27 July 2020
Russian
Original: English

Группа экспертов для проведения всестороннего исследования проблемы киберпреступности
Вена, 27–29 июля 2020 года

Проект доклада

Добавление

II. Перечень предварительных рекомендаций и выводов (*продолжение*)

A. Международное сотрудничество

1. В соответствии с планом работы Группы экспертов настоящий пункт содержит подборку предложений, внесенных государствами-членами на совещании по пункту 2 повестки дня, озаглавленному «Международное сотрудничество». Настоящие предварительные рекомендации и выводы были представлены государствами-членами, и их включение не означает их одобрения Группой экспертов, и их перечисление не зависит от степени их важности:

1) Что касается сферы определения киберпреступности для целей международного сотрудничества, то странам следует обеспечить достаточную степень криминализации киберпреступлений, охватывающую не только киберпреступления, но и другие преступления, часто совершаемые с использованием Интернета и электронных средств (преступления, совершаемые с помощью кибернетических технологий), такие как кибермошенничество, киберхищения, вымогательство, отмывание денег, торговля наркотиками и оружием, детская порнография и террористическая деятельность.

2) Что касается механизмов международного сотрудничества, то государствам рекомендуется присоединиться к существующим многосторонним договорам, таким как Будапештская конвенция и Конвенция об организованной преступности, которые обеспечивают правовую основу для оказания взаимной правовой помощи, а в отсутствие двусторонних ДВПП использовать такие договоры; при отсутствии какого-либо международного договора государства могут просить другое государство о сотрудничестве на основе принципа взаимности; Будапештская конвенция должна также использоваться в качестве стандарта для наращивания потенциала и оказания технической помощи во всем мире, при этом внимание обращается на ведущиеся переговоры по второму дополнительному протоколу к Будапештской конвенции в целях дальнейшего расширения трансграничного сотрудничества. В другом выступлении было вновь высказано мнение о том, что Будапештская конвенция имеет ограниченное применение в силу ее характера как регионального документа и статуса ратификации, а также

отсутствия целостного подхода, не учитывающего современные тенденции в области киберпреступности и не в полной мере подходящего для развивающихся стран. Внимание было обращено на резолюцию 74/247 Генеральной Ассамблеи от 27 декабря 2019 года, в которой Ассамблея постановила учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В других выступлениях было отмечено, что новые рамки или документы по киберпреступности не должны идти вразрез с существующими и что они не должны заставлять государства отказываться от действующих договоров или принятых ранее обязательств, а также уже существующих соглашений или нарушать их.

3) При проведении расследований киберпреступлений необходимо иметь стратегических партнеров, таких как члены существующих организаций, включая Организацию американских государств, Группу семи или Интерпол.

4) При проведении расследований и судебных разбирательств необходимо уважать суверенитет и юрисдикцию государств. Никакие требования о прямом получении данных, находящихся в другой стране, не должны предъявляться к любым предприятиям или лицам без предварительного согласия этой страны.

5) Эффективность международного сотрудничества следует повысить путем создания механизмов быстрого реагирования в рамках международного сотрудничества, а также каналов связи через сотрудников по связи и ИТ-системы между национальными органами для трансграничного сбора доказательств и передачи электронных доказательств в режиме онлайн.

6) Государствам следует продолжать расширять сотрудничество в целях защиты важнейших объектов инфраструктуры и укреплять сети взаимодействия между группами по реагированию на чрезвычайные ситуации в компьютерной сфере (CERT и CSIRT).

7) Государствам следует рассмотреть вопрос о создании новаторских протоколов для обмена информацией, в том числе оперативными данными и доказательствами преступных деяний, в целях ускорения таких процедур.

8) Необходимо вновь подтвердить приверженность всех государств-членов делу обеспечения охраны и безопасности ИКТ путем использования их исключительно в мирных целях и активизации международных усилий по борьбе с любой злонамеренной деятельностью в киберпространстве во время серьезных кризисов на глобальном, региональном и местном уровнях.

9) Процедуры международного сотрудничества должны быть оптимизированы таким образом, чтобы максимальная помощь оказывалась в рамках возможностей, вытекающих из внутренней правовой базы, регулирующей просьбы о международном сотрудничестве, касающихся сохранения электронных доказательств, доступа к записанной в журнале информации и информации о регистрации пользователей, которая не нарушает права человека и основные свободы или имущественные права.

10) Странам рекомендуется уделять особое внимание необходимой соразмерности следственных действий с соблюдением основных свобод и режимов защиты личных данных, связанных с частной перепиской.

11) Международное сотрудничество в борьбе с киберпреступностью должно также учитывать гендерные и возрастные подходы и потребности уязвимых групп населения.

12) Что касается масштабов международного сотрудничества, то, хотя взаимная правовая помощь должна предоставляться только национальными органами власти, сотрудничество не должно ограничиваться государственными ведомствами, а должно также охватывать частный сектор, например, провайдеров

интернет-услуг (ПИУ). В этой связи было рекомендовано принять положения, допускающие прямое сотрудничество с ПИУ в других правовых системах в отношении просьб о предоставлении информации об абонентах, просьб об обеспечении сохранности данных и срочных просьб.

13) Варианты борьбы с киберпреступностью и защиты общества всегда должны обеспечивать соблюдение прав человека и конституционных гарантий и способствовать созданию более свободного, открытого, безопасного и жизнеспособного киберпространства для всех.

14) Странам рекомендуется упорядочить сотрудничество с этой отраслью и активизировать взаимодействие между государственными и частными поставщиками услуг, в частности в целях решения проблем, создаваемых вредоносными криминальными материалами в Интернете.

15) Частные компании, в частности ПИУ, несут совместную ответственность за предупреждение и расследование киберпреступлений. Такие компании должны ускорить и расширить свои отклики на просьбы об оказании правовой помощи, предлагать их в странах, где они расположены, и обеспечивать наличие соответствующих каналов связи с местными органами власти.

16) Необходимо укреплять публично-частные партнерства. В тех случаях, когда таких партнерств не существует, они должны создаваться, при этом частные компании должны участвовать в рабочих группах (многосторонних форумах) и в обсуждении вопроса об укреплении подхода к борьбе с киберпреступлениями.

17) Неправительственные организации и научные круги также должны принимать участие в усилиях по предупреждению киберпреступности и борьбе с ней, поскольку они обеспечивают всеохватывающую, плюралистическую и всеобъемлющую перспективу, в частности для обеспечения защиты прав человека, особенно свободы выражения мнений и неприкосновенности частной жизни.

18) Странам предлагается присоединиться к уполномоченным сетям специалистов-практиков, шире использовать и укреплять их в целях сохранения допустимых электронных доказательств и обмена ими, включая круглосуточную Сеть, специализированные сети по киберпреступности и каналы Интерпола для оперативного полицейского сотрудничества, а также сетевое взаимодействие со стратегическими партнерами-союзниками, с целью обмена данными по вопросам киберпреступности и создания условий для быстрого реагирования и сведения к минимуму утраты важнейших доказательств. В ходе мероприятий было также рекомендовано использовать полицейское сотрудничество и другие методы неофициального сотрудничества, прежде чем использовать каналы ВПП.

19) Каждое государство должно создать настоящий круглосуточный контактный центр, имеющий соответствующие ресурсы для содействия сохранению цифровых данных наряду с традиционной международной взаимопомощью по уголовным делам, опираясь на успешную модель замораживания данных в соответствии с Конвенцией Совета Европы.

20) Странам следует укреплять межучрежденческое сотрудничество и повышать операционную совместимость путем стандартизации запросов информации и процедур удостоверения подлинности, а также участия многих заинтересованных сторон.

21) Страны должны улучшить реализацию национальных законов и усилить внутреннюю координацию и взаимодействие для сбора и обмена информацией и доказательствами для целей судебного преследования.

22) Государствам следует активизировать меры по обмену финансовой или денежно-кредитной информацией, замораживанию счетов и конфискации активов для обеспечения того, чтобы преступники не могли пользоваться выгодами от преступной деятельности.

23) Государствам рекомендуется создавать совместные следственные группы с другими странами на двустороннем, региональном или международном уровнях в целях укрепления потенциала правоохранительных органов.

24) Государствам следует также обеспечивать эффективную работу с электронными доказательствами и их допустимость в суде, в том числе в тех случаях, когда они предназначены для иностранного государства или получены от него. В этой связи странам рекомендуется продолжать или начать усилия по реформированию законодательства в области борьбы с киберпреступностью и использования электронных доказательств, следуя положительным примерам и реформам во всем мире.

25) Рекомендуется разработать правовые рамки, включающие также аспекты экстерриториальной юрисдикции в отношении киберпреступлений.

26) Странам следует совершенствовать механизмы смягчения последствий конфликтов, а также решать проблемы, связанные с определением и возможностями расследования киберпреступлений.

27) Государствам следует работать над стандартизацией и распространением процедурных средств ускоренной подготовки данных и расширения поиска (таких, как распоряжения о предъявлении, а также распоряжения об ускоренном сохранении или трансграничном доступе и т. д.) в целях облегчения работы правоохранительных органов и их непосредственного сотрудничества с ПИУ и решения проблем, связанных с отслеживанием электронных доказательств и их надлежащим использованием.

28) Государствам следует содействовать разработке и стандартизации совместимых технических стандартов для цифровой криминалистической экспертизы и трансграничного поиска электронных доказательств.

29) Рекомендуется вкладывать средства в создание эффективного центрального органа по вопросам международного сотрудничества в уголовно-правовой сфере для обеспечения эффективности механизмов сотрудничества, в том числе в области борьбы с киберпреступностью; рекомендуется создать специальные подразделения для расследования киберпреступлений и удовлетворять просьбы о сохранении данных, поступающие от другого государства по круглосуточной сети (или в определенных обстоятельствах непосредственно от провайдера), с тем чтобы как можно быстрее обеспечить сохранность необходимых данных. Более оперативному получению данных может способствовать более глубокое понимание информации, необходимой для успешного выполнения просьбы об оказании ВПП.

30) Эффективное международное сотрудничество требует наличия национальных законов, устанавливающих процедуры, позволяющие осуществлять международное сотрудничество. В этой связи национальные законы должны разрешать международное сотрудничество правоохранительных органов.

31) Помимо внутреннего законодательства, международное сотрудничество в борьбе с киберпреступностью опирается как на официальное договорное сотрудничество, так и на традиционную помощь полиции. Когда мы обсуждаем новый документ по киберпреступности, важно, чтобы страны помнили о том, что новый документ не должен вступать в противоречие с существующими документами, которые уже позволяют многим странам осуществлять международное сотрудничество в режиме реального времени. В этой связи странам следует обеспечить, чтобы любой новый документ по киберпреступности не противоречил существующим договорам.

32) Устойчивое наращивание потенциала и оказание технической помощи в целях расширения возможностей во всех оперативных областях и укрепления потенциала национальных органов в области борьбы с киберпреступностью должны иметь приоритетное значение и расширяться, включая создание сетей, проведение совместных совещаний и учебных мероприятий, обмен

информацией о наилучших видах практики, учебными материалами и данными о типовых формах сотрудничества. Такое наращивание потенциала и подготовка должны включать в себя узкоспециализированную подготовку специалистов-практиков, которая способствует, в частности, участию женщин-экспертов и дополнительно учитывает потребности законодателей и лиц, ответственных за разработку политики, в более эффективном решении вопросов хранения данных для целей правоохранительной деятельности; сотрудников правоохранительных органов, следователей и аналитиков для повышения их способности проводить криминалистическую экспертизу и использовать открытые исходные коды при проведении расследований и в цепи обеспечения сохранности электронных доказательств, а также при сборе электронных доказательств и обмене ими; и судей, прокуроров, представителей центральных органов власти и адвокатов для эффективного рассмотрения и урегулирования соответствующих дел.

33) Настоятельно необходимо разработать адекватные и, по возможности, единообразные правила и сроки удержания/сохранения данных, с тем чтобы обеспечить возможность сохранения или получения электронных доказательств в поддержку дальнейших просьб об оказании ВПП.

34) Группа 77 и Китая признают, что международное сотрудничество имеет важное значение для сбора электронных доказательств и обмена ими в контексте трансграничных расследований и что необходимо оперативно и эффективно реагировать на просьбы об оказании взаимной правовой помощи, связанной с сохранением и получением электронных доказательств. Группа также подчеркивает, что в этом процессе должны соблюдаться принципы суверенитета и взаимности.

35) Группа 77 и Китая также призывают УНП ООН и далее представлять национальным правительственным экспертам программы по наращиванию потенциала и подготовке кадров в области борьбы с киберпреступностью в целях расширения возможностей по выявлению и расследованию киберпреступлений. Такая деятельность по наращиванию потенциала в этой области должна учитывать потребности развивающихся стран, обеспечивать уделение особого внимания уязвимостям каждой страны с целью оказания адресной технической помощи и содействовать обмену самыми современными знаниями в наилучших интересах специалистов-практиков и заинтересованных сторон.

36) УНП ООН разработало «Программу составления просьб об оказании взаимной правовой помощи» для оказания содействия специалистам-практикам системы уголовного правосудия в составлении просьб об оказании взаимной правовой помощи. УНП ООН также разработало «Практическое руководство по запрашиванию электронных доказательств в других странах», которое предоставляется по запросу правительственным специалистам-практикам в государствах-членах. Таким образом, страны могут извлечь пользу из использования этих важнейших документов, разработанных УНП ООН.

37) КППУП следует рассмотреть вопрос о продлении плана работы МГЭ на период после 2021 года в качестве форума для обмена информацией о киберпреступности между специалистами-практиками.

38) Некоторые выступавшие рекомендовали, чтобы согласование и принятие Конвенции Организации Объединенных Наций для поощрения сотрудничества в борьбе с киберпреступностью способствовали повышению эффективности международного сотрудничества в борьбе с киберпреступностью.

39) Экспертам УНП ООН в Вене было рекомендовано заниматься разработкой новой конвенции.

IV. Организация работы совещания (*продолжение*)

C. Заявления

2. С заявлениями выступили эксперты следующих государств-членов и государства со статусом наблюдателя, не являющегося государством-членом: Алжир, Аргентина, Армения, Бразилия, Государство Палестина, Государство Палестина от имени Группы 77 и Китая, Египет, Индия, Канада, Колумбия, Ливан, Мексика, Нидерланды, Норвегия, Португалия, Российская Федерация, Румыния, Соединенные Штаты Америки, Чили и Эквадор.