UNODC/CCPCJ/EG.4/2019/2

Distr.: General
12 April 2019
Russian
Original: English

Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 27–29 марта 2019 года

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 развитие 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. На этом совещании Группа экспертов рассмотрела и утвердила подборку тем для рассмотрения и методологию исследования (E/CN.15/2011/19, приложения I и II).

3. Второе совещание Группы экспертов состоялось в Вене 25–28 февраля 2013 года. На этом совещании Группа экспертов приняла к сведению всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, подготовленное Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) под руководством Группы экспертов во исполнение мандата, предусмотренного в резолюции 65/230 Генеральной Ассамблеи, и в соответствии с подборкой тем для рассмотрения и методологией исследования, утвержденными на первом совещании Группы экспертов. Были высказаны различные мнения относительно содержания, выводов и вариантов, представленных в исследовании (см. UNODC/CCPCJ/EG.4/2013/3).

4. В Дохинской декларации о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности, принятой на тринадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и одобренной Генеральной Ассамблеей в резолюции 70/174, государства-члены отметили деятельность Группы экспертов и предложили Комиссии рассмотреть вопрос о том, чтобы рекомендовать Группе экспертов на основе проводимой ею работы продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления существующих мер и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

5. Третье совещание Группы экспертов состоялось в Вене 10–13 апреля 2017 года. На этом совещании Группа экспертов рассмотрела, в частности, вопрос об утверждении подготовленных Докладчиком кратких докладов о работе первого и второго совещаний Группы экспертов, проект всестороннего исследования проблемы киберпреступности и замечания к нему, а также вопросы дальнейшей работы над проектом исследования. Она также обменялась информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве.

6. В своей резолюции 26/4, принятой на двадцать шестой сессии в мае 2017 года, Комиссия просила Группу экспертов продолжать свою работу и при этом проводить периодические совещания и выступать в качестве платформы для дальнейшего обсуждения вопросов существа, касающихся киберпреступности, внимательно следя за новыми тенденциями, в соответствии с Салвадорской декларацией и Дохинской декларацией. Также в этой резолюции Комиссия просила Группу экспертов продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления существующих мер и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

7. Четвертое совещание Группы экспертов состоялось в Вене 3–5 апреля 2018 года. На этом совещании Группа экспертов основное внимание уделила связанным с киберпреступностью вопросам законодательства, правовой основы и криминализации. Были обсуждены изменения в области законодательства и политики, направленные на борьбу с киберпреступностью на национальном и международном уровнях, и рассмотрены меры по криминализации киберпреступлений на национальном уровне. Кроме того, Группа экспертов утвердила предложение Председателя по плану работы Группы экспертов на период 2018–2021 годов (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. Расширенное бюро на своем заседании 2 ноября 2018 года определило сроки проведения пятого совещания Группы экспертов и согласовало его предварительную повестку дня.

II. Перечень предварительных рекомендаций и выводов

9. В соответствии с планом работы Группы экспертов на период 2018–2021 годов Докладчик подготовит на каждом из совещаний Группы экспертов в 2019 и 2020 годах, при содействии Секретариата и на основе обсуждений и дискуссий Группы экспертов, перечень предварительных выводов и рекомендаций, предложенных государствами-членами, которые должны быть четкими и ориентированными на укрепление практических мер по противодействию киберпреступности. Согласно плану работы этот перечень будет включен в доклад о работе каждого совещания в форме подборки внесенных государствами-членами предложений для дальнейшего обсуждения на обзорном совещании, которое должно состояться не позднее 2021 года. Как указано в плане работы, на этом обзорном совещании Группа экспертов рассмотрит предварительные выводы и рекомендации и составит из них сводный перечень принятых выводов и рекомендаций для представления Комиссии. Перед обзорным совещанием предложенные государствами-членами предварительные выводы и рекомендации будут направлены всем государствам-членам наблюдателям и другим заинтересованным сторонам для представления замечаний, которые затем до начала обзорного совещания будут размещены в Интернете для рассмотрения делегациями.

A. Правоохранительная деятельность и расследования

10. В соответствии с планом работы настоящий пункт содержит подборку предложений, внесенных государствами-членами на заседании по пункту 2 повестки дня под названием «Правоохранительная деятельность и расследования». Настоящие предварительные рекомендации и выводы были представлены государствами-членами, их включение не означает их одобрения Группой экспертов и они перечислены безотносительно степени их важности:

a) некоторые государства-члены высказали мнение, что ввиду динамичного, сложного и транснационального характера киберпреступности было бы преждевременным обсуждать общие стандарты в рамках международного сотрудничества. Поэтому государствам-членам следует продолжать работать над новыми международными мерами противодействия киберпреступности, рассматривая возможность разработки в рамках Организации Объединенных Наций нового глобального правового документа по киберпреступности. Этот документ следует рассматривать, в частности, принимая во внимание озабоченности и интересы всех государств-членов и предлагаемый проект конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности, представленный Генеральному секретарю 11 октября 2017 года (A/C.3/72/12, приложение);

b) в то же время другие государства-члены высказали мнение, что рассмотрение вопроса о новом глобальном правовом документе не является необходимым или целесообразным, поскольку проблемы, связанные с киберпреступностью и достаточной подготовкой следователей, прокуроров и судей, лучше всего решать посредством наращивания потенциала, активного диалога и сотрудничества между правоохранительными органами и использования существующих документов, таких как Конвенция Совета Европы о киберпреступности (Будапештская конвенция). Исходя из этого, государствам-членам следует продолжать действовать согласно и/или присоединиться к существующим многосторонним правовым документам по киберпреступности, таким как Будапештская конвенция, которую многие государства считают наиболее полезным

руководством для разработки соответствующего внутреннего законодательства по борьбе с киберпреступностью, как материально-правового, так и процессуального характера, и содействия международному сотрудничеству в борьбе с такого рода преступностью;

c) ввиду транснационального характера киберпреступности и того факта, что значительное большинство глобальных киберпреступлений совершаются организованными группами, государствам-членам следует также более широко применять Конвенцию Организации Объединенных Наций против транснациональной организованной преступности для содействия обмену информацией и доказательствами в ходе уголовных расследований, касающихся киберпреступности;

d) государствам-членам следует поощрять международное сотрудничество в борьбе с киберпреступностью и участвовать в нем, используя существующие документы, заключая двусторонние соглашения на основе принципа взаимности и поддерживая, в сотрудничестве с УНП ООН, регулярное сетевое взаимодействие и обмен информацией между судебными и правоохранительными органами;

e) странам следует повышать квалификацию сотрудников полиции в сфере расследования киберпреступлений путем предоставления им профессиональной подготовки, которую предлагают многие страны, а также УНП ООН и другие партнеры и которая имеет целью укрепление потенциала в области выявления и расследования киберпреступлений и борьбы с киберпреступностью. Деятельность по наращиванию потенциала в этой области должна, в частности, учитывать потребности развивающихся стран, уделять особое внимание уязвимостям каждой страны с целью оказания адресной технической помощи и содействовать обмену самыми современными знаниями, максимально соблюдая интересы получателей такой помощи;

f) государствам рекомендуется продолжать предоставлять УНП ООН необходимые мандаты и финансовую поддержку для получения ощутимых результатов при осуществлении проектов по наращиванию потенциала в этой области;

g) странам следует выделять средства на подготовку специалистов по расследованию киберпреступлений и на создание партнерств, использующих механизмы сотрудничества для получения важных доказательств;

h) государствам-членам следует и далее прилагать усилия по созданию и поддержке в правоохранительных, прокурорских и судебных органах специализированных подразделений, органов и структур по борьбе с киберпреступностью, с тем чтобы у них были необходимые знания и оборудование для решения проблем, связанных с киберпреступностью, и для сбора и использования электронных доказательств и обмена ими в уголовном производстве;

i) учитывая, что для ликвидации рынков киберпреступности требуются среднесрочные и долгосрочные стратегии правоохранительной деятельности, включая сотрудничество с международными партнерами, эти стратегии должны быть упреждающими и преимущественно ориентированными на борьбу с организованными киберпреступными группами, члены которых могут находиться во многих странах;

j) странам следует продолжать вводить нормы материального права в отношении новых и возникающих форм преступности в киберпространстве, используя технологически нейтральные формулировки, чтобы обеспечить их

соответствие будущему развитию событий в области информационно-коммуникационных технологий;

k) развитие внутреннего процессуального права должно идти в ногу с развитием технологий и обеспечивать правоохранительным органам надлежащую оснащенность для борьбы с интернет-преступностью. Соответствующие законы следует разрабатывать с учетом применимых технических концепций и практических потребностей следователей, занимающихся расследованием киберпреступлений, при условии обеспечения соблюдения надлежащей правовой процедуры, неприкосновенности частной жизни, гражданских свобод и прав человека, а также принципов соразмерности и субсидиарности и гарантий, обеспечивающих судебный надзор. Кроме того, государствам-членам следует выделить ресурсы на принятие внутреннего законодательства, которое признает законными:

i) просьбы об оперативном обеспечении сохранности компьютерных данных, направляемые лицу, осуществляющему контроль над этими данными, то есть поставщикам интернет-услуг и услуг связи, с целью сохранения и обеспечения целостности этих данных в течение определенного периода времени в связи с их потенциальной неустойчивостью;

ii) поиск и выемку хранимых данных с цифровых устройств, которые часто являются наиболее актуальными доказательствами совершения электронного преступления;

iii) распоряжения о предоставлении информации в электронной форме, которая может иметь меньшую степень защиты неприкосновенности частной жизни, такой как технические параметры трафика и абонентские данные;

iv) сбор технических параметров трафика и контента в режиме реального времени в соответствующих случаях;

v) международное сотрудничество между национальными правоохранительными органами;

l) поскольку расследование киберпреступности требует творческого подхода, технической проницательности и совместных усилий прокуратуры и полиции, странам следует поощрять тесное сотрудничество прокуратуры и полиции на раннем этапе расследования в целях получения достаточных доказательств для предъявления обвинений выявленным субъектам;

m) при проведении расследований по делам о киберпреступлениях сотрудникам правоохранительных органов надлежит руководствоваться рекомендациями следователей для обеспечения соблюдения надлежащих процессуальных норм;

n) национальным правоохранительным органам следует устанавливать контакты и взаимодействовать с национальными провайдерами интернет-услуг и другими частными отраслевыми группами. Такая информационная работа способствует проведению расследований правоохранительными органами, укрепляя доверие и сотрудничество между заинтересованными сторонами;

o) странам следует руководствоваться гибкими подходами к применимым юрисдикционным основам в области борьбы с киберпреступностью, в том числе в большей степени учитывать место предоставления услуг в сфере информационно-коммуникационных технологий, а не место нахождения данных;

p) странам следует инвестировать в повышение осведомленности широкой общественности и частного сектора о киберпреступности с целью

исправления ситуации, характеризуемой меньшим числом заявлений о киберпреступлениях по сравнению с другими видами преступлений;

q) государствам-членам следует развивать механизмы публично-частного партнерства в борьбе с киберпреступностью, в том числе посредством принятия законодательства и создания каналов для диалога с этой целью, с тем чтобы содействовать сотрудничеству между правоохранительными органами, поставщиками услуг связи и научными кругами в целях углубления знаний и повышения эффективности мер по противодействию киберпреступности;

r) государствам следует принять меры для поощрения участия поставщиков интернет-услуг в предупреждении киберпреступности и оказании поддержки правоприменительной деятельности и следственным мероприятиям, в том числе путем установления во внутреннем законодательстве соответствующих положений относительно обязательств этих поставщиков услуг, и четко определить сферу и границы таких обязательств с целью защиты законных прав и интересов поставщиков услуг;

s) государствам следует усилить следственную и правоприменительную деятельность в отношении актов пособничества, подстрекательства и подготовки к совершению киберпреступлений, с тем чтобы эффективно противодействовать действиям всей цепочки киберпреступности;

t) государствам следует продолжать работу по укреплению потенциала и расширению возможностей судебных и правоохранительных органов осуществлять расследование и судебное преследование по делам, связанным с киберпреступностью. Особое внимание в работе по наращиванию потенциала следует уделить растущим проблемам, связанным с облачными вычислениями, даркнетом и появлением других технологий. Кроме того, государствам рекомендуется оказывать помощь в укреплении потенциала развивающимся странам.

B. Электронные доказательства и уголовное правосудие

11. В соответствии с планом работы настоящий пункт содержит подборку предложений, внесенных государствами-членами на заседании по пункту 3 повестки дня под названием «Электронные доказательства и уголовное правосудие». Настоящие предварительные рекомендации и выводы были представлены государствами-членами, их включение не означает их одобрения Группой экспертов и они перечислены безотносительно степени их важности:

a) государствам-членам следует разработать и применять юридические полномочия, юрисдикционные и другие процессуальные нормы в целях эффективного расследования киберпреступлений и преступлений, совершаемых с помощью технических средств, на национальном уровне и обеспечения эффективного сотрудничества при расследовании транснациональных дел, принимая во внимание необходимость эффективного обеспечения законности, национального суверенитета и защиты права на частную жизнь и других прав человека. Это может быть:

i) корректировка правил доказывания для обеспечения того, чтобы электронные доказательства можно было собирать, сохранять, аутентифицировать и использовать в уголовном производстве;

ii) принятие положений об отслеживании электронных сообщений на национальном и международном уровнях;

iii) принятие положений, регламентирующих произведение внутренних и международных обысков;

iv) принятие положений о перехвате электронных сообщений, передаваемых с использованием компьютерных сетей и аналогичных средств массовой информации;

v) принятие норм материального и процессуального права, не связанных с конкретными технологиями, чтобы страны могли бороться с новыми и появляющимися формами киберпреступности;

vi) согласование национального законодательства;

vii) принятие нового или усиление действующего законодательства, позволяющего признать допустимость доказательств в электронной форме, а также определить и установить сферу их применения;

b) государствам-членам следует содействовать усилиям по повышению квалификации сотрудников правоохранительных органов, в том числе сотрудников специализированных правоохранительных структур, прокуратуры и судебных органов, с тем чтобы такие сотрудники обладали хотя бы базовыми техническими знаниями относительно электронных доказательств и могли эффективно и оперативно реагировать на просьбы о помощи в отслеживании электронных сообщений и принимать другие меры, необходимые для расследования киберпреступлений;

c) государствам-членам следует содействовать наращиванию потенциала в целях повышения эффективности расследований, улучшения понимания киберпреступности и имеющихся технических средств и технологий для борьбы с нею и создания прокурорам, судьям и центральным национальным органам условий для надлежащего уголовного преследования и вынесения судебных решений по делам, связанным с такими преступлениями;

d) государствам-членам следует содействовать усилиям по наращиванию потенциала центральных органов, участвующих в международном сотрудничестве, применительно к требованиям и процедурам, касающимся взаимной правовой помощи, в том числе путем организации обучения составлению обстоятельных запросов, содержащих достаточную информацию, для получения электронных доказательств;

e) государствам-членам следует рассмотреть подход, предусматривающий использование «группы обвинения», который сочетает компетенции и ресурсы различных учреждений и объединяет прокуроров, служащих следственных органов и экспертов-криминалистов для проведения расследований. Такой подход позволяет прокурорам рассматривать и представлять доказательства в электронной форме;

f) допустимость электронных доказательств не должна зависеть от того, были ли они собраны за пределами юрисдикции страны, при условии, что достоверность доказательств не снижена и что доказательства собраны законно, например на основании договора о взаимной правовой помощи или многостороннего соглашения или в сотрудничестве со страной, обладающей юрисдикцией;

g) государствам-членам следует принять необходимые меры для введения в действие законодательства, обеспечивающего допустимость электронных доказательств, учитывая, что допустимость доказательств, в том числе в электронной форме, является вопросом, который каждая страна должна решать в соответствии с ее внутренним законодательством;

h) государствам-членам следует расширять международное сотрудничество между правоохранительными органами, прокуратурой, судебными органами и поставщиками интернет-услуг с целью устранения разрыва между тем, с какой скоростью орудуют киберпреступники, и быстротой реагирования со стороны правоохранительных органов. При этом государствам-членам следует использовать такие существующие механизмы, как круглосуточные каналы связи и сотрудничество по линии Международной организации уголовной полиции (Интерпол), а также договоры о взаимной правовой помощи, для развития международного сотрудничества с использованием доказательств в электронной форме. Государствам-членам следует продолжать работу по согласованию и рационализации процедур, касающихся взаимной правовой помощи, и разработке общей схемы для ускорения процедуры оперативного сбора и передачи трансграничных доказательств в электронной форме;

i) государствам-членам рекомендуется активнее обмениваться опытом и информацией, в том числе о внутреннем законодательстве, национальных процедурах и передовой практике расследования трансграничных киберпреступлений, а также информацией об организованных преступных группах и используемых ими приемах и методах;

j) государствам-членам следует развивать сеть координаторов между правоохранительными органами, судебными органами и прокуратурой;

k) государствам-членам следует оценить возможность поручения Группе экспертов или экспертам УНП ООН проводить, при участии государств-членов, ежегодную оценку тенденций в области киберпреступности и новых угроз и опубликовывать ее;

l) УНП ООН следует содействовать проведению более широких исследований в целях определения новых форм и моделей правонарушений, последствий нарушения закона в ключевых областях и изменений в сфере телекоммуникаций, включая расширение Интернета вещей, внедрение технологий блокчейн и криптовалют и использование искусственного интеллекта в сочетании с машинным обучением;

m) в рамках Глобальной программы борьбы с киберпреступностью УНП ООН следует поощрять, поддерживать и осуществлять, в соответствующих случаях, проекты технического сотрудничества и технической помощи при условии наличия ресурсов. Благодаря таким проектам выход на экспертов по предупреждению преступности, компьютерной безопасности, законодательству, судебному преследованию, методам расследования и смежным вопросам получат государства, нуждающиеся в информации или помощи в этих областях;

n) УНП ООН следует разработать образовательную программу, направленную на повышение уровня знаний и осведомленности о мерах по борьбе с киберпреступностью, особенно в области сбора доказательств в электронной форме, для судебных органов и органов прокуратуры государств-членов;

o) государствам-членам следует принять меры по расширению сотрудничества в сборе доказательств в электронной форме, включая следующие:

i) обмен информацией об угрозах киберпреступности;

ii) обмен информацией об организованных киберпреступных группах, в том числе об используемых ими приемах и методах;

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

iv) обмен информацией о национальных стратегиях и инициативах по борьбе с киберпреступностью, в том числе о внутреннем законодательстве и порядке привлечения киберпреступников к ответственности;

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

vi) развитие сети координаторов, объединяющей правоохранительные органы, судебные органы и прокуратуру;

vii) согласование и рационализация процедур, касающихся взаимной правовой помощи, и разработка общей схемы для ускорения процедуры оперативного сбора и передачи трансграничных доказательств в электронной форме;

viii) проведение практикумов и семинаров с целью повышения способности правоохранительных и судебных органов составлять запросы, в контексте договоров о взаимной правовой помощи, относительно сбора доказательств по вопросам, касающимся киберпреступлений;

ix) установление стандартов и единообразия в процедурных аспектах сбора и передачи доказательств в цифровой форме;

x) разработка общего подхода к механизмам обмена информацией с поставщиками услуг в связи с расследованием киберпреступлений и сбором доказательств;

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

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

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

xiv) оказание развивающимся странам помощи в укреплении потенциала в области компьютерной криминалистики (форензики), в том числе путем создания лабораторий компьютерной криминалистики;

xv) проведение практикумов и семинаров для повышения осведомленности о передовой практике в области борьбы с киберпреступностью;

xvi) создание международного агентства по проверке и сертификации средств цифровой криминалистики, подготовка руководств и повышение способности правоохранительных и судебных органов противодействовать киберпреступности;

p) странам следует вкладывать средства в создание и укрепление потенциала в области цифровой криминалистики, включая подготовку кадров и сертификацию на соответствие требованиям по информационной 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;

q) в правовых системах, использующих следственную модель, при которой сотрудники судебных органов также являются следователями, работникам органов правосудия следует получить специальную подготовку по вопросам киберпреступности;

r) вследствие того, что некоторые судьи не знакомы с цифровыми доказательствами, к такого рода доказательствам часто применяются более высокие стандарты в отношении аутентификации и допуска. Однако следует учитывать, что никаких практических оснований для установления более высоких стандартов в отношении безупречности цифровых доказательств по сравнению с традиционными доказательствами нет. Вероятность изменения или подделки цифровых доказательств не больше, чем для других доказательств. По сути, изменить или сфабриковать цифровые доказательства, возможно, даже сложнее, поскольку для удостоверения подлинности или предоставления доказательства изменения можно использовать различные математические алгоритмы, например значения хеш-функции;

s) государствам следует повысить эффективность внутренней межведомственной координации и взаимодействия, включая обмен достоверной информацией и оперативными данными, с частным сектором, организациями гражданского общества и другими заинтересованными сторонами в целях содействия эффективному международному сотрудничеству и взаимодействию;

t) государствам следует принять новое или усилить действующее законодательство, чтобы можно было признать допустимость электронных доказательств, а также определить и установить сферу применения электронных доказательств;

u) государства могут рассмотреть вопрос об установлении в своем внутреннем законодательстве того, что в качестве электронных доказательств признаются следующие данные: технические параметры трафика, например файлы регистрации; содержание информации, например электронные письма; сведения об абонентах, например информация о регистрации пользователей; и другие данные, которые хранятся, обрабатываются и передаются в цифровом формате и которые создаются во время совершения преступления и поэтому могут использоваться для подтверждения фактов этого преступления;

v) государствам рекомендуется повышать способность осуществлять сбор электронных доказательств, создавать группы специалистов, обладающих как юридическими, так и техническими знаниями, и расширять сотрудничество в области обмена опытом и профессиональной подготовки в этой области. УНП ООН рекомендуется принимать участие в этих усилиях;

w) государствам рекомендуется предусмотреть в своем внутреннем законодательстве соответствующие методы сбора электронных доказательств, такие как выемка и обеспечение сохранности оригинального носителя, сбор на месте, дистанционный сбор и верификация. Государствам-членам рекомендуется производить фиксацию электронных доказательств для предотвращения добавления, уничтожения или изменения с помощью таких мер, как вычисление контрольной суммы электронного доказательства, блокировка учетных записей вебприложений и установление защиты от записи;

x) государствам рекомендуется установить технические нормы и стандарты для сбора электронных доказательств;

y) государствам следует обеспечить, чтобы сбор электронных доказательств осуществлялся с соблюдением надлежащей процедуры;

z) государствам в своем внутреннем законодательстве следует установить правила оценки подлинности, целостности, законности и актуальности электронных доказательств и учитывать специфику электронных доказательств при применении правил, касающихся первичных доказательств, показаний с чужих слов и исключения доказательств, полученных незаконным путем;

aa) при сборе электронных доказательств за рубежом государствам следует уважать суверенитет государств, в которых находятся данные, соблюдать надлежащую процедуру и уважать законные права соответствующих лиц и организаций. В этой связи государствам следует также воздерживаться от одностороннего применения интрузивных или деструктивных технических методов при производстве следственных действий;

bb) государствам рекомендуется проводить консультации с другими государствами в целях дальнейшего совершенствования международной правовой помощи и сотрудничества в правоприменительной сфере путем оптимизации соответствующих процедур и методов, с тем чтобы облегчить расследование киберпреступлений и сбор электронных доказательств;

cc) государствам следует рассмотреть возможность принятия международных типовых положений о полномочиях следствия, касающихся сбора электронных доказательств, и изучить возможность согласования глобального юридически обязывающего документа по борьбе с киберпреступностью в рамках Организации Объединенных Наций. Этот документ может включать общепринятые положения о трансграничном сборе электронных доказательств.

III. Резюме обсуждения

A. Правоохранительная деятельность и расследования

12. На своих 1, 2 и 3-м заседаниях 27 и 28 марта 2019 года Группа экспертов рассмотрела пункт 2 повестки дня, озаглавленный «Правоохранительная деятельность и расследования».

13. В дискуссии по этому пункту участвовали: г-н Шенкуо Ву (Китай); г-жа Иоана Албани (Румыния); г-н Мартин Гершаник (Аргентина); г-н Педру Верделью (Португалия); и г-н Антон Курдюков (Российская Федерация).

14. В ходе последующего обсуждения Группа экспертов рассмотрела примеры предполагаемых преступных деяний, совершаемых в цифровой среде и создающих значительные трудности для работников системы уголовного правосудия и следователей при возбуждении и проведении расследований и последующего уголовного преследования. К таким примерам относятся мошенничество в Интернете, использование Интернета в террористических целях, использование даркнета для осуществления незаконной деятельности и совершение развратных действий в отношении детей и их сексуальная эксплуатация посредством преступного использования информационно-коммуникационных технологий. Кроме того, Группа экспертов была проинформирована о концептуальной взаимозависимости и о разграничении между киберпреступностью и кибербезопасностью, а также о тенденциях и проблемах, связанных с киберпреступностью, включая атаки с использованием программ-выкупов; тактику социальной инженерии, используемой для совершения мошеннических действий (фишинг, мошенническая рассылка от имени руководства внутри организации, вишинг, смишинг); использование платформы «Cobalt Strike» для проведения атак в отношении банковской системы; Интернет вещей; майнинг криптовалют и взлом шифрования; и скимминг и связанные с этим преступления.

15. Был вновь обсужден вопрос о том, есть ли необходимость во всеобъемлющем глобальном правовом документе по киберпреступности или же государствам следует сосредоточиться на эффективном осуществлении существующих документов, включая Будапештскую конвенцию. Некоторые выступавшие высказали мнение, что в разработке дополнительных правовых документов по киберпреступности нет необходимости, учитывая, что Будапештская конвенция обеспечивает достаточную основу для разработки надлежащих внутренних и международных мер по противодействию киберпреступности. Было отмечено, что к Будапештской конвенции присоединились 63 государства, что свидетельствует о том, что Будапештская конвенция открыта для присоединения государств, не являющихся членами Совета Европы. Кроме того, было отмечено, что Конвенция служит некоторым государствам, не являющимся ее участниками, вдохновляющим примером для согласования внутренних законодательных норм как материально-правового, так и процессуального характера. Было также отмечено, что концепция «согласование национальных норм» включает не только случаи совпадения и общего определения, но и случаи, когда международные нормы являются полезными для разработки национальных правил. Было отмечено, что Будапештская конвенция дополняет другие региональные документы, такие как Конвенция Африканского союза о кибербезопасности и защите персональных данных, принятая в 2014 году, и Международный кодекс поведения в области информационной безопасности, изданный Шанхайской организацией сотрудничества.

16. Однако другие выступавшие высказали мнение, что для решения проблем, связанных с быстрым развитием интернет-технологий, которые не охвачены существующими механизмами, участниками которых к тому же являются не все государства, необходим глобальный правовой документ по киберпреступности, разработанный в рамках Организации Объединенных Наций. Было подчеркнуто, что такой документ предполагается подготовить в рамках возглавляемого Организацией Объединенных Наций процесса, в ходе которого все государства-члены могут взять на себя ответственность за оптимизацию усилий по борьбе с киберпреступностью с учетом или на основе существующих документов, таких как Будапештская конвенция и вышеупомянутая Конвенция Африканского союза. В этой связи были упомянуты резолюция 73/187 Генеральной Ассамблеи от 17 декабря 2018 года о противодействии использованию информационно-коммуникационных технологий в преступных целях и изложенное в ней поручение Генеральному секретарю запросить у государств-членов информацию о трудностях, с которыми они сталкиваются в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, и представить Генеральной Ассамблее доклад, подготовленный на основе этой информации, для рассмотрения на ее семьдесят четвертой сессии. Было также высказано мнение, что Будапештская конвенция является недостаточно прозрачной и инклюзивной, не учитывает обеспокоенность всех государств-членов и устанавливает сложные и непрозрачные процедуры внесения поправок в ее текст, что может быть помехой ввиду постоянно меняющегося характера киберпреступности.

17. Был упомянут текущий переговорный процесс, касающийся принятия второго дополнительного протокола к Будапештской конвенции, с целью установления четких правил и более эффективных процедур по некоторым или всем следующим вопросам: положения о более эффективном и оперативном международном сотрудничестве; положения, допускающие прямое сотрудничество с поставщиками услуг в других правовых системах в отношении просьб о предоставлении информации об абонентах, просьб об обеспечении сохранности данных и срочных просьб; и принципы и надежные гарантии практики, связанной

с трансграничным доступом к информации, включая требования, предъявляемые к защите данных.

18. Было также подчеркнуто, что Конвенция об организованной преступности может быть полезным инструментом для решения проблем, порождаемых киберпреступностью, особенно с учетом транснационального характера этих проблем. Было предложено рассмотреть вопрос о разработке дополнительного протокола к Конвенции об организованной преступности, касающегося конкретно киберпреступности.

19. Делегации и участники дискуссионной группы проинформировали Группу экспертов об успешных национальных усилиях по осуществлению правовых и процессуальных мер по борьбе с киберпреступностью. Для некоторых выступавших Будапештская конвенция и сопутствующие ей проекты по созданию потенциала являются важнейшими составными элементами в этой области. Был обстоятельно рассмотрен вопрос о законодательной реформе на национальном уровне, в том числе вопрос о масштабах такой реформы. Было обращено внимание на необходимость инклюзивных и основанных на широком участии процессов для обеспечения учета мнений различных заинтересованных сторон. Была отмечена необходимость обеспечения правовой определенности и ясности на основе принципа nullum crimen nulla poena sine lege (без закона нет ни преступления, ни наказания) и необходимость использования в новом законодательстве технологически нейтральных формулировок, с тем чтобы такое законодательство неизменно соответствовало быстрому развитию информационно-коммуникационных технологий.

20. Обсуждались также проблемы, возникающие в связи с коллизиями, касающимися территориальной юрисдикции, особенно в тех случаях, когда, например, штаб-квартира поставщика услуг может находиться в одной юрисдикции, а контролер данных находится в другой стране или данные хранятся в другой юрисдикции или в нескольких юрисдикциях. Было также отмечено, что может быть полезным использование гибких подходов к применимым юрисдикционным основам в области борьбы с киберпреступностью, в том числе в большей степени учет места предоставления услуг в области информационно-коммуникационных технологий, а не места нахождения данных.

21. Группа экспертов также подчеркнула необходимость наличия надлежащих процессуальных полномочий для получения электронных доказательств, включая данные и метаданные, для проведения расследований, касающихся не только киберпреступлений, но и других форм преступности. Такие электронные доказательства могут включать сведения об абоненте, данные о содержании контента или технические параметры трафика. Было отмечено, что при расследовании правонарушений, связанных с электронными доказательствами, приходится сталкиваться с такими технологическими новшествами, как программное обеспечение для анонимизации, высококачественное шифрование и использование виртуальных валют, и что следователям, возможно, потребуется принять новые стратегии и рассмотреть вопрос о порядке использования специальных методов расследования и дистанционного применения цифровой криминалистики для сбора таких электронных доказательств при обеспечении допустимости и приемлемости использования таких доказательств в суде. Особое внимание было уделено усилению координирующей роли компетентных национальных органов, таких как генеральная прокуратура или специализированные органы прокуратуры.

22. В ходе обсуждения особое внимание было также уделено вопросу о том, каким образом обеспечить баланс между необходимостью принятия правоохранительными органами эффективных мер реагирования на киберпреступность и

защитой основных прав человека, в частности права на неприкосновенность частной жизни. Правила сохранения данных могут отражать прагматический подход к обеспечению возможности для поставщиков коммуникационных услуг играть более весомую роль в борьбе с киберпреступностью посредством более активного сотрудничества с правоохранительными органами при том условии, что такие законодательные акты осуществляются с соблюдением должных процессуальных гарантий и обеспечением должной защиты личных данных. Был упомянут доклад Управления Верховного комиссара по правам человека о праве на неприкосновенность личной жизни в цифровой век (A/HRC/27/37), который был представлен Совету по правам человека в соответствии с резолюцией 68/167 Генеральной Ассамблеи.

23. Группа экспертов вновь заявила о важности международного сотрудничества в области трансграничного расследования киберпреступлений и уголовного преследования за их совершение. Некоторые выступавшие отметили, что число просьб об оказании взаимной правовой помощи для получения и обеспечения сохранности электронных доказательств быстро растет и что традиционные формы сотрудничества, особенно те, что характеризуются длительными процессами, связанными с взаимной правовой помощью, не способствуют оперативному доступу к данным. Другие выступавшие отметили, что взаимная правовая помощь остается важным инструментом для обмена данными между странами. Некоторые выступавшие также отметили, что ключевыми компонентами для обеспечения своевременного доступа к данным являются наращивание потенциала и обучение выполнению требований, касающихся взаимной правовой помощи, включая составление обстоятельных запросов, содержащих достаточную информацию, для получения электронных доказательств. Кроме того, некоторые страны рекомендовали использовать сети 24/7 для просьб об оперативном обеспечении сохранности данных, учитывая недолговечность таких доказательств, которые можно переслать или уничтожить одним щелчком компьютерной мыши.

24. Различные виды практики были упомянуты в качестве примеров того, как содействовать развитию международного сотрудничества в отношении электронных доказательств, в частности на оперативном уровне. Эти виды практики включают прямую передачу просьб о взаимной правовой помощи между компетентными органами сотрудничающих государств; более частое использование специально разработанных инструментов международного сотрудничества с целью гарантировать целостность электронных доказательств, таких как оперативное обеспечение сохранности компьютерных данных; совместные расследования; использование электронных средств для передачи просьб о взаимной правовой помощи с уделением особого внимания потенциальной полезности инициативы Интерпола в отношении безопасной электронной передачи сообщений об оказании взаимной правовой помощи; обмен информацией между контактными центрами сети 24/7; и более частое использование возможностей сотрудничества между органами полиции, в том числе при содействии Интерпола, в целях сбора оперативной информации. Был упомянут также Европейский центр по борьбе с киберпреступностью, созданный Агентством Европейского союза по сотрудничеству правоохранительных органов в 2013 году для усиления принимаемых правоохранительными органами мер по противодействию киберпреступности в Европейском союзе.

25. Группа экспертов также рассмотрела вопрос о трансграничном доступе к данным. В целом было отмечено, что применяемые государствами практики и процедуры, а также условия и гарантии, относящиеся к этим практикам и процедурам, значительно различаются. Были высказаны опасения по поводу потенциальных правовых проблем, вызванных определенной практикой в отношении трансграничного доступа к данным. Кроме того, особое внимание было уделено

процессуальным правам подозреваемых, соображениям неприкосновенности частной жизни и защите личных данных, методам и законности доступа к данным, хранящимся в другой юрисдикции, и соблюдению принципа национального суверенитета.

26. Группа экспертов подчеркнула важность устойчивого наращивания потенциала для повышения эффективности и квалификации всех действующих лиц на оперативном уровне в целях решения проблем, связанных с киберпреступностью. В этой связи выступавшие отметили полезность обмена информацией об успешных видах практики и опыте между специалистами-практиками не только в рамках государств, но и между государствами. Некоторые выступавшие упомянули об активизации подготовки кадров и процесса укрепления потенциала в связи с созданием специализированных структур по борьбе с киберпреступностью или подразделений при прокуратуре и правоохранительных органах. В этой связи было подчеркнуто, что, поскольку электронные доказательства все чаще используются при расследовании других видов преступлений, крайне важно создать специализированные структуры, обладающие конкретным опытом, знаниями и оперативными навыками, для расследования этих преступлений.

27. Группа экспертов также обсудила важность поощрения и укрепления сотрудничества между национальными органами власти и частным сектором, в частности поставщиками услуг связи и интернет-услуг, в целях улучшения сохранности данных и доступа к ним. Было подчеркнуто растущее значение такого сотрудничества на национальном уровне, особенно в чрезвычайных обстоятельствах, связанных с тяжкими преступлениями, а также признано, что для обеспечения аналогичного уровня сотрудничества в рассмотрении транснациональных дел необходимо приложить более активные усилия. В этой связи было указано на опасность противоречащих друг другу требований к поставщикам услуг связи и поставщикам интернет-услуг, а именно на то, как сбалансировать их реакции с учетом требований законодательства соответствующих государств.

28. Многие выступавшие сообщили о принятии национальных мер по разработке и реализации стратегий и политики в области кибербезопасности; принятию и/или обновлению законодательства о киберпреступности; внедрению нового следственного инструментария для сбора и установления подлинности электронных доказательств, которые будут использоваться в целях доказывания в уголовном судопроизводстве, с учетом гарантий соблюдения прав человека; внедрению институциональных механизмов, призванных обеспечить более эффективное использование ресурсов в борьбе с киберпреступностью; и содействию международному сотрудничеству в борьбе с киберпреступностью. Один из выступавших отметил, что различия между кибербезопасностью и киберпреступностью являются главным соображением, учитываемым при организации внутригосударственных мер реагирования и определении сфер полномочий в этих вопросах на институциональном уровне.

29. Многие выступавшие поддержали деятельность Группы экспертов как единственного всеохватного и оптимального глобального форума, в рамках которого государства-члены имеют возможность проводить дискуссии и обмениваться мнениями о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей совершенствования национальных и международных правовых и иных мер по противодействию киберпреступности. Был упомянут также полезный вклад Комиссии в эту работу. Было отмечено, что уникальный мандат Группы экспертов предусматривает ее роль в качестве площадки для дискуссий по этой теме; однако это вовсе не исключает другие инициативы, направленные

на создание всеобъемлющей системы глобального управления для борьбы с киберпреступностью.

30. Было заявлено о поддержке проводимой УНП ООН работы по оказанию технической помощи и созданию потенциала для принятия согласованных мер противодействия киберпреступности.

31. Некоторые выступавшие выразили также признательность за выпуск публикации «Practical Guide for Requesting Electronic Evidence Across Borders» («Практическое руководство по направлению в другие страны запросов о предоставлении электронных доказательств»). Руководство было совместно разработано и выпущено УНП ООН, Исполнительным директоратом Контртеррористического комитета и Международной ассоциацией прокуроров и направлено государствам-членам и сотрудникам их систем уголовного правосудия через портал УНП ООН для распространения электронных ресурсов и законов о борьбе с преступностью. Руководство, подготовленное в сотрудничестве с государствами-членами, международными и региональными организациями и такими поставщиками коммуникационных услуг, как Facebook, Google, Microsoft и Uber, содержит информацию о действиях, которые можно предпринять на национальном уровне для сбора, обеспечения сохранности и передачи электронных доказательств с общей целью обеспечить эффективность взаимной правовой помощи на практике.

B. Электронные доказательства и уголовное правосудие

32. На своих 4-м и 5-м заседаниях 28 и 29 марта 2019 года Группа экспертов рассмотрела пункт 3 повестки дня, озаглавленный «Электронные доказательства и уголовное правосудие».

33. В дискуссии по этому пункту участвовали: г-н Сяофей Чжай (Китай); г-н Маркко Куннапу (Эстония); г-жа Камила Босх (Чили); г-н Джузеппе Корасанити (Италия); г-н Вадим Смехнов (Российская Федерация) и г-жа Брайони Дейли Уитворт (Австралия).

34. В ходе последующих прений была отмечена двоякая роль электронных доказательств. С одной стороны, было признано, что использование технологий и цифровой инфраструктуры создает больше возможностей для лиц и организованных преступных сообществ, совершающих серьезные преступления в информационной среде с помощью компьютерных технологий, для расширения масштабов их незаконной деятельности, причинения ущерба более широкому кругу лиц и увеличения своей прибыли. С другой стороны, было также подчеркнуто, что электронные доказательства играют все более важную роль в выявлении и расследовании всех видов преступлений и уголовном преследовании за их совершение.

35. Многие выступавшие отметили, что электронные доказательства приобретают все большее значение в уголовном производстве, и описали различные национальные подходы к определению сферы применения этих доказательств. Некоторые выступавшие указали на отсутствие на международном уровне общепризнанного определения электронных доказательств, притом что формулирование правил в отношении таких доказательств и их допустимости на национальном уровне является прерогативой государств-членов. Выступавшие обратили внимание на необходимость того, чтобы в процессуальном законодательстве предусматривалось предоставление компетентным правоохранительным органам полномочий официально собирать электронные доказательства, соблюдая при этом конфиденциальность, неприкосновенности частной жизни, права

человека, надлежащие правовые процедуры и другие правовые гарантии. Было отмечено, что следственные полномочия могут быть различными, начиная от традиционных процессуальных полномочий и общих следственных полномочий и заканчивая различными конкретными цифровыми методами расследования.

36. Было выражено согласие с тем, что одной из ключевых мер в борьбе с киберпреступностью и проведении цифровых расследований является сохранение целостности электронных доказательств и улик и обеспечение их подлинности и допустимости использования в качестве доказательств в соответствующем уголовном судопроизводстве. В этом контексте были упомянуты национальные стандарты, процедуры и требования, касающиеся обращения с электронными доказательствами. Группа экспертов вновь подчеркнула необходимость повышения потенциала и технических знаний компетентных органов для эффективного и действенного решения соответствующих задач.

37. Группа экспертов рассмотрела факторы, имеющие значение при оценке допустимости электронных доказательств. Была подчеркнута важность соблюдения принципа пропорциональности при использовании специальных методов расследования применительно к киберпреступлениям, включая использование секретных агентов и удаленной компьютерно-технической экспертизы, особенно в отношении даркнет. Было отмечено, что во многих внутригосударственных правовых системах этот принцип был опробован прежде всего судебной инстанцией, осуществляющей надзор за следствием, и судом, в зависимости от обстоятельств. Обоснованность может определяться исходя из тяжести рассматриваемого преступления или числа лиц, неприкосновенность частной жизни которых была нарушена в результате использования специальных методов расследования; типов компьютерных данных, о которых идет речь; доступности менее ограничительной альтернативной меры; наличия определенных справедливых процессуальных требований в процессе принятия решений; и наличия у затрагиваемых лиц адекватных возможностей для правовой защиты.

38. Было обращено внимание на рост числа программных средств и приложений со встроенным шифрованием, что делает доступ к данным в качестве электронных доказательств сложным и длительным в отсутствие надлежащих ключей дешифрования. Были высказаны практические предложения относительно путей решения этой проблемы, включая сотрудничество с другими странами, для которых возможен доступ к зашифрованной информации, использование Европейского центра по борьбе с киберпреступностью и сотрудничество с отраслью, способной разработать механизмы, обеспечивающие своевременный доступ к зашифрованным данным.

39. Было также упомянуто использование в расследованиях искусственного интеллекта, в частности применительно к распознаванию лиц и нарушениям авторских прав. В целом, искусственный интеллект может предлагать решения, позволяющие эффективнее использовать время и ресурсы при исследовании больших объемов данных в поисках важных электронных доказательств.

40. Были обсуждены сведения об абонентах как типе данных, которые наиболее часто запрашивают органы уголовного правосудия при расследовании киберпреступлений и других дел, связанных с электронными доказательствами. В этой связи многие выступавшие упомянули о трудностях соотнесения сведений об абонентах с конкретным адресом интернет-протокола (IP), использованным в уголовном преступлении. Было отмечено, что, хотя статические IP-адреса стабильны и присваиваются конкретному абоненту на время действия соглашения об обслуживании, а поставщики услуг могут посмотреть такую информацию в базе данных абонентов, у поставщиков услуг есть возможность присвоить IP-адрес нескольким пользователям. Поэтому существует необходимость в

определении абонента, которому был присвоен IP-адрес на конкретный момент времени. Было также отмечено, что причина динамического распределения IP-адресов заключается в том, что в версии 4 интернет-протокола доступно лишь их ограниченное количество. Эта проблема будет решена после завершения перехода к версии 6 интернет-протокола или на более продвинутом этапе.

41. Был также обсужден вопрос о различиях между типами запрашиваемых данных и их влиянии на эффективность и оперативность механизмов международного сотрудничества для получения электронных доказательств. Рассмотренные решения касались, в частности, укрепления сотрудничества между правоохранительными органами, продолжении многостороннего диалога по вопросам транснационального доступа к компьютерным данным и установления отдельного режима доступа к сведениям об абонентах, как это определено в пункте 3 статьи 18 Будапештской конвенции.

42. Многие выступавшие упомянули о проблемах, связанных с криптовалютами, при расследовании киберпреступлений. Группе экспертов было сообщено о разработанном УНП ООН курсе обучения специалистов по расследованиям, связанным с криптовалютами. Целью подготовки состоит в повышении уровня квалификации сотрудников правоохранительных органов, аналитиков, прокуроров и судей в вопросах, касающихся криптовалюты, в том числе методов отслеживания биткоинов при проведении финансовых расследований, поиска информационных ресурсов и взаимодействия в изучении материалов международных судебных дел.

43. По пункту 3 повестки дня некоторые выступавшие обсудили вопросы юрисдикции. Особое внимание было обращено на недавние изменения в национальной судебной практике, касающиеся толкования принципа территориальности в тех случаях, когда компьютерные данные хранятся на облачных серверах в других юрисдикциях.

44. Выступавшие согласились с тем, что международное сотрудничество имеет первостепенное значение для сбора электронных доказательств и обмена ими в контексте трансграничных расследований. Было подчеркнуто, что государствам следует в полной мере использовать Конвенцию об организованной преступности и соответствующие многосторонние, региональные и двусторонние договоры и соглашения о борьбе с киберпреступностью в целях укрепления международного сотрудничества в области оказания правовой помощи и правоприменения в соответствующих случаях при соблюдении принципов суверенитета, равенства и взаимности. Была подчеркнута важность развития сетевого взаимодействия для обмена опытом и знаниями, в частности, для решения проблем, возникающих в связи с различием национальных требований в отношении приемлемости, доказательной силы и целостности и подлинности таких доказательств.

45. Многие выступавшие уделяли первостепенное внимание необходимости устойчивого наращивания потенциала в рамках национальных правоохранительных систем и систем уголовного правосудия, включая повышение квалификации специалистов-практиков из центральных органов, занимающихся международным сотрудничеством. Было отмечено, что такое наращивание потенциала имеет важное значение, особенно для развивающихся стран, как с точки зрения людских ресурсов, инфраструктуры и оборудования, так и с точки зрения преодоления разрыва в цифровых технологиях с развитыми странами. В целом было выражено согласие с тем, что наращивание потенциала правоохранительных органов и органов уголовного правосудия в области борьбы с киберпреступностью будет постоянным и непрерывным процессом, учитывая, что непрерывно появляются новые технологии и новые методы совершения преступлений. Таким

образом, подавляющее большинство выступавших указали на техническую помощь и сотрудничество как на важные предпосылки для укрепления внутреннего потенциала и создания возможностей для обмена передовым опытом и практикой проведения расследований и для распространения новых методов.

46. В этой связи ряд выступавших сообщили о трудностях, обусловленных ограниченностью ресурсов в области криминалистической экспертизы, нехваткой технико-криминалистических средств и оборудования, которые часто бывают дорогостоящими, и огромным количеством собираемых для анализа данных. Были отмечены также трудности с набором достаточно квалифицированных кадров.

C. Прочие вопросы

47. На своем 6-м заседании 29 марта 2019 года Группа экспертов рассмотрела пункт 4 повестки дня, озаглавленный «Прочие вопросы».

48. Один из выступавших запросил информацию о докладе о противодействии использованию информационно-коммуникационных технологий, который во исполнение резолюции 73/187 должен быть представлен Генеральной Ассамблее на ее семьдесят четвертой сессии. В ответ представитель Секретариата сослался на содержащийся в резолюции мандат, подчеркнув, что 13 февраля 2019 года государствам-членам была направлена вербальная нота с предложением представить информацию о трудностях, с которыми они сталкиваются в борьбе с использованием информационно-коммуникационных технологий в преступных целях, и указанием на то, что эта информация будет использована для подготовки доклада. Крайним сроком для представления странами информации была определена пятница, 12 апреля 2019 года. По истечении этого срока Секретариат соберет воедино полученную информацию для доработки доклада в мае 2019 года.

IV. Организация работы совещания

A. Открытие совещания

49. Совещание открыл заместитель председателя Группы экспертов Андре Рипл (Бразилия), исполняющий функции Председателя пятого совещания Группы экспертов.

B. Заявления

50. С заявлениями выступили эксперты из следующих государств-членов: Австралии, Алжира, Аргентины, Армении, Беларуси, Бразилии, Буркина-Фасо, Вьетнама, Германии, Грузии, Доминиканской Республики, Индии, Индонезии, Иордании, Ирана (Исламская Республика), Испании, Италии, Канады, Китая, Колумбии, Коста-Рики, Кувейта, Мавритании, Малайзии, Мексики, Марокко, Нигера, Нигерии, Нидерландов, Норвегии, Объединенных Арабских Эмиратов, Парагвая, Перу, Российской Федерации, Сербии, Словакии, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Таиланда, Филиппин, Франции, Чили, Шри-Ланки, Эквадора, Эстонии, Южной Африки и Японии.

51. С заявлениями выступили также представители двух межправительственных организаций: Европейского союза и Совета Европы.

C. Утверждение повестки дня и другие организационные вопросы

52. На своем 1-м заседании 27 марта 2019 года Группа экспертов утвердила следующую предварительную повестку дня:

1. Организационные вопросы:
   a) открытие совещания;
   b) утверждение повестки дня
2. Правоохранительная деятельность и расследования
3. Электронные доказательства и уголовное правосудие
4. Прочие вопросы
5. Утверждение доклада.

D. Участники

53. В работе совещания приняли участие представители 105 государств-членов, института сети программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, УНП ООН, межправительственных организаций и частного сектора.

54. Список участников содержится в документе UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1http://undocs.org/UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1.

E. Документация

55. Помимо проекта всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора на рассмотрение Группы экспертов были представлены следующие документы:

a) аннотированная предварительная повестка дня (UNODC/CCPCJ/EG.4/2019/1);

b) Chair's proposal for the workplan of the Expert Group for the period 2018–2021, based on Commission on Crime Prevention and Criminal Justice resolution 26/4 (Предложение Председателя по плану работы Группы экспертов на период 2018–2021 годов, подготовленное на основе резолюции 26/4 Комиссии по предупреждению преступности и уголовному правосудию) (UNODC/CCPCJ/EG.4/2018/CRP.1).

V. Утверждение доклада

56. На своем 6-м заседании 29 марта 2019 года Группа экспертов утвердила свой доклад (UNODC/CCPCJ/EG.4/2019/2).