19 April 2021
Russian
Original: English

Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, прошедшего в Вене 6–8 апреля 2021 года

I. Введение

1. В резолюции 65/230 Генеральная Ассамблея просила Комиссию по предупреждению преступности и уголовному правосудию учредить в соответствии с пунктом 42 документа «Салвадорская декларация 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 состоялось 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 25–28 февраля 2013 года. На нем Группа экспертов приняла к сведению проект всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, подготовленный Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) под ее руководством во исполнение мандата, предусмотренного в резолюции 65/230 Генеральной Ассамблеи, на основе подборки тем и методологии исследования, утвержденных на первом совещании Группы экспертов.

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, помимо всего прочего, рассмотрела вопрос об утверждении кратких докладов о работе своих первых двух совещаний, подготовленных Докладчиком, а также проект всестороннего исследования проблемы киберпреступности, замечания к нему и вопросы дальнейшей работы над проектом исследования. В ходе совещания был проведен обмен 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. В этой же 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 уделила основное внимание связанным с киберпреступностью вопросам законодательства, правовой основы и криминализации. Были обсуждены последние изменения законодательства и политики в области противодействия киберпреступности на национальном и международном уровнях. Группа экспертов также рассмотрела подходы к криминализации киберпреступлений на национальном уровне. На том же совещании Группа экспертов утвердила предложение Председателя по плану своей работы на период 2018–2021 годов (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. Пятое совещание Группы экспертов состоялось в Вене 27–29 марта 2019 года. На этом совещании Группа экспертов сосредоточила внимание на таких темах, как правоохранительная деятельность и расследования, а также электронные доказательства и уголовное правосудие, связанные с киберпреступностью. На этом совещании Группа экспертов была проинформирована, в частности, об успехах стран в осуществлении правовых и процессуальных мер противодействия киберпреступности и мер по внедрению нового следственного инструментария для сбора и установления подлинности электронных доказательств, которые будут использоваться в целях доказывания в уголовном судопроизводстве. В ходе обсуждения особое внимание было также уделено вопросу о том, как обеспечить баланс между необходимостью принятия правоохранительными органами эффективных мер реагирования на киберпреступность и защитой основных прав человека, в частности права на неприкосновенность частной жизни. Группа экспертов особо отметила необходимость устойчивого наращивания потенциала в целях расширения возможностей, имеющихся на национальном уровне, и создания благоприятных условий для обмена передовой практикой и опытом проведения расследований.

9. На шестом совещании Группы экспертов, состоявшемся в Вене 27–29 июля 2020 года, Докладчиком был составлен перечень предварительных рекомендаций и выводов по темам международного сотрудничества и предупреждения киберпреступности. В соответствии с планом работы Группы экспертов на 2019–2021 годы этот перечень был включен в доклад о работе шестого совещания (UNODC/CCPCJ/EG.4/2020/2) в виде подборки замечаний государств-членов для дальнейшего обсуждения на итоговом совещании, которое должно состояться не позднее 2021 года.

10. Сроки проведения седьмого совещания Группы экспертов с 6 по 8 апреля 2021 года были утверждены ее расширенным бюро 23 ноября 2020 года при помощи процедуры «отсутствия возражений». Предварительная повестка дня седьмого совещания была согласована расширенным бюро 14 декабря 2020 года также при помощи процедуры «отсутствия возражений». Ввиду сохранения ситуации, связанной с коронавирусной инфекцией COVID-19, 11 марта 2021 года в соответствии с той же процедурой был утвержден смешанный формат проведения седьмого совещания под руководством Председателя. На заседании расширенного бюро, проведенном 31 марта 2021 года, было решено оформить доклад о работе совещания в виде процедурного доклада без резюме обсуждений, которое подготавливает Председатель, а выводы и рекомендации изложить в приложении к докладу.

II. Организация работы совещания

A. Открытие совещания

11. Совещание открыл заместитель председателя Группы экспертов Андре Рипл (Бразилия), исполнявший функции Председателя седьмого совещания Группы экспертов.

B. Утверждение повестки дня и другие организационные вопросы

12. На 1-м заседании 6 апреля 2021 года Группа экспертов утвердила следующую предварительную повестку дня:

1. Организационные вопросы:
   a) открытие совещания;
   b) утверждение повестки дня
2. Рассмотрение всех предварительных выводов и рекомендаций, сделанных на четвертом, пятом и шестом совещаниях Группы экспертов, состоявшихся в 2018, 2019 и 2020 годах, и подготовка выводов и рекомендаций для представления Комиссии по предупреждению преступности и уголовному правосудию
3. Обсуждение будущей работы Группы экспертов
4. Прочие вопросы
5. Утверждение доклада.

C. Заявления

13. По предложению Председателя Группа экспертов договорилась о том, что делегации воздержатся от заявлений общего характера по пункту 1 повестки дня. Было также достигнуто согласие с тем, что из-за нехватки времени выступления по пунктам 2 и 3 повестки дня будут ограничены максимум тремя минутами каждое и что у делегаций будет также возможность направить свои заявления в письменном виде в секретариат, который разместит их на веб-сайте седьмого совещания Группы экспертов.

14. По пункту 3 повестки дня с заявлениями выступили Австралия, Чили, Колумбия, Европейский Союз (от имени своих государств-членов), Йемен, Доминиканская Республика, Бразилия, Нидерланды, Боливарианская Республика Венесуэла, Новая Зеландия, Гватемала, Нигерия, Соединенные Штаты Америки, Китай, Российская Федерация, Франция, Куба, Япония, Южная Африка, Польша, Канада,

Бельгия, Австрия, Аргентина, Норвегия, Исламская Республика Иран, Португалия, Кыргызстан, Гондурас, Соединенное Королевство Великобритании и Северной Ирландии, Индия, Мексика, Никарагуа и Сирийская Арабская Республика.

D. Организация работы

15. На своем 1-м заседании 6 апреля Группа экспертов начала рассмотрение списка выводов и рекомендаций, относящихся к темам «Законодательство и правовая основа» и «Криминализация», изложенным в документе зала заседаний под названием «Компиляция всех предварительных выводов и рекомендаций, предложенных государствами-членами в ходе совещаний Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенных в 2018, 2019 и 2020 годах» (UNODC/CCPCJ/EG.4/2021/CRP.1). С этой целью Председатель предложил делегациям указать на наличие у них возражений, по существу или по формулировке, против того или иного вывода или какой-либо рекомендации. Затем эти возражения были отражены в сводном тексте, который был выведен на экран и впоследствии распространен среди делегаций в электронном виде.

16. На своем 2-м заседании 6 апреля Группа экспертов завершила первое чтение списка предварительных выводов и рекомендаций, по которым не было принято решения на совещаниях Группы экспертов в 2018 и 2019 годах, и приступила к детальному рассмотрению тех выводов и рекомендаций, по которым не удалось достичь консенсуса из-за вопросов, связанных с формулировкой.

17. На своем 3-м заседании 7 апреля Группа экспертов завершила первое чтение списка выводов и рекомендаций, по которым не было принято решения на совещании Группы экспертов в 2020 году, и продолжила подробное рассмотрение тех из них, по которым не было достигнуто консенсуса. Рабочая группа также обсудила вопрос о том, как довести до сведения Комиссии те выводы и рекомендации, достичь консенсуса по которым не удалось.

18. На своем 4-м заседании 7 апреля Группа экспертов продолжила подробное обсуждение некоторых выводов и рекомендаций, по которым не было достигнуто консенсуса. Мнения разошлись относительно того, будут ли представлены Комиссии те выводы и рекомендации, по которым не было достигнуто консенсуса.

19. На своем 5-м заседании 8 апреля Группа экспертов продолжила обсуждение вопроса о том, будут ли представлены Комиссии предварительные выводы и рекомендации, по которым не было достигнуто консенсуса. Председатель предложил, и совещание согласилось с этим, что в настоящем докладе будет отражен тот факт, что Группа экспертов рассмотрела все выводы и рекомендации, содержащиеся в документе UNODC/CCPCJ/EG.4/2021/CRP.1, в ускоренном порядке из-за сокращения количества часов, отведенных на седьмое совещание Группы экспертов, ввиду принятия организационных мер, связанных с COVID-19, т. е. в общей сложности 12 часов вместо обычных 18. Группа экспертов также согласилась передать Комиссии 63 согласованных вывода и рекомендации, содержащиеся в приложении к настоящему докладу.

20. Также на своем 5-м заседании Группа экспертов рассмотрела пункт 3 повестки дня, озаглавленный «Обсуждение будущей работы Группы экспертов». По вопросу о будущей работе Группы экспертов мнения разошлись, что отражено в заявлениях, загруженных на веб-сайт седьмого совещания Группы экспертов[1].

E. Участники

21. В работе совещания участвовали представители 111 государств-членов, 5 институтов сети программы Организации Объединенных Наций в области

[1] См. www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime_2021.html.

предупреждения преступности и уголовного правосудия, 3 подразделений Организации Объединенных Наций и 11 межправительственных организаций, а также представители научных кругов и частного сектора.

22. Список участников содержится в документе UNODC/CCPCJ/EG.4/2021/INF/1/Rev.1.

F. Документация

23. Группе экспертов были представлены следующие документы:

a) Аннотированная предварительная повестка дня (UNODC/CCPCJ/EG.4/2021/1);

b) Компиляция всех предварительных выводов и рекомендаций, предложенных государствами-членами в ходе совещаний Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенных в 2018, 2019 и 2020 годах (UNODC/CCPCJ/EG.4/2021/CRP.1).

III. Утверждение доклада

24. На своем 6-м заседании 8 апреля 2021 года Группа экспертов утвердила настоящий доклад.

Приложение

Выводы и рекомендации, согласованные Группой экспертов и вынесенные на рассмотрение Комиссии по предупреждению преступности и уголовному правосудию

Законодательство и правовая основа

1. Государствам-членам следует обеспечить, чтобы их законодательные положения отвечали требованиям времени с учетом технического прогресса посредством принятия законодательства, содержащего технически нейтральные формулировки и предусматривающего уголовную ответственность за деятельность, признаваемую незаконной, а не за использование технических средств. Государствам-членам следует по мере необходимости и целесообразности также рассмотреть вопрос о разработке на внутригосударственном уровне согласованной терминологии для описания киберпреступной деятельности и содействия, насколько это возможно, точному толкованию соответствующего законодательства правоохранительными и судебными органами.

2. Государствам-членам следует оказывать поддержку Управлению Организации Объединенных Наций по наркотикам и преступности (УНП ООН) в разработке образовательного проекта или учебной программы, направленных на повышение осведомленности сотрудников судебных органов и органов прокуратуры, судебных экспертов по цифровым технологиям государств-членов и сотрудников частных образований о киберпреступности и соответствующих мерах и использовать инструменты наращивания потенциала и платформу управления электронными данными для повышения осведомленности гражданского общества о воздействии киберпреступности.

3. УНП ООН следует активно участвовать в деятельности по наращиванию потенциала в интересах всех нуждающихся в помощи государств-членов, особенно развивающихся стран. Такая деятельность по наращиванию потенциала должна быть политически нейтральной и свободной от каких-либо условий, а также должна быть результатом тщательных консультаций и добровольного выбора странами — получателями помощи. С точки зрения содержания эта деятельность по наращиванию потенциала должна охватывать как минимум следующие области: обучение судей, прокуроров, следователей и сотрудников правоохранительных органов по вопросам расследования киберпреступлений, работа с электронными доказательствами, система обеспечения сохранности хранения и судебная экспертиза.

Криминализация

4. Государствам-членам следует учитывать тот факт, что многие основные положения уголовного законодательства, применяемые к офлайновым преступлениям, могут также применяться к преступлениям, совершенным в режиме онлайн. В этой связи государствам-членам с целью укрепления правоохранительной деятельности следует применять, в надлежащих случаях, действующие положения внутреннего законодательства и международного права в отношении преступлений, совершаемых в онлайновой среде.

5. В той степени, в которой они уже не сделали этого, государствам-членам следует рассмотреть вопрос о криминализации:

a) незаконного получения доступа к компьютерным системам или их взлома;

b) незаконного перехвата или повреждения компьютерных данных и повреждения компьютерных систем;

c) незаконного вмешательства в компьютерные данные и системы.

6. Государствам-членам следует изучить пути оказания помощи для своевременного и безопасного обмена информацией между следователями и прокурорами, занимающимися делами, связанными с киберпреступностью, в том числе посредством укрепления сетей национальных учреждений, которые могут работать круглосуточно.

Правоохранительная деятельность и расследования

7. Государствам рекомендуется продолжать предоставлять УНП ООН необходимые мандаты и финансовую поддержку для получения ощутимых результатов при осуществлении проектов по наращиванию потенциала в этой области.

8. Странам следует выделять средства на подготовку специалистов по расследованию киберпреступлений и на создание партнерств, использующих механизмы сотрудничества для получения важных доказательств.

9. Странам следует выделять средства на 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.

10. Развитие внутреннего процессуального права должно идти в ногу с развитием технологий и обеспечивать правоохранительным органам надлежащую оснащенность для борьбы с киберпреступностью. 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, прав человека и основных свобод. Кроме того, государствам-членам следует выделить ресурсы на принятие внутреннего законодательства, которое допускает:

a) сбор информации о трафике и контенте в режиме реального времени в соответствующих случаях;

b) международное сотрудничество между национальными правоохранительными органами.

Электронные доказательства[2] и уголовное правосудие

11. 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.

12. 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.

[2] По поводу термина «электронные доказательства» одно из государств-членов отметило, что понятие «электронные» означает способ передачи или хранения данных и может также относиться, например, к радиоволнам или оптоволокну. Было также отмечено, что в данном случае имеются в виду не «электронные доказательства», а «цифровая информация», состоящая из единиц и нулей. Другое государство-член указало на то, что термин «электронные доказательства» включает в себя доказательства как в цифровой, так и в аналоговой форме.

13. 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.

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

15. В правовых системах, использующих следственную модель, при которой сотрудники судебных органов также являются следователями, работникам органов правосудия следует проходить специальную подготовку по вопросам киберпреступности.

16. Государства могут рассмотреть вопрос о признании в их внутреннем законодательстве в качестве электронных доказательств следующих данных: информация о трафике, 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.

17. Государствам-членам следует разработать и применять нормативно-правовую базу, юрисдикционные правила и другие процессуальные нормы в целях эффективного расследования киберпреступлений на национальном уровне и обеспечения эффективного международного сотрудничества в этой области посредством эффективного правоприменения при уважении национального суверенитета и соблюдении права на неприкосновенность частной жизни и всех прав человека. Эти меры могут включать:

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

b) принятие положений об отслеживании электронных сообщений на национальном и международном уровнях.

18. Государствам-членам следует прилагать усилия к расширению сотрудничества в сборе электронных доказательств. В этой связи им рекомендуется рассмотреть, в частности, следующие направления работы:

a) обмен информацией об угрозах киберпреступности;

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

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

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

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

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

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

Международное сотрудничество

19. Для повышения эффективности международного сотрудничества следует создать механизмы быстрого рассмотрения просьб о международной помощи и наладить каналы связи между национальными органами через сотрудников по связи и информационные системы с целью облегчения трансграничного сбора доказательств и передачи электронных доказательств в режиме онлайн.

20. Необходимо оптимизировать процедуры международного сотрудничества таким образом, чтобы в пределах возможностей, предоставляемых внутренней нормативно-правовой основой, обеспечить оказание максимально широкой помощи в выполнении просьб о международном сотрудничестве, касающихся сохранности электронных доказательств и предоставления доступа к файлам регистрации и учетным записям пользователей, не нарушая права человека и основные свободы или имущественные права.

21. Странам рекомендуется особо внимательно следить за адекватностью действий следственных органов и уважать основные свободы и требования защиты персональных данных, связанные с тайной частной переписки.

22. Странам рекомендуется наладить более эффективное сотрудничество с отраслью и активизировать взаимодействие между государством и частными поставщиками услуг, в частности в целях решения проблем, связанных с размещением в интернете материалов вредоносного и противозаконного содержания.

23. Для обеспечения сохранности допустимых электронных доказательств и обмена ими странам рекомендуется присоединиться к авторизованным сетям специалистов, включая круглосуточные сети, специализированные сети по киберпреступности и каналы оперативного полицейского взаимодействия Международной организации уголовной полиции (Интерпол), и активнее использовать и развивать их, а также наладить связи со стратегическими партнерами с целью обмена данными по вопросам киберпреступности, оперативного принятия мер реагирования и сведения к минимуму опасности утраты важных доказательств. Прежде чем задействовать каналы взаимной правовой помощи, рекомендуется также использовать каналы полицейского взаимодействия и другие методы неофициального сотрудничества.

24. Государствам-членам следует делиться информацией о национальных подходах к решению проблемы своевременного доступа к электронным доказательствам с другими государствами-членами, чтобы те могли использовать этот опыт для повышения эффективности собственных процедур.

25. Государствам-членам следует ввести в практику направление и прием просьб о взаимной правовой помощи с использованием электронных средств с целью сокращения задержек, связанных с международной пересылкой документов.

26. Странам следует обеспечить выполнение требований национального законодательства и усилить координацию и взаимодействие на национальном уровне в вопросах сбора информации и доказательств и обмена ими для целей уголовного преследования.

27. В целях укрепления потенциала правоохранительных органов государствам рекомендуется создавать совместные следственные группы с другими странами на двустороннем, региональном или международном уровнях.

28. Для эффективного международного сотрудничества необходимо, чтобы в национальном законодательстве были предусмотрены соответствующие процедуры. Поэтому необходимо обеспечить, чтобы национальное законодательство допускало возможность международного сотрудничества между правоохранительными органами.

29. Следует уделять приоритетное внимание и прилагать более активные усилия к устойчивому наращиванию потенциала и оказанию технической помощи в целях расширения возможностей во всех сферах оперативной деятельности и

укрепления потенциала национальных органов в области борьбы с киберпреступностью, в том числе путем развития связей, проведения совместных совещаний и курсов подготовки, обмена передовым опытом, учебными материалами и типовыми формами для сотрудничества. Такие мероприятия по наращиванию потенциала и подготовке кадров должны включать узкоспециализированные учебные курсы для практических работников, направленные, в частности, на привлечение женщин-экспертов, а также учитывать потребности законодателей и ответственных должностных лиц в более глубоком понимании вопросов сохранения данных для целей правоохранительной деятельности. Одним из направлений работы по наращиванию потенциала и подготовке кадров должно быть повышение квалификации сотрудников правоохранительных органов, следователей и аналитиков в таких областях, как судебная экспертиза, использование данных из открытых источников при расследовании, порядок передачи и хранения электронных доказательств, сбор электронных доказательств за рубежом и обмен ими. Другим направлением такой работы является повышение квалификации судей, прокуроров, сотрудников центральных органов власти и адвокатов в вопросах ведения соответствующих дел и вынесения решений.

30. Большое значение для сбора и совместного использования электронных доказательств в контексте трансграничных расследований и для оперативного и эффективно реагирования на просьбы о взаимной правовой помощи, связанной с сохранением и получением электронных доказательств, имеет международное сотрудничество. В процессе такого сотрудничества следует соблюдать принципы суверенитета и взаимности.

31. УНП ООН рекомендуется и далее проводить программы по наращиванию потенциала и подготовке кадров в области борьбы с киберпреступностью для национальных правительственных экспертов в целях повышения их квалификации в области выявления и расследования киберпреступлений. В рамках работы по наращиванию потенциала необходимо учитывать потребности развивающихся стран, уделять особое внимание факторам уязвимости каждой страны с целью оказания адресной технической помощи и содействовать обмену актуальными знаниями в наилучших интересах специалистов-практиков и заинтересованных сторон.

32. Для оказания содействия сотрудникам органов уголовного правосудия в составлении просьб о взаимной правовой помощи УНП ООН разработало «Программу составления просьб об оказании взаимной правовой помощи». Управление также разработало «Практическое руководство по истребованию электронных доказательств в других странах», которое доступно по запросу сотрудникам государственных органов государств-членов. Эти основные пособия УНП ООН могут быть полезными для стран.

33. Всем государствам-членам рекомендуется принять активное участие в работе специального комитета по разработке новой конвенции.

34. Государствам-членам следует рассмотреть вопрос о выделении средств на создание специальных централизованных подразделений по противодействию киберпреступности и региональных технических подразделений по расследованию уголовных преступлений.

35. Государствам-членам следует также рассмотреть возможность создания внутри центральных органов, отвечающих за оказание взаимной правовой помощи, самостоятельных подразделений по борьбе с киберпреступностью в качестве экспертных центров по вопросам международного сотрудничества в этой сложной области. Такие специализированные подразделения будут не только полезны в повседневной практике оказания взаимной правовой помощи, но и позволят оказывать целенаправленную помощь в создании потенциала, например в области подготовки кадров для удовлетворения потребностей национальных и иностранных органов власти в быстром и эффективном получении взаимной правовой помощи, связанной с обеспечением электронных доказательств по делам о киберпреступлениях.

36. Государствам-членам следует рассмотреть вопрос о ведении электронных баз данных для облегчения доступа к статистическим данным по входящим и исходящим просьбам о взаимной правовой помощи, связанной с электронными доказательствами, для обеспечения возможности оценки эффективности и работоспособности.

37. Государствам-членам следует напомнить о необходимости действовать через центральные органы при передаче просьб о взаимной правовой помощи и взаимодействии с компетентными органами по вопросам их выполнения с целью соблюдения требований действующих договоров и сокращения задержек в процессе работы.

Предупреждение

38. Следует признать, что предупреждение киберпреступности является обязанностью не одного государства, а требует участия всех заинтересованных сторон, включая правоохранительные органы, частный сектор, особенно поставщиков интернет-услуг, неправительственные организации, учебные заведения, научные круги и население в целом.

39. Было рекомендовано обеспечить, чтобы у населения был легкий доступ к таким инструментам предупреждения киберпреступности, как онлайн-платформы, аудиоклипы и наглядные информационные материалы, изложенные простым и понятным языком, а также платформы для сообщения о нарушениях.

40. Было высказано мнение о необходимости разработки долгосрочных государственных стратегий предупреждения киберпреступности, включающих разработку информационных кампаний на тему безопасного пользования интернетом.

41. В рамках работы по предупреждению и противодействию киберпреступности государствам следует уделять особое внимание профилактике и пресечению гендерного насилия, в частности насилия в отношении женщин и девочек, и преступлений на почве ненависти.

42. Профилактическая работа должна носить упреждающий, регулярный и непрерывный характер и проводиться с учетом интересов уязвимых категорий населения.

43. Государствам следует организовать учебную подготовку для судей, специализирующихся на делах о киберпреступлениях, и обеспечить следственные органы высокоэффективными средствами для отслеживания операций с криптовалютой и противодействия ее использованию в преступных целях.

44. Было рекомендовано наращивать коллективный потенциал компетентных учреждений и изменить подход к противодействию киберпреступности с ответного на профилактический. Было также рекомендовано создать надежный механизм для стимулирования и облегчения обмена оперативными данными о возможных способах совершения преступлений.

45. Государствам-членам рекомендуется продолжать эффективную профилактическую работу на национальном и международном уровнях и уделять особое внимание таким инициативным мерам, как проведение информационно-разъяснительной работы об опасности киберпреступности и информационных кампаний, посвященных конкретным методам совершения киберпреступлений, включая фишинг и использование вредоносных программ (программ-вымогателей), и ориентированных на разную целевую аудиторию, например молодежь и людей старшего возраста. Государствам-членам также рекомендуется и далее уделять особое внимание повышению вероятности привлечения к ответственности и наказания правонарушителей и предупреждению преступности путем выявления и пресечения незаконной деятельности в интернете. Органам полиции и прокуратуры следует выделять средства для выявления киберугроз, оповещения о них и принятия необходимых мер реагирования. Огромную важность имеет развитие публично-

частных партнерств. Подобные профилактические мероприятия не требуют принятия дополнительных законов или подзаконных актов.

46. Из-за сохранения «цифрового разрыва» некоторые развивающиеся страны не имеют возможности предупреждать, выявлять и пресекать киберпреступления и поэтому более уязвимы перед создаваемыми ими угрозами.

47. УНП ООН настоятельно рекомендуется и далее оказывать техническую помощь в области предупреждения и противодействия киберпреступности при поступлении соответствующей просьбы.

48. Государствам-членам рекомендуется и далее проводить эффективную профилактическую работу на национальном и международном уровнях, уделяя особое внимание принятию превентивных мер, направленных на повышение осведомленности о рисках, связанных с киберпреступностью, и вероятности привлечения к ответственности и наказания правонарушителей, и прилагая усилия к предупреждению дальнейших преступлений путем выявления и пресечения незаконной деятельности в интернете.

49. Странам следует вести сбор данных по широкому спектру вопросов для более глубокого понимания тенденций с целью выработки обоснованной политики и оперативных мер борьбы с киберпреступностью.

50. При разработке стратегий предупреждения киберпреступности следует учитывать необходимость защиты прав человека.

51. Одним из направлений национальных стратегий противодействия киберпреступности должно быть развитие потенциала системы уголовного правосудия. Следует уделять приоритетное внимание оказанию помощи развивающимся странам в укреплении потенциала правоохранительных органов в области предупреждения киберпреступности.

52. Государствам следует разрабатывать и развивать программы поддержки жертв киберпреступлений.

53. Государствам следует проводить обследования для оценки воздействия киберпреступности на коммерческие предприятия, в том числе для сбора информации о принимаемых мерах, подготовке кадров, видах киберинцидентов, с которыми сталкиваются коммерческие предприятия, и расходах на предотвращение подобных инцидентов и устранение их последствий.

54. Государствам следует оказывать поддержку коммерческим предприятиям и профессиональным сообществам в повышении осведомленности о рисках киберпреступности, реализации стратегий смягчения последствий кибератак и совершенствовании методов работы в киберпространстве, поскольку подобные мероприятия в дальнейшем оказывают значительный профилактический эффект.

55. Необходимо внимательно изучать способы совершения киберпреступлений путем анализа оперативных данных и проведения криминологических исследований с целью более эффективного использования имеющихся ресурсов и выявления уязвимостей.

56. Странам следует рассмотреть вопрос о принятии конкретных и адресных мер для обеспечения безопасности детей в интернете. В рамках такой работы необходимо обеспечить, чтобы национальная нормативно-правовая база, практические договоренности и механизмы международного сотрудничества обеспечивали возможность сообщать о фактах сексуальных надругательств над детьми и сексуальной эксплуатации детей в интернете, выявлять и расследовать такие факты, осуществлять уголовное преследование в связи с ними и принимать сдерживающие меры.

57. Важным партнером в предупреждении киберпреступности является отрасль информационных технологий. Странам следует рассмотреть целесообразность создания механизмов сотрудничества с отраслью, в том числе по вопросам передачи сообщений о нарушениях компетентным национальным органам и

удаления из сети материалов вредоносного и незаконного содержания, в частности материалов с изображением сцен сексуальной эксплуатации детей и жестокого насилия.

58. Следует на регулярной основе выпускать бюллетени с информацией о предотвращенных инцидентах и доводить их до сведения пользователей, организаций и других заинтересованных сторон с целью содействия предотвращению киберинцидентов, потенциально способствующих преступной деятельности.

59. Государствам следует активно привлекать женщин-экспертов к работе по предупреждению и расследованию киберпреступлений.

60. Для обобщения национального и регионального опыта следует создать многосторонний банк данных, который будет способствовать распространению передовой практики, наработанной в разных контекстах.

61. Следует проводить более активную информационную работу по проблеме киберзапугивания и угроз применения насилия или жестокого обращения в интернете и оказывать помощь в законодательной сфере, направленную на борьбу с этими явлениями.

62. Государствам рекомендуется выделять средства на развитие кадрового потенциала с целью повышения профессиональной квалификации сотрудников всей системы уголовного правосудия, поскольку такая работа является действенной мерой предупреждения киберпреступности, оказывающей мощный сдерживающий эффект.

63. УНП ООН следует способствовать обмену информацией о наилучших видах практики в области принятия эффективных мер предупреждения киберпреступности.