тем чтобы избежать обнаружения или контроля, а также на необходимость новых следственных полномочий и методов. В этой связи было отмечено, что некоторые формы вредоносных программ могут использоваться правоохранительными органами так же, как это делают преступники, но что такие случаи, в зависимости от обстоятельств, могут вызывать серьезную обеспокоенность в отношении обеспечения верховенства права, прав человека или юрисдикционных требований.

16. Хотя сфера охвата исследования и мандат Группы экспертов нацелены на рассмотрение внутренних и международных мер противодействия киберпреступности в рамках уголовного законодательства или систем уголовного правосудия, ряд экспертов отметили, что не связанные с уголовной ответственностью разделы законодательства имеют важнейшее значение для понимания внутренних мер решения этой проблемы и достижения международного консенсуса в отношении того, каким образом следует реагировать на нее. Одним из таких указанных разделов являются национальные и международные системы защиты прав человека, которые, по мнению некоторых экспертов, оказывают прямое воздействие на масштабы криминализации и на внутренние и транснациональные следственные полномочия и практику. В этой связи было подчеркнуто, что готовность и правовая способность многих государств сотрудничать будут зависеть от наличия взаимоприемлемых гарантий, обеспечивающих соблюдение принципов верховенства права и прав человека. Был также затронут вопрос о том, в какой степени более общие или упреждающие меры по обеспечению прав человека, такие как законы или стандарты в области защиты данных, являются важным фактором. Эксперты также отметили целый ряд внутренних неуголовных законов, которые применяются к различным видам деятельности частного сектора или физических лиц, затрагивающих как инфраструктуру, в которой киберпреступность имеет место, так и способность или обязанность компаний сотрудничать в деле предупреждения и проведения расследований. В качестве общих примеров были приведены законы или технические стандарты, касающиеся неприкосновенности частной жизни и защиты данных, юридической обязанности сообщать о преступлениях или сотрудничать различным образом с правоохранительными органами, и юридические обязанности или добровольная практика в такой области, как шифрование и техническая защищенность.

17. В отношении предложенных или возможных будущих внутренних правовых или иных мер реагирования было выражено общее согласие с тем, что в этой области были достигнуты существенные успехи, сначала в нескольких развитых государствах-членах в 1980-х и 1990-х годах, затем и во многих других государствах. Большинство экспертов рассказали о законодательных и других усилиях, предпринимаемых в последние годы, при этом многие из них отметили активизацию национальных усилий по наращиванию потенциала, с тем чтобы быть в курсе новых технических достижений. Была подчеркнута важность объединения усилий, направленных на предупреждение киберпреступности и борьбу с ней, в таких не предусматривающих уголовной ответственности областях, как управление, развитие торговли и национальные стратегии развития. Кроме того, было достигнуто общее согласие в отношении необходимости оказания помощи в целях развития и технического содействия для обеспечения того, чтобы киберпреступность не способствовала «цифровому

разрыву» между государствами-членами и не стала препятствием на пути развития. Было также достигнуто общее согласие с тем, что усилия по борьбе с киберпреступностью в странах с развитой правовой и правоохранительной системой не должны переносить решения этой транснациональной глобальной проблемы в страны с менее развитыми возможностями. Ряд экспертов представили информацию о текущих национальных и региональных усилиях по оказанию технической помощи. Национальные эксперты и представители частного сектора также подчеркнули, что такое предупреждение преступности и наращивание потенциала являются той областью, в которой частный сектор намерен и может внести существенный вклад.

18. В отношении существующих и предлагаемых или возможных международных правовых мер реагирования был высказан целый ряд мнений и было подчеркнуто наличие некоторых серьезных различий в возможных подходах. Мнения разошлись в отношении криминализации конкретных форм поведения и следственных полномочий или методов, при этом многие эксперты отметили, что в качестве основы как для международного сотрудничества, так и технической помощи необходимо, насколько это возможно, обеспечить согласование законов и общих подходов. Было отмечено, что киберпреступность создает аналогичные проблемы во всем мире и что существует общая заинтересованность в обмене юридическим опытом и выявлении и восполнении пробелов в области криминализации или правоохранительной деятельности, которыми могут воспользоваться преступники.

19. Ряд экспертов и несколько организаций высказали замечания в отношении нынешней и возможной роли международных организаций. Было отмечено, что несколько региональных и субрегиональных организаций занимаются разработкой и поддержкой правовых основ и стандартов, включая Конвенцию Совета Европы о киберпреступности, Соглашение о сотрудничестве между государствами – членами Содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации (2001 год), Соглашение о сотрудничестве в области обеспечения международной информационной безопасности и соответствующие стандарты и правила Европейского союза. Был также отмечен целый ряд мероприятий в области исследований, развития технической помощи или наращивания потенциала. Была отмечена необходимость координации мандатов и деятельности субъектов и деятельности, нацеленной на борьбу с киберпреступностью и связанные с ней области, включая права человека, коммерческие и другие не связанные с уголовной ответственностью разделы публичного и частного международного права и регулирования развития технологий. Многие эксперты приветствовали инициативы региональных организаций, однако некоторые из них подчеркнули тот факт, что глобальный характер компьютерных сетей и киберпреступности настоятельно требует участия Организации Объединенных Наций, в частности Комиссии по предупреждению преступности и уголовному правосудию и Управления Организации Объединенных Наций по наркотикам и преступности. Ряд экспертов приветствовали настоящее исследование как первое крупное мероприятие, посвященное этой теме и проводимое под эгидой Комиссии, в то время как другие обратили внимание на имевшие место в прошлом обсуждения проблемы киберпреступности или компьютерной преступности Комиссией, Генеральной Ассамблеей и другими органами[1]. Несколько экспертов упомянули о Руководстве Ор-

[1] См. резолюцию 1999/23 Экономического и Социального Совета под названием «Работа Программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия», E/CN.15/2001/4 и E/CN.15/2002/8; *Доклад Международного комитета по контролю над наркотиками за 2001 год* (издание Организации Объединенных Наций, в продаже под № R.02.XI.1), пункты 5-83; резолюции Генеральной Ассамблеи 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года; *восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Гавана, 27 августа – 7 сентября 1990 года: доклад, подготовленный Секретариатом* (издание Организации Объединенных Наций, в продаже под № 91.IV.2), глава I, раздел C, *десятый Конгресс Организации Объединенных Наций*

ганизации Объединенных Наций по предупреждению преступности, связанной с применением компьютеров, и борьбе с ней, которое было разработано в 1994 году, и высказали мнение, что его можно обновить и переиздать[2].

20. В отношении возможной разработки нового международно-правового документа или конвенции по киберпреступности одни эксперты не высказали никакого мнения, а другие обменялись целым рядом разных мнений в отношении наилучшего подхода. Было отмечено, что этот вопрос был в центре политических обсуждений, которые привели к последующему компромиссу на двенадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Результаты этих обсуждений, содержащиеся в Салвадорской декларации, стали основой мандата самой Группы экспертов. В этой связи ряд экспертов высказали обеспокоенность тем, что уделение особого внимания характеру возможной правовой основы международных действий против киберпреступности может привести к тому, что государства-члены или эксперты будут игнорировать или недооценивать трудности решения многих конкретных проблем, которые может повлечь за собой подобный подход, будь то в контексте правового инструмента или нет. Было также подчеркнуто, что в Салвадорской декларации содержится призыв провести исследование с целью изучения возможных путей укрепления существующих мер и предложения новых. К числу этих мер относятся правовые и иные меры по противодействию киберпреступности как на национальном, так и международном уровне, при этом было отмечено, что для тщательного изучения всех возможных мер реагирования необходим сбалансированный подход.

21. В отношении настоящего исследования некоторые эксперты высказали мнение, что в процессуальном и методологическом плане оно должно включать рассмотрение как практической осуществимости, так и целесообразности такого документа и его возможного содержания или элементов. Другие эксперты сочли, что цель первой части исследования должна заключаться в сборе и представлении фактических данных и что рассмотрение правовых мер реагирования будет проводиться Группой экспертов, Комиссией и другими политическими органами после сбора таких данных. Было достигнуто общее согласие с тем, что возможное рассмотрение этого вопроса должно быть проведено самой Группой экспертов и что в исследовании следует изучить все варианты эффективной правовой базы, включая универсальную международную базу и другие меры по борьбе с киберпреступностью (см. E/CN.15/2011/19, приложение I, пункт 33 (b)). В этой связи было также проведено обсуждение вопроса о том, подразумевают ли ссылки на «международно-правовой документ» документы универсального характера или также включают документы, разработанные или открытые для ратификации или присоединения только на региональной или неуниверсальной основе. Ряд экспертов отметили, что документы, не имеющие универсального характера, которые были согласованы между двумя или более государствами-членами, такие как Конвенция Совета Европы по киберпреступности, все же являются международно-правовыми документами, в то время как другие эксперты высказали мнение, что этот термин относится только к документам универсального характера.

по предупреждению преступности и обращению с правонарушителями, Вена, 10-17 апреля 2000 года: доклад, подготовленный Секретариатом (издание Организации Объединенных Наций, в продаже под № R.00.IV.8), пункты 161-174 и *одиннадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Бангкок, 18-25 апреля 2005 года: доклад, подготовленный Секретариатом* (издание Организации Объединенных Наций, в продаже под № R.05.IV.7), пункты 323-340.

[2] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5). Эксперты отметили, что обновление и переиздание этого Руководства были ранее рекомендованы в исследовании проблемы киберпреступности 2000-2001 годов и в исследовании случаев экономического мошенничества и преступлений, связанных с использованием личных данных. См. E/CN.15/2001/4, пункт 52 (a)(i) и E/CN.15/2007/8, пункт 37 (g).

22. Что касается существа вопроса, то некоторые эксперты высказали мнение, что специальные механизмы или правовые документы, разработанные на региональной основе, в частности Конвенция Совета Европы о киберпреступности, не предусматривают достаточных мер реагирования и что необходим правовой документ, разработанный в рамках открытого процесса и открытый для всеобщей ратификации или присоединения под эгидой Организации Объединенных Наций. Они отметили, что глобальный характер информационно-коммуникационных технологий и киберпреступности настоятельно требует разработки универсального правового документа, и указали на то, что такие процессы и инструменты не являются новым подходом к борьбе с транснациональными формами преступности. Эти эксперты также подчеркнули важность достижения исходного консенсуса в отношении мер противодействия киберпреступности в качестве основы для разработки такого документа и важность Организации Объединенных Наций как единственного форума, в рамках которого могут эффективно решаться соответствующие вопросы. Был также затронут ряд других конкретных проблем, включая необходимость проведения открытых переговоров и достижения консенсуса, нежелание некоторых государств-членов присоединиться к Конвенции Совета Европы о киберпреступности, поскольку они не участвовали в согласовании этого документа, и неспособность некоторых государств-членов присоединиться к этой Конвенции по политическим причинам или в силу наличия практических проблем, связанных с конкретными положениями самой Конвенции. Одна из таких проблем связана с положениями Конвенции, которая допускает определенные формы прямого трансграничного расследования и, в частности, возможность прямого доступа к данным на основе согласия частных сторон, владеющих или распоряжающихся этими данными, без обязательного уведомления или получения согласия государства, на территории которого эти данные физически находятся. Эти эксперты также указали на проблемы, связанные с общей правовой или правозащитной базой и различиями в политических подходах, правовых традициях или культуре в отношении элементов криминализации. Некоторые из экспертов, выступавших за открытую разработку международно-правового документа, также высказали мнение, что Конвенция Европейского союза о киберпреступности уже устарела и не затрагивает другие вопросы, которые, по их мнению, должны быть рассмотрены или включены.

23. Другие эксперты отметили, что разработка нового международно-правового документа на открытой основе практически неосуществима, учитывая неотложный характер этой проблемы, и масштабы некоторых проблем, которые должны быть решены на основе консенсуса. Они отметили, что этот вопрос был затронут на двенадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и в ходе предыдущих мероприятий, и высказали мнение, что позиции по целому ряду вопросов национального суверенитета и внутреннего законодательства являются настолько разными, что это не позволяет разработать полезный и эффективный документ в течение разумного срока. Они выразили надежду на то, что исследование будет способствовать уточнению схожих черт и различий подхода в национальном законодательстве и той степени, в какой может быть достигнут консенсус. По их мнению, более эффективный подход заключается в том, чтобы сосредоточить внимание на более неотложных потребностях в технической помощи и разработке неофициальных механизмов сотрудничества, которые позволят ускорить расследование. Они отметили, что, хотя суверенитет, юрисдикция и права человека могут быть важными факторами, эти проблемы, возможно, необязательно решать. Они также высказали мнение, что основной проблемой, с которой сталкиваются правоохранительные органы, является отсутствие национального потенциала и приемлемых неофициальных каналов и что основным содержанием будущей работы должно быть решение этой проблемы. Эти эксперты также отметили, что сложность киберпреступности и скорость, с которой могут совершаться преступления, требуют использования гибких подходов в каждом конкретном случае, особенно в том, что каса-

ется методов расследования, которые разрешены в одних правовых системах, но не разрешены в других. В этой связи они сочли важным укреплять взаимное доверие между правоохранительными органами при помощи таких имеющихся средств, как круглосуточно работающие сети. Они также высказали обеспокоенность в связи с тем, что возможные попытки разработки нового всеобъемлющего международно-правового документа по киберпреступности может потребовать значительного времени без достижения гарантированного успеха. На этой основе они согласились с тем, что в той мере, в какой такая международная правовая база необходима, наилучшим вариантом будет использование Конвенции Совета Европы о киберпреступности, которая была разработана в контексте Совета Европы, но также открыта для присоединения других государств. Ряд экспертов отметили также, что Конвенция Совета Европы о киберпреступности является также полезной в качестве «мягкого варианта» правового регулирования, который может служить для государств-членов базисным руководством в отношении положений о криминализации, следственных полномочиях или электронных доказательствах или других законов, даже если эти государства не хотят или не могут присоединиться к ней и полностью выполнять ее положения.

24. В целом обсуждение возможного универсального и всеобъемлющего международно-правового документа было посвящено желательности или целесообразности его разработки, а не его возможному содержанию или конкретным вопросам, которые могут быть затронуты в ходе согласования. Ряд экспертов отметили, что, по их мнению, последний момент является важным элементом исследования, в рамках которого будут определены вопросы и проблемы и предложены подходы к их решению. Один из экспертов затронул более конкретные подробности, высказав мнение, что основную форму Конвенции Организации Объединенных Наций против коррупции можно использовать для решения таких вопросов, как криминализация, предупреждение, техническая помощь, международное сотрудничество и защита национального суверенитета. Другой эксперт отметил, что, хотя глобальное обсуждение вопросов терроризма может быть сопряжено с большими трудностями, существует по крайней мере определенная возможность рассмотреть целесообразность распространения действия такого документа на конкретные террористические преступления или другие связанные с терроризмом преступления и что использование технологий террористическими группами может регулироваться положениями, касающимися киберпреступности в целом.

25. В этой связи была также упомянута Конвенция об организованной преступности. Некоторые эксперты высказали мнение, что эта Конвенция является полезным инструментом, принимая во внимание тот факт, что большинство государств-членов ратифицировали ее или присоединились к ней. Кроме того, значительная часть киберпреступлений, как представляется, носит «транснациональный характер» и совершается при участии «организованной преступной группы», что означает выполнение требований статьи 3 для применения Конвенции. Другие эксперты отметили, что она не распространяется на случаи, связанные с киберпреступностью, когда участие организованных преступных групп отсутствует, и что она не в полной мере касается особых видов международного сотрудничества, которое может быть необходимо при расследовании дел, связанных с киберпреступностью. Было также отмечено отсутствие определенности в отношении серьезности некоторых форм киберпреступности и в отношении того, отвечают ли эти формы пороговому требованию «серьезности преступления» для применения этой Конвенции, как это определено в ее статье 2 (b). Целый ряд различных мнений был также высказан в отношении применения и полезности антитеррористических документов в тех случаях, когда террористы либо осуществляют атаки на технические средства или сети или используют их для других целей.

26. Был также затронут ряд конкретных проблем, касающихся существующих или возможных будущих правовых механизмов международного сотрудниче-

ства, включая необходимость поиска эффективных решений некоторых общих проблем, изложенных в пункте 7 настоящего доклада. В отношении международного сотрудничества в целом был высказан ряд мнений в отношении того, каким образом можно осуществлять такое сотрудничество на своевременной основе в соответствии с существующими международными и региональными правовыми документами, такими как Конвенция об организованной преступности и Конвенция Совета Европы о киберпреступности, и по различным двусторонним или неофициальным каналам. Ряд экспертов высказали обеспокоенность по поводу необходимости достижения консенсуса в отношении криминалистических стандартов, касающихся сбора, сохранения, передачи, аутентификации и использования цифровых данных в качестве доказательства в рамках уголовных или иных юридических процедур. Некоторые эксперты отметили также, что различия в национальных законах, касающихся допустимости таких методов, как перехват сообщений и внедрение в преступные группы или маскировка под преступников либо организация засад на них, могут вызывать обеспокоенность в тех случаях, когда при проведении расследований в режиме реального времени задействованы или затронуты другие юрисдикции. Другие эксперты отметили также, что во внутреннем законодательстве могут иметь место различия в отношении требований обеспечения прав человека, указав в качестве примера различия в положениях о неприкосновенности частной жизни, которые применяются к данным, используемым для направления и отслеживания сообщений, и фактическому содержанию этих сообщений.

27. В отношении процедур транснациональных расследований ряд экспертов, особенно те из них, которые имеют опыт работы в правоохранительных органах, отметили, что, хотя обычные каналы оказания взаимной правовой помощи необходимы при расследовании транснациональных дел, они более не являются достаточными в делах, связанных с киберпреступностью. Они подчеркнули, что скорость, с которой преступники могут теперь совершать киберпреступления и затем стирать или скрывать электронные доказательства, требует наличия намного более оперативных и прямых следственных полномочий и методов. Было достигнуто общее согласие с тем, что вопрос скорости создает серьезную и растущую проблему, хотя многие эксперты подчеркнули также необходимость уважения национального суверенитета, равноправия, независимости и территориальной юрисдикции. Последняя группа экспертов отметила, что, несмотря на возможность повышения эффективности механизмов оказания взаимной правовой помощи, их основная функция заключается в защите суверенитета и предупреждении возможности несоблюдения основных требований обеспечения верховенства права в каждом государстве, включая требования, касающиеся соблюдения прав человека и процедурных гарантий. В этом также заключалось одно из конкретных опасений, высказанных в отношении Конвенции Совета Европы о киберпреступности. Один эксперт отметил, что эта Конвенция заходит слишком далеко, допуская возможность экстерриториального допуска к данным, в то время как другой эксперт выразил надежду на то, что соответствующие положения будут изменены, с тем чтобы пойти еще дальше в этом направлении. Эксперты по вопросам правоохранительной деятельности в целом высказали мнение, что самой серьезной проблемой для расследования транснациональных киберпреступлений и судебного преследования за их совершение является разрыв между краткими сроками расследования и значительно более длительными сроками международного сотрудничества. Ряд экспертов отметили также, что эти проблемы становятся все более серьезными, поскольку такие изменения, как «облачная обработка компьютерных данных», увеличивают число разных юрисдикций, которые могут участвовать в таких процессах, и затрудняют точное определение в краткие сроки физического местонахождения. Эксперты также затронули более общие проблемы, касающиеся необходимости практических формул или понимания того, каким образом ответственность в отношении следственных элементов и элементов возбуждения преследования должна распределяться между различными юрисдикционными заявителями в случаях участия ряда разных государств.

28. Несколько экспертов и представители частного сектора подчеркнули важность предупреждения. Были отмечены как технические средства, такие как использование прикладных программ обеспечения безопасности, предназначенных для защиты неприкосновенности систем и данных, так и социальные средства, такие как подготовка системных пользователей и включение элементов киберпреступности в соответствующие школьные и университетские программы. Эксперты отметили, что весьма широкие масштабы и постоянный характер деятельности, связанной с киберпреступностью, включая рассылку спама и функционирование ботнетов, указывают на важность наличия возможности принимать соответствующие меры, поскольку отдельные преступления постоянно совершаются в отношении новых потерпевших, нередко при помощи автоматически действующих устройств. В качестве важной меры как в области предупреждения преступности, так и в области оперативного расследования была названа способность отслеживать и устранять вредоносные программы. Среди названных соответствующих мер была отмечена возможность создания полномочий и способности блокировать или «удалять» веб-сайты, используемые для совершения преступлений или распространения незаконного контента или вредоносных программ. В связи с этой мерой обсуждались также вопросы уголовного законодательства и прав человека, а также юрисдикционные и технические вопросы. Некоторые эксперты отметили, что такая мера будет связана как с юридическими полномочиями, так и с технической способностью отслеживать и удалять вредоносные программы. Другие эксперты указали на то, что частные операторы инфраструктуры могут играть важную роль как в создании систем, обеспечивающих защиту от вредоносных программ, так и в удалении таких программ. Было также отмечено, что трансграничное сотрудничество между государственным и частным секторами имеет важное значение, поскольку ботнеты имеют транснациональный характер.

29. В контексте Салвадорской декларации и мандата на проведение исследования были рассмотрены важная роль частного сектора и необходимость эффективного сотрудничества между государственным и частным секторами. Ряд экспертов и представителей частного сектора затронули вопросы, касающиеся сотрудничества между государственным и частным секторами. Было отмечено, что широкий охват и развитие деятельности частного сектора в разных технических и нормативных условиях затрудняют возможность определения в юридических целях таких основных терминов, как «поставщик услуг», но что это необязательно создает проблему для развития успешных видов практики в области сотрудничества. Применительно к частному сектору было отмечено, что проблема соблюдения юридических требований разных стран является серьезной проблемой для компаний, занимающихся международной деятельностью. Кроме того, было отмечено, что, хотя правительства, как правило, рассматривают частный сектор как единое целое, он фактически состоит из очень многих субъектов с различными функциями и возможностями, что имеет серьезные последствия в тех случаях, когда существует потребность в различных формах помощи или сотрудничества.

30. Несколько экспертов подчеркнули необходимость выявления успешных усилий и извлечения соответствующих уроков, а также необходимость повышения осведомленности сотрудников правоохранительных органов о том, что частный сектор может или не может сделать. Эксперты отметили, что сотрудничество возможно и желательно в целом ряде конкретных областей, включая предупреждение, сотрудничество при проведении расследований, сбор более общей информации об изменении форм преступлений и криминальных тенденциях и обучение следователей и экспертов-криминалистов новым технологиям по мере их разработки и появления на рынке. Одним конкретным вопросом, затронутым в связи с государственно-частным сотрудничеством при проведении расследований, был вопрос о том, в какой мере применяются правовые гарантии в тех случаях, когда частные компании участвуют в расследованиях. Смежные вопросы включали применение системы судебного надзора и гарантий обеспечения прав человека, защиту национального суверенитета в случае

участия транснациональных компаний или осуществления транснациональных операций и допустимость информации, полученной в качестве доказательства.

31. Ряд экспертов подчеркнули важность технической помощи и обмена информацией как в рамках всеобъемлющего международно-правового документа, так и с учетом более насущных потребностей и средств осуществления. Было отмечено, что этот же вопрос был определен в качестве отдельного и конкретного приоритета в Салвадорской декларации, и несколько экспертов подчеркнули, что техническая помощь крайне необходима и не может быть отложена до завершения текущего исследования. Было также отмечено, что характер этой проблемы требует, чтобы такой обмен информацией носил взаимный характер. Некоторые эксперты указали на то, что техническая помощь в деле борьбы с киберпреступностью также связана с более широкими вопросами, включая стратегии развития и целый ряд конкретных усилий или проектов. Секретариат отметил, что УНП ООН поручено развивать и оказывать техническую помощь и ему требуются только необходимые внебюджетные ресурсы для начала работы. Эксперты, представляющие другие участвующие межправительственные организации, выразили готовность сотрудничать в области оказания технической помощи.

32. Сфера охвата исследования проблемы киберпреступности и будущая работа в этой области неоднократно затрагивались в ходе сессии. В отношении вопросов, касающихся терроризма, в конечном итоге был достигнут консенсус в отношении того, что в исследовании следует избегать таких тем, как проведение широких или открытых расследований случаев терроризма. В той мере, в какой этот вопрос затрагивается, особое внимание следует уделить самой киберпреступности в контексте терроризма (см. E/CN.15/2011/19, пункт 3). Несколько экспертов в более общем плане отметили, что изменения, связанные как с киберпреступностью, так и с терроризмом, создают проблемы и возможность для вероятного взаимодействия в отношении результатов, связанных с действующим мандатом Группы экспертов и самим исследованием. Было отмечено, что, хотя государства могут рассматривать некоторые более серьезные угрозы в качестве проблем киберпреступности со стратегической точки зрения, большинство фактических мероприятий будет проводиться в связи с существующими конкретными или общими преступлениями или в рамках возможной работы по борьбе с киберпреступностью. Аналогичные замечания были сделаны в отношении кибертерроризма. Было отмечено, что смысл термина «кибертерроризм» не совсем ясен и что также отсутствует международный консенсус в отношении сферы охвата термина «терроризм». Вместе с тем этот факт необязательно мешает прогрессу в деле достижения и осуществления консенсуса в отношении конкретных проблем или мероприятий. Было также отмечено, что многие виды деятельности в режиме онлайн, осуществляемые в поддержку террористических групп, будут охвачены более общими преступлениями.

C. Всестороннее исследование проблемы киберпреступности (пункт 5 повестки дня)

33. Договоренность, достигнутая Группой экспертов на ее первой сессии, документально отражена в приложениях к ее докладу по процедурным вопросам Комиссии по предупреждению преступности и уголовному правосудию (см. UNODC/CCPCJ/EG.4/2011/3 и E/CN.15/2011/19). При рассмотрении вариантов этого исследования был отмечен ряд вопросов и подходов. Секретариат представил смету расходов на подготовку документа исследования в объеме 150-200 страниц и проведение дальнейших сессий Группы экспертов. Было также отмечено, что расходы на проведение первых сессий были покрыты за счет регулярного бюджета, хотя дальнейшая работа Группы экспертов и УНП ООН зависит от выделения внебюджетных взносов. Были обсуждены другие варианты, включая использование более мелких и менее дорогостоящих

подгрупп, однако было достигнуто общее согласие с тем, что исследование должно проводиться под контролем самой Группы экспертов для обеспечения надзора за работой и сохранения открытых и межправительственных результатов. Большинство экспертов подчеркнули, что эти вопросы требуют рассмотрения на правительственном уровне и что процесс должен быть открытым для всех государств-членов. Вместе с тем было достигнуто согласие с тем, что каждая региональная группа может назначить до шести правительственных экспертов, с которыми Секретариат может консультироваться по конкретным вопросам и на специальной основе. Была выражена уверенность в беспристрастности Секретариата как основного учреждения, ответственного за проведение исследований и представление соответствующих отчетов, и было подчеркнуто, что возможные результаты будут рассмотрены межправительственной группой экспертов открытого состава до представления Комиссии по предупреждению преступности и уголовному правосудию.

D. Выводы и рекомендации, утверждение доклада и закрытие совещания (пункты 6-8 повестки дня)

34. Как было отмечено выше, Группа экспертов утвердила краткий доклад Секретариата по процедурным вопросам в дополнение к перечню основных тем, которые должны быть охвачены исследованием, и методологии проведения исследования с учетом изменений, внесенных в ходе совещания. Помимо этого никаких конкретных выводов или рекомендаций не было предложено или рассмотрено[3]. Было достигнуто согласие с тем, что доклады о результатах совещаний Бюро Группы экспертов будут подготовлены и распространены региональными группами. Докладчик отметил, что в дополнение к утвержденным основным и методическим текстам будет подготовлен и распространен для утверждения доклад, содержащий резюме хода обсуждений Группы экспертов, как только он будет составлен и распространен на всех шести официальных языках[4].

[3] Дополнительная информация по пунктам 6-8 повестки дня содержится в докладе о работе совещания межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 17-21 января 2011 года (E/CN.15/2011/19).

[4] Как отмечалось в пункте 2 выше, этого не было сделано после первой (2011 год) и второй (2013 год) сессий из-за отсутствия средств.