Организация Объединенных Наций E/CN.15/2018/6

Экономический и Социальный Совет

Distr.: General
22 February 2018
Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Двадцать седьмая сессия
Вена, 14–18 мая 2018 года
Пункт 5 предварительной повестки дня*
Тематическое обсуждение «Меры, принимаемые в системе уголовного правосудия с целью предупреждения киберпреступности во всех ее формах и борьбы с ней, в том числе путем укрепления сотрудничества на национальном и международном уровнях»

Руководство для тематического обсуждения «Меры, принимаемые в системе уголовного правосудия с целью предупреждения киберпреступности во всех ее формах и борьбы с ней, в том числе путем укрепления сотрудничества на национальном и международном уровнях»

Записка Секретариата

Резюме

Настоящее руководство для тематического обсуждения «Меры, принимаемые в системе уголовного правосудия с целью предупреждения киберпреступности во всех ее формах и борьбы с ней, в том числе путем укрепления сотрудничества на национальном и международном уровнях», которое будет проведено Комиссией по предупреждению преступности и уголовному правосудию на ее двадцать седьмой сессии, было подготовлено Секретариатом в соответствии с решением 18/1 Комиссии. В своем решении 2016/241 Экономический и Социальный Совет постановил, что основной темой двадцать седьмой сессии Комиссии будет тема «Меры, принимаемые в системе уголовного правосудия с целью предупреждения киберпреступности во всех ее формах и борьбы с ней, в том числе путем укрепления сотрудничества на национальном и международном уровнях». В настоящей записке предлагается ряд вопросов по соответствующим тематическим областям для проведения тематического обсуждения, ставятся некоторые проблемы с целью формирования структуры обсуждения и приводится справочная информация.

* E/CN.15/2018/1.

I. Введение

1. В своем решении 2016/241 Экономический и Социальный Совет постановил, что основной темой двадцать седьмой сессии Комиссии по предупреждению преступности и уголовному правосудию будет тема «Меры, принимаемые в системе уголовного правосудия с целью предупреждения киберпреступности во всех ее формах и борьбы с ней, в том числе путем укрепления сотрудничества на национальном и международном уровнях».

2. На своей возобновленной двадцать шестой сессии, проходившей 7 и 8 декабря 2017 года, Комиссия утвердила предложение Председателя относительно следующего подхода к организации тематического обсуждения на ее двадцать седьмой сессии: тематические прения будут проходить в ходе одного заседания в первой половине дня и одного заседания во второй половине дня. Прения в первой половине дня будут посвящены подтеме «Текущие проблемы», а прения во второй половине дня подтеме «Возможные меры реагирования на них».

3. Настоящая записка подготовлена Секретариатом в соответствии с решением 18/1 Комиссии под названием «Руководящие принципы проведения тематических обсуждений в Комиссии по предупреждению преступности и уголовному правосудию», в котором Комиссия постановила, что обсуждение главной темы будет проходить на основе руководства для дискуссий, содержащего перечень вопросов для рассмотрения участниками.

II. Справочная информация: подготовка почвы для проведения тематического обсуждения

4. Стремительное развитие Интернета и компьютерных технологий способствовало преобразованию обществ во всем мире, но также привело к появлению новых возможностей для совершения преступлений. Компьютеры, сети и данные могут быть связаны с совершением различного рода преступлений, причем эта связь может принимать почти любые формы. Они стали и объектами преступления, и орудиями его совершения, а также привели к возникновению новых мотивов и возможностей для расширения преступной деятельности. Они часто склоняют чашу весов, на одной чаше которых у преступника находятся риски, а на другой — выгода, в пользу последнего. Кроме того, вследствие лежащей в основе Интернета цифровой архитектуры, а также имеющегося глобального доступа к информационно-коммуникационным технологиям (ИКТ) киберпреступность связана с организованной преступностью и часто носит транснациональный характер[1].

5. В своей резолюции 65/230 Генеральная Ассамблея одобрила Салвадорскую декларацию о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире, принятую на двенадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, и просила Комиссию по предупреждению преступности и уголовному правосудию учредить, в соответствии с пунктом 42 Салвадорской декларации, 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

[1] *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations publication, Sales No. E.10.IV.6), p. 204; и *Всемирный доклад о наркотиках за 2017 год: Проблема наркотиков и организованная преступность, незаконные финансовые потоки, коррупция и терроризм* (Издание Организации Объединенных Наций, в продаже под № R.17.XI.11), стр. 17.

возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

6. Этот мандат был вновь подтвержден 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, которая была принята на тринадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и одобрена Генеральной Ассамблеей в ее резолюции 70/174.

7. Группа экспертов для проведения всестороннего исследования проблемы киберпреступности провела в общей сложности четыре совещания в 2011, 2013, 2017 и 2018 годах, соответственно. В своей резолюции 22/7 от 26 апреля 2013 года Комиссия по предупреждению преступности и уголовному правосудию приняла к сведению всестороннее исследование по киберпреступности, подготовленное Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) под эгидой Группы экспертов, и обсуждение его содержания на втором совещании Группы экспертов, проведенном в Вене 25–28 февраля 2013 года (см. UNODC/CCPCJ/EG.4/2017/3), на котором были высказаны различные мнения относительно содержания, выводов и вариантов, представленных в исследовании, и просила Группу экспертов, при необходимости при содействии Секретариата, продолжить работу по выполнению своего мандата.

8. В своей резолюции 26/4, принятой на ее двадцать шестой сессии 26 мая 2017 года, Комиссия по предупреждению преступности и уголовному правосудию 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 и Дохинской декларациями, а также просила Группу экспертов продолжать 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. В этой же резолюции Комиссия постановила, что Группа экспертов должна посвятить свои будущие совещания изучению на структурированной основе каждого из основных вопросов, изложенных в исследовании, без ущерба для других вопросов, включенных в ее мандат, с учетом, в надлежащих случаях, взносов, полученных во исполнение резолюции 22/7 Комиссии, и обсуждений на предыдущих совещаниях Группы экспертов.

9. В более широком контексте все большее признание, как это отражено в Повестке дня в области устойчивого развития на период до 2030 года, принятой Генеральной Ассамблеей в ее резолюции 70/1, получает тот факт, что исключительно важное значение для обеспечения устойчивого развития имеют уменьшение конфликтов, масштабов преступности, насилия и дискриминации и обеспечение широкого участия, благого управления и верховенства права. В этой связи особую значимость имеет цель 16 Повестки дня на период до 2030 года («Содействовать построению миролюбивого и открытого общества в интересах устойчивого развития, обеспечивать доступ к правосудию для всех и создавать эффективные, подотчетные и основанные на широком участии учреждения на всех уровнях»). Цель 16 связана с борьбой с киберпреступностью, которая, наряду с другими формами преступности, включая организованную преступность, подрывает принципы благого управления и верховенства права, ставит под угрозу безопасность и развитие и оказывает дестабилизирующее воздействие на государства-члены (см. E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1, пункт 4).

10. На четвертом семинаре-практикуме по теме «Современные тенденции в области преступности, последние изменения и свежие решения, в частности новые технологии как средство совершения преступлений и инструмент борьбы с преступностью», который будет проведен в рамках четырнадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию в Японии в апреле 2020 года, будут рассматриваться, среди прочего, такие вопросы как аспекты киберпреступности.

11. В свете вышеизложенного, на тематическом обсуждении по вопросу о киберпреступности, которое состоится в ходе двадцать седьмой сессии Комиссии, планируется проанализировать последние события. Тематическое обсуждение должно выступать в качестве платформы для дальнейшего обсуждения и обмена мнениями и опытом среди государств-членов. В целях содействия проведению тематического обсуждения были определены восемь тематических областей, имеющих отношение к киберпреступности, в том числе области, непосредственно охватываемые основной темой. Каждая из этих восьми тематических областей рассматриваются по отдельности в разделе III ниже, при этом текущие проблемы и возможные меры реагирования (как было согласовано на возобновленной двадцать шестой сессии Комиссии, см. пункт 2 выше), а также примерный список вопросов или тем для дальнейшего обсуждения приводится в отдельных подразделах.

III Тематические области: вопросы для обсуждения

A. Виды киберпреступлений и связанные с ними угрозы

Существующие проблемы

12. Понятие «киберпреступность» не является сугубо юридическим или криминалистическим термином, не является оно также и четко определенной или описанной категорией уголовных преступлений. Хотя было достигнуто общее согласие относительно перечня основных видов злоупотреблений и правонарушений, главным образом связанных с использованием компьютеров, однако помимо этого в настоящее время не существует глобального консенсуса относительно значения этого термина. Такая ситуация возникла вследствие широкого распространения компьютерных технологий и их многофункциональности, а также динамичного развития ИКТ и способов их использования с конца 1950-х годов.

13. В зависимости от контекста термин «киберпреступность» может относиться к преступлениям, совершаемым с помощью ИКТ, преступлениям, совершаемым в отношении объектов ИКТ и, собственно, в отношении их пользователей, или же может относиться к сценариям преступлений, в которых ИКТ играют косвенную или вспомогательную роль[2]. Термин «киберпреступность» используется для описания широкого круга преступлений, включая преступления в отношении компьютерных данных и систем (такие как хакерство), подлог и мошенничество с использованием компьютерных технологий (такие как фишинг), преступления, связанные с контентом (такие как распространение материалов, связанных с сексуальными надругательствами над детьми)[3], и преступления, связанные с нарушением авторских прав (такие как распространение пиратского контента).

14. Все более активное использование компьютерных технологий, наряду с тенденцией к оцифровке данных способствовало повышению значимости ком-

[2] Christopher Ram, “Cybercrime” in *Routledge Handbook of Transnational Criminal Law*, Neil Boister and Robert J. Currie, eds. (New York, Routledge, 2015), p. 379.

[3] См. United Nations Office on Drugs and Crime, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, (Vienna, 2015).

пьютерных данных. Вследствие этого компьютерные данные стали частой мишенью атак, принимающих различные формы: от воздействия на данные до информационного шпионажа. В настоящее время сформировалась развитая цифровая теневая экономика, ресурсом которой являются данные. Краденые персональные и финансовые данные — например, в целях получения доступа к действующим банковским счетам и кредитным картам и мошеннического создания новых кредитных линий — имеют денежное выражение. Такое положение дел является питательной средой для целого ряда различных преступных деяний, включая фишинг, фарминг, распространение вредоносного программного обеспечения и взлом корпоративных баз данных, осуществлению которых помогает полномасштабная инфраструктура, в которую входят разработчики вредоносных кодов, специализированные хостинг-провайдеры и отдельные лица, способные использовать сети взломанных компьютеров в целях проведения автоматизированных атак.

15. Так, в частности, краеугольным камнем большинства киберпреступлений по-прежнему являются разработка и распространение вредоносного программного обеспечения. С конца 2013 года программы-шифровальщики (программы-вымогатели, осуществляющие зашифровку данных криптографическим кодом) являются ведущим вредоносным программным обеспечением в плане создания угроз и последствий. По примеру программ, осуществляющих кражу информации, целью кампаний с использованием программ-шифровальщиков все чаще становятся структуры публичного и частного секторов[4].

16. Преступники постоянно ищут новые способы и технологии в целях повышения эффективности своих схем деятельности и увеличения прибыли. Анонимный характер онлайн-операций и использование криптовалют уменьшают риск обнаружения преступников правоохранительными органами. Расширение использования виртуальных частных сетей, «луковых» маршрутизаторов и шлюзов трансляции сетевых адресов операторского уровня (когда IP-адреса используются несколькими пользователями) ограничивает возможности следователей устанавливать связь между доказательствами и преступниками.

17. Масштабы киберпреступности растут параллельно с расширением Интернета, тем самым еще больше увеличивая уязвимость пользователей Интернета. Кроме того, эта угроза, которую создают различные формы киберпреступности, носит многоаспектный характер, а ее объектами все чаще становятся не столько граждане, сколько компании и правительства. Орудия совершения киберпреступлений представляют собой прямую угрозу безопасности и играют все более важную роль в содействии совершению большинства форм организованной преступности и терроризма.

Возможные меры реагирования

18. Беспрецедентные масштабы этой проблемы, а также многочисленные виды поведения, квалифицируемые в качестве киберпреступлений, ставят под угрозу способность властей принимать эффективные и результативные меры реагирования. В то же время киберпространство может также создавать новые возможности и обеспечивать инструментарий для выявления киберпреступлений. Использование ИКТ преступниками может обеспечить систему уголовного правосудия рядом «наводок» в плане расследования и получения доказательств. В настоящее время в распоряжении властей имеется больше данных о преступной деятельности, чем когда-либо ранее, и они, при использовании этой информации должным образом, могут сделать сбор оперативных данных и процедуры расследования эффективными с точки зрения затрат. В качестве интересного примера можно привести использование криптовалют в преступных целях. Операции с криптовалютами стали возможны благодаря технологии блокчейн. Несмотря на существующие в настоящее время технические и правовые пробелы в

[4] European Police Office, *European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (The Hague, 2017), p. 30.

технологии блокчейн, эта технология, благодаря ряду ее аспектов, может стать полезным инструментом в работе правоохранительных органов по отслеживанию ими подозрительных операций и обнаружению улик (см. E/CN.15/2018/CRP.1, пункт 164).

19. Опытные следователи в области цифровых технологий, прошедшие подготовку в рамках активизации усилий по наращиванию потенциала, способны получать электронные доказательства совершения киберпреступления, даже если преступники всячески стараются избегать оставлять цифровые следы или стирают их. В зависимости от времени хранения информации данные журнала выхода в Интернет позволяют установить время подключения к Интернету, а также источники получения данных и их адреса назначения.

20. Кроме того, ввиду все большей зависимости общества от Интернета и электронного общения правоохранительные органы разработали новые инструменты для расследования преступлений в режиме онлайн и стали использовать, например, программное обеспечение для выявления преступных схем. Правоохранительные органы также используют инструменты социальных сетей, чтобы улучшать отношения с местными общинами или призывать общественность к сотрудничеству в проведении уголовных расследований.

21. В этой связи чрезвычайно важно, чтобы государства рассмотрели вопрос о разработке многодисциплинарных стратегий с целью решения проблем и модернизации их потенциала для проведения успешного и эффективного расследования, а также судебного преследования по делам, связанным с киберпреступностью. Междисциплинарные стратегии могут варьироваться от принятия нормативных мер и директивных инициатив до предупреждения киберпреступлений и проведения подготовки компетентных органов, о чем говорится ниже.

Вопросы для обсуждения

22. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие уроки были извлечены из анализа меняющихся тенденций в области киберпреступности?

b) Как лучше всего использовать эти уроки для разработки эффективных нормативных мер реагирования и директивных стратегий по борьбе с киберпреступностью на национальном уровне?

c) Как различные виды киберпреступности влияют на способность государств-членов вести систематический учет соответствующих преступлений и осуществлять обмен информацией для целей правоохранительной деятельности на региональном и международном уровнях, в том числе информацией об участии организованных преступных групп, а также о методах деятельности таких групп и о методологических средствах, используемых в определении форм киберпреступности?

d) В какой степени содержащиеся в Конвенции Организации Объединенных Наций против транснациональной организованной преступности определения терминов «организованная преступная группа» и «структурно оформленная группа» применимы к киберпространству, в частности когда преступники, защита которых зачастую обеспечивается за счет анонимности, взаимодействуют друг с другом, не зная, кем является другой человек?

B. Правовые меры борьбы с киберпреступностью: аспекты, связанные с криминализацией

Существующие проблемы

23. При проведении оценки существующих проблем, связанных с разработкой правовых мер по противодействию киберпреступности, целесообразно учитывать, как эти проблемы возникали и обострялись на протяжении многих лет. Исторически сложилось так, что появление услуг, связанных с использованием компьютеров, и технологий, связанных с Интернетом, породило новые формы преступности вскоре после внедрения таких технологий. Одним из примеров является разработка в 1970-х годах компьютерных сетей, после чего вскоре произошел первый несанкционированный доступ к компьютерным сетям. Точно так же первые преступления, связанные с программным обеспечением, появились вскоре после появления в 1980-е годы персональных компьютеров, когда эти системы использовались для того, чтобы копировать программные продукты. К концу 1990-х годов сети стали одной из важнейших составляющих инфраструктуры ИКТ, что вызвало еще большую обеспокоенность в связи с угрожающими ей некоторыми формами киберпреступности. Это, в свою очередь, привело к необходимости обеспечивать кибербезопасность, а также в этой связи проявилась тенденция к введению уголовной ответственности или назначению наказания в особо строгой форме за совершение определенных видов атак на жизненно важную инфраструктуру[5].

24. Помимо новых определений и понятий, появление которых связано со стремительно развивающимися технологиями, существует насущный вопрос о том, каким образом рассматривать киберпреступность: в качестве нового явления и выделить совершенно новые составы преступления, связанные с этим явлением, или же попытаться применить существующие определения преступлений и, в случае необходимости, расширить или скорректировать их. Некоторые страны приняли новые законы, выделяющие компьютерное мошенничество в самостоятельный состав преступления, в то время как другие классифицировали незаконное копирование или повреждение данных, ограничение доступа к данным или ненадлежащее использование данных в качестве новых составов преступлений, ввиду того что существующие определения касаются только материального имущества. В качестве еще одного примера можно привести хищение личных данных, которое в некоторых юрисдикционных системах было выделено в отдельный состав преступления.

25. В тех случаях, когда предпочтительным является корректировка уже существующего уголовного законодательства, законодательные органы часто сталкиваются с длительными процедурами в целях пересмотра и обновления законодательства. Таким образом, основная трудность заключается в преодолении этих задержек, возникающих с момента обнаружения новых видов преступных злоупотреблений и заканчивая принятием законодательных поправок, необходимых для борьбы с ними. По мере того как растет скорость инноваций в области ИКТ, эта проблема становится важной и актуальной как никогда прежде.

Возможные меры реагирования

26. Надлежащее законодательство является основой расследования и уголовного преследования киберпреступлений. Таким образом, законодатели должны постоянно реагировать на развитие ИКТ и следить за эффективностью суще-

[5] См., в частности, Aunshul Rege-Patwardhan, “Cybercrimes against critical infrastructures: a study of online criminal organization and techniques”, *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 22, No. 3 (2009), p. 261; Luca Montanari and Leonardo Querzoni, eds., *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (March 2014). См. также резолюцию 2341 (2017) Совета Безопасности об угрозах международному миру и безопасности, создаваемых террористическими актами.

ствующих положений. Для определения пробелов и решения проблем, связанных с выполнением требования об обоюдном признании деяния уголовно наказуемым в контексте международного сотрудничества, необходим тщательный анализ существующих национальных законов. Законодательные органы также могут извлечь пользу из обязывающих и не обязывающих для исполнения многосторонних документов.

27. В целях обеспечения долгосрочного эффекта новые законы, по возможности, должны иметь гибкий и технологически нейтральный характер с учетом необходимости обеспечения правовой определенности и точности. В законах должна также решаться задача, связанная с необходимостью предоставления быстрого доступа к информации через национальные границы. Наконец, законодательные органы могут потребовать обеспечить достаточный объем подготовки и руководящих указаний, с тем чтобы они могли разрабатывать четкие положения и принимать эффективные законы.

Вопросы для обсуждения

28. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие уроки удалось извлечь из предпринимаемых на национальном уровне усилий, направленных на разработку законодательства, касающегося борьбы с киберпреступностью, и обеспечение его исполнения, а также на интеграцию этого законодательства в более широкую национальную стратегию по борьбе с киберпреступностью?

b) Обеспечивает ли национальное законодательство достаточную правовую основу для эффективного выявления, расследования и судебного преследования по фактам всех преступлений, связанных с киберпреступностью? Какие пробелы необходимо устранить?

c) Какое влияние оказывают действующие многосторонние документы на сферу охвата национальных правовых рамок в области борьбы с киберпреступностью? Удалось ли обеспечить согласованность национальных правовых мер реагирования, основанных на таких документах, и если да, то в какой степени?

d) Оказывает ли многообразие национальных подходов к введению уголовной ответственности за совершение киберпреступлений какое-нибудь влияние на масштабы международного сотрудничества в свете требования об обоюдном признании соответствующего деяния уголовно наказуемым?

C. Процессуальные полномочия и электронные доказательства

Существующие проблемы

29. Национальные следственные полномочия играют ключевую роль в сборе электронных доказательств. Обзор следственных полномочий на национальном уровне показал большое многообразие подходов к использованию электронных доказательств для расследования преступлений. Эти подходы объединяет то, что уже существующие полномочия могут истолковываться как применимые в отношении данных в качестве нематериальных доказательств и что для особенно интрузивных мер, например для расследований методами удаленной криминалистики, существуют юридические полномочия. Несмотря на различия в юридических полномочиях, необходимо обеспечить набор специальных следственных мероприятий, которые должны применяться для сбора электронных доказательств. Такие меры могут включать оперативное обеспечение сохранности компьютерных данных; постановления о предоставлении доступа к хранимым данным о контенте; постановления о предоставлении доступа к хранимым данным о потоках информации; постановления о предоставлении доступа к информации

об абонентах; сбор в режиме реального времени информации о контенте; сбор в режиме реального времени данных о потоках информации; досмотр компьютерного оборудования или хранимых на нем данных; выемка компьютерного оборудования или хранимых на нем данных; трансграничный доступ к компьютерной системе или данным; и использование средств удаленной компьютерно-технической экспертизы. С примерами национальных законов о следственных мероприятиях можно ознакомиться в Хранилище данных по киберпреступности УНП ООН и на информационно-справочном портале «Распространение электронных ресурсов и законов о борьбе с преступностью» (ШЕРЛОК). Следственные полномочия должны соответствовать уровню развития современных технологий. Эти полномочия должны осуществляться на основе правовых и институциональных рамок, способствующих своевременной и эффективной координации и сотрудничеству между частным сектором и соответствующими правительственными ведомствами на национальном, региональном и международном уровнях при соблюдении прав человека. Ввиду того что ИКТ затрагивают такие области, как неприкосновенность частной жизни и свободное выражение мнений, крайне важно, чтобы весомой составляющей этих рамок было соблюдение прав человека.

30. В идеале электронные доказательства должны быть приемлемы в рамках уголовного судопроизводства. Однако тот факт, что электронные доказательства приобретают все большее значение в уголовном производстве, вызывает прежде неизвестные проблемы. В частности, электронные доказательства весьма хрупки и могут быть легко изменены или удалены. Таким образом, одной из наиболее важных мер в компьютерно-технической экспертизе является обеспечение целостности электронных доказательств. Важно также гарантировать целостность данных в целях обеспечения точности и достоверности доказательств. Кроме того, для того чтобы электронные доказательства были приемлемы в рамках уголовного судопроизводства, их сбор должен осуществляться с помощью установленных процедур, обеспечивающих защиту прав человека.

31. Более того, сотрудничество правоохранительных органов с другими соответствующими субъектами, в том числе из частного сектора, приобретает в последние годы особенно важное значение для эффективного расследования киберпреступлений и сбора связанных с ними электронных доказательств. В целом операторы связи играют важную роль в обеспечении доступности электронных доказательств. На способность операторов предоставлять органам информацию в рамках расследований могут влиять нормы внутреннего законодательства о неприкосновенности частной жизни.

Возможные меры реагирования

32. С учетом того факта, что электронные доказательства неустойчивы, для обращения с ними, а также для обеспечения их подлинности и целостности необходимо установить определенные стандарты и требования. Эти стандарты и требования включают общие правила и процедуры, такие как ведение архивов, использование общепринятых технологий и привлечение квалифицированных экспертов к проведению расследований.

33. Для расследования увеличивающегося числа случаев киберпреступлений, в том числе случаев, связанных с надругательствами над детьми и их эксплуатацией, необходимы электронные доказательства, имеющиеся в распоряжении третьих лиц. Поэтому крайне важно, чтобы промышленный сектор и правительства работали сообща в целях разработки механизмов, предоставляющих правоохранительным органам своевременный доступ к данным в чрезвычайных ситуациях. Такие механизмы должны дополняться справедливыми и прозрачными правовыми процедурами для проведения обычных расследований.

34. Совещание группы экспертов, посвященное вопросу законного доступа к цифровым данным по всему миру, совместно организованное УНП ООН и Ис-

полнительным директоратом Контртеррористического комитета в сотрудничестве с Международной ассоциацией прокуроров, было проведено в Вене 12 и 13 февраля 2018 года. Цель этого совещания состояла в том, чтобы заложить основу для разработки практического руководства для центральных органов, прокуроров и следователей по получению электронных доказательств от иностранных юрисдикционных систем в ходе проведения трансграничных расследований, связанных с противодействием терроризму и организованной преступности. Это совещание дало возможность обменяться информацией о национальных законах и руководствах, а также реальными примерами дел, демонстрирующими получение опыта и извлечение уроков из получения электронных доказательств от операторов связи, находящихся в иностранных юрисдикционных системах.

Вопросы для обсуждения

35. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) С какими проблемами сталкиваются следственные органы при попытке обеспечить соблюдение требований по использованию специальных методов расследования, а также по сбору электронных доказательств и обмену ими в целях выявления и расследования киберпреступлений, а также уголовного преследования за их совершение, и какие успешные виды практики имеются в области реагирования на эти проблемы?

b) Какой опыт в области применимости таких доказательств в рамках судопроизводства получили государства-члены?

c) Каких результатов удалось достигнуть в области сотрудничества с финансовым сектором в сборе электронных доказательств, связанных с доходами от киберпреступности (как в случае с «денежными мулами»)?

d) Каковы главные проблемы — с точки зрения верховенства права и прав человека — в деле эффективного использования и внедрения методов, связанных с расследованием киберпреступлений и уголовным преследованием за их совершение?

e) Какие уроки удалось извлечь из усилий, направленных на укрепление сотрудничества между правоохранительными органами и операторами связи в целях получения электронных доказательств для выявления и расследования киберпреступлений, а также уголовного преследования за их совершение?

D. Вопросы юрисдикции

Существующие проблемы

36. В международном праве предусматривается ряд оснований для осуществления юрисдикции в отношении киберпреступлений, а также в первую очередь предусматриваются различные виды юрисдикции по территориальному принципу и по принципу гражданства. Некоторые из этих оснований могут быть закреплены в многосторонних документах по противодействию киберпреступности. В настоящее время основанием для расширенной или объективной территориальной юрисдикции часто является возникновение элемента состава преступления, его последствия или какая-либо иная значительная увязка с территорией государства. Кроме того, государства должны определить страну, в которой имеются наиболее благоприятные условия для уголовного преследования лиц, подозреваемых в совершении преступлений, на основе таких факторов, как местоположение доказательств или местонахождение преступников.

37. Применение целого ряда юрисдикционных основ разными странами может привести к тому, что на юрисдикцию для судебного преследования за совершение одного и того же киберпреступления будут претендовать несколько стран.

Риск возникновения коллизий юрисдикций еще более возрастает при применении принципа территориальности к случаям, когда то или иное государство не является местонахождением ни правонарушителя, ни потерпевшей стороны, но когда при совершении преступления использовалась инфраструктура этого государства.

38. Использование облачных вычислений создает целый ряд проблем для системы уголовного правосудия, в частности в том, что касается обеспечения соблюдения применимых законов и уголовной юрисдикции. Органам уголовного правосудия зачастую бывает неясно, в чьей юрисдикции находятся хранящиеся данные и какой правовой режим применяется к ним. Поставщик услуг может иметь свой головной офис в одной юрисдикционной системе, а подчиняться правовому режиму второй юрисдикционной системы, при этом данные хранятся в рамках третьей юрисдикционной системы. Одни и те же данные могут храниться в нескольких юрисдикционных системах при помощи технологии «зеркал», а также они могут перемещаться между юрисдикционными системами, тем самым еще больше усложняя эти проблемы.

39. Более того, зачастую неясно, кем является поставщик «облачных» услуг: контролером или обработчиком данных, принадлежащих пользователю, и, следовательно, неясно, чье законодательство применяется. Еще одним неясным моментом является вопрос о статусе данных — на хранении или в стадии передачи — и, следовательно, могут ли и на какой юрисдикционной основе выполняться распоряжения о предоставлении данных, проведении осмотра и выемки данных, а также о перехвате и сборе данных в режиме реального времени. Кроме того, нелокализованный характер облачного хранения данных создает проблемы для проведения онлайн-экспертизы и исследования в силу архитектуры «облака» (мультиарендность, распределение и дробление данных), а также в силу правовых проблем, связанных с обеспечением целостности и достоверности при сборе данных, контролем за хранением доказательств, правами собственности на данные или юрисдикцией[6].

Возможные меры реагирования

40. Во многих случаях несколько государств могут претендовать на юрисдикцию в отношении киберпреступлений, и поэтому важное значение имеет проведение консультаций для решения вопроса о том, какое государство должно осуществлять преследование. Это решение может быть сопряжено с юридическими, дипломатическими и практическими проблемами, такими как обоснованность юрисдикционных и других правовых требований каждого государства и вопроса о том, могут ли преступники быть выданы государству, желающему осуществлять уголовное преследование, а также прагматическими соображениями, такими как издержки и другие препятствия, стоящими на пути передачи доказательственной массы из одного государства в другое государство, обеспечения приемлемости доказательств в ходе процессуальных действий и фактического предъявления в суде. В случае возникновения юрисдикционных коллизий они обычно разрешаются с помощью проведения официальных и неофициальных консультаций между странами. Если принимается решение о том, что одно из нескольких возможных государств должно осуществлять преследование, то юрисдикция других государств фактически может быть передана. Передача уголовного производства, будучи отдельной формой международного сотрудничества, создает контекст и рамки для ее осуществления[7].

[6] Council of Europe, Cybercrime Convention Committee (T-CY), “Criminal justice access to data in the cloud: challenges”, discussion paper prepared by the T-CY Cloud Evidence Group, 26 May 2015, document T-CY (2015)10, pp. 10–14.

[7] См. справочный документ Секретариата о практических соображениях, успешных видах практики и трудностях, возникающих в области передачи уголовного производства как отдельной формы международного сотрудничества по уголовно-правовым вопросам (CTOC/COP/WG.3/2017/2).

41. Работа по укреплению международного и регионального сотрудничества в целях получения электронных доказательств проводится также на многосторонней основе. В июне 2017 года Комитет участников Конвенции Совета Европы о киберпреступности одобрил подготовку второго протокола к Конвенции о киберпреступности в целях введения четких правил и более эффективных процедур для получения электронных доказательств «в облаке» в ходе проведения конкретных уголовных расследований. Круг ведения был утвержден 8 июня 2017 года, а переговоры запланированы к проведению с сентября 2017 года по декабрь 2019 года.

Вопросы для обсуждения

42. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие критерии определяют юрисдикцию для целей осуществления мер, принимаемых в системе уголовного правосудия, в рамках дел, связанных с киберпреступностью? Каким образом эти критерии применяются к делам, связанным с облачным хранилищем данных, когда данные зачастую не «оседают в одном месте»?

b) Какой опыт был накоплен в ходе проведения консультаций по разрешению коллизий юрисдикций в отношении киберпреступлений? Какие существуют проблемы и успешные виды практики, и какие уроки были извлечены?

E. Межведомственная координация и сотрудничество на национальном уровне

Существующие проблемы

43. Многосторонние стратегии по противодействию киберпреступности являются важнейшим элементом борьбы с киберпреступностью. Юридические, технические и институциональные проблемы, созданные киберпреступностью, имеют серьезные последствия и могут быть решены только с помощью последовательной стратегии, учитывающей существующие инициативы и роли различных участников. Эффективная борьба с киберпреступностью требует наличия развитых организационных структур, позволяющих избежать дублирования, обладающих четко определенными полномочиями и способных координировать действия всех заинтересованных сторон, с тем чтобы они могли предпринимать согласованные действия. Без надлежащих структур проведение эффективных стратегий и программных инициатив будет чрезвычайно трудной задачей.

44. Сдерживание киберпреступности также является составной частью национальных стратегий в области кибербезопасности и защиты важнейшей информационной инфраструктуры. Речь идет, в частности, о принятии законодательства о противодействии неправомерному использованию ИКТ в преступных или иных целях и о борьбе с действиями, целью которых является подрыв целостности важнейшей национальной инфраструктуры. Сдерживание киберпреступности представляет собой общую ответственность, требующую скоординированных действий со стороны правительственных органов, частного сектора и граждан в целях предупреждения инцидентов, связанных с киберпреступностью, подготовки к ним, реагированию на них и восстановлению после них. Разработка и осуществление национальной стратегии по борьбе с киберпреступностью требует всеобъемлющего подхода, включающего сотрудничество и координацию в отношениях между соответствующими партнерами на институциональном уровне.

45. Тем не менее институциональная координация создает ряд трудностей, большинство из которых связаны с ресурсами и возможностями, которыми располагает каждая страна. Необходимо учитывать также некоторые другие факторы, включая степень поддержки частного сектора, например, посредством

публично-частных партнерств, или меры саморегулирования и самозащиты, которыми располагает частный сектор.

Возможные меры реагирования

46. Установление партнерств между несколькими ведомствами стало общепринятой практикой в деле борьбы с киберпреступностью, включая преступления в отношении детей с использованием технологических средств, на стратегическом уровне. В целях реагирования на многоаспектные проблемы, возникающие в ходе борьбы с киберпреступностью, операторам связи и публичным учреждениям, таким как правоохранительные органы и органы уголовного правосудия, необходимо создать публично-частные партнерства, в рамках которых они могут укреплять доверие и налаживать двусторонний диалог. В более широком плане может потребоваться принятие государствами регулирующих мер, которые выходят за рамки уголовного права и стимулируют активное участие частного сектора в предупреждении преступности. Такой подход может быть полезным для создания условий, позволяющих реагировать на возникающие угрозы и способствующих борьбе с ними.

47. Целевые группы по организованной преступности, использующей Интернет, могут быть полезным инструментом для принятия согласованных действий по борьбе с киберпреступностью. Такие целевые группы должны быть способны реагировать на меняющиеся криминальные реалии и способствовать созданию, например, большего числа постоянных групп для обмена информацией и специальных механизмов для проведения таких конкретных операций, как ликвидация бот-сетей. В любом случае власти должны обладать гибкостью для привлечения различных заинтересованных сторон, таких как правоохранительные органы, частный сектор, научные круги и группы пользователей, а также эффективно координировать с ними для достижения желаемого результата.

48. Интернет еще больше изменил фокус регулирования ИКТ в рамках работы правительств. Органы, регулирующие ИКТ, уже вовлечены в ряд мероприятий, направленных на решение проблемы киберпреступности. Это особенно актуально для таких сфер, как регулирование контента, безопасность информационных сетей и защита потребителей, поскольку пользователи стали более уязвимыми. Привлечение регулятивных органов к решению этих проблем было вызвано тем, что киберпреступность подрывает расширение сферы ИКТ и развитие сторон, предлагающих сопутствующие продукты и услуги. Новые функции и обязанности регулятивных органов ИКТ по борьбе с киберпреступностью можно рассматривать как часть более глобальной тенденции превращения централизованных моделей регулирования по борьбе с киберпреступностью в более гибкие механизмы[8].

Вопросы для обсуждения

49. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие проблемы встречаются на национальном уровне в деле укрепления институционального потенциала и межведомственной координации в целях борьбы с киберпреступностью?

b) Имеется ли какой-либо опыт разработки типовых рамочных основ или руководящих принципов, связанных с сотрудничеством между соответствующими заинтересованными сторонами на национальном уровне в целях предупреждения киберпреступности и борьбы с ней? Если да, то каким образом такие типовые рамочные основы или руководящие принципы способствовали укреплению реального сотрудничества?

[8] International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Geneva, 2012), p. 101.

F. Международное сотрудничество

Существующие проблемы

50. Помимо положений, касающихся введения уголовной ответственности за деяния киберпреступности и предоставления процессуальных полномочий, существующие документы могут содержать положения о механизмах международного сотрудничества при трансграничном расследовании киберпреступлений и преследовании за их совершение. Органы системы уголовного правосудия и правоохранительные органы сталкиваются со все большими проблемами в области международного сотрудничества в деле борьбы с киберпреступностью. Несмотря на теоретическую возможность идентификации местонахождения конкретного компьютера в конкретный момент времени, появление технологий «облачных» вычислений, зашифровки данных криптографическим кодом и децентрализованных сетей обмена информацией и средств хранения означает, что соответствующие данные могут существовать в нескольких копиях, распространяться между многими устройствами и местами нахождения и переноситься в другое географическое местоположение в течение нескольких секунд[9].

51. Учитывая, что электронные доказательства характеризуются неустойчивостью, для международного сотрудничества в деле борьбы с киберпреступностью требуется своевременное реагирование, включая обеспечение сохранности и предоставления данных поставщиками услуг, и способность запрашивать проведение специальных следственных мероприятий. К одной из проблем, часто встречающихся при запросе таких данных из других юрисдикционных систем, относятся задержки с реагированием на запросы, которые зачастую превышают срок хранения данных и могут позволить преступникам полностью уничтожить важнейшие электронные доказательства. К числу других часто встречающихся проблем относятся: отсутствие гибкости и готовности со стороны запрашиваемого органа, неопределенность, будет ли этот орган представлять доказательства в форме, которая может использоваться в уголовном производстве, и различия в определениях составов уголовных преступлений с точки зрения сотрудничающих государств[10].

52. На втором совещании Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, которое состоялось в 2013 году, большинство экспертов согласилось с тем, что для решения проблемы киберпреступности необходимо более широкое и оперативное международное сотрудничество, особенно в связи с тем, что масштабы этой проблемы по-прежнему растут, а зависимость от технологий, используемых в законных целях, приводит к тому, что возможная угроза киберпреступности приобретает все более серьезный характер. Кроме того, были высказаны разные мнения в отношении наилучшего стратегического подхода и приоритетов в области решения проблем, связанных с киберпреступностью[11]. В этой связи существуют разногласия в вопросе о том, следует ли разрабатывать новый универсальный правовой документ о противодействии киберпреступности, в котором, среди прочего, будут охватываться аспекты международного сотрудничества на глобальном уровне, или же международному сообществу следует и впредь опираться на существующие многосторонние документы, включая Конвенцию Совета Европы о киберпреступности.

---

[9] Справочный документ для семинара-практикума 3: «Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество» (A/CONF.222/12), пункт 32.

[10] См. справочный документ, подготовленный Секретариатом о сборе электронных доказательств и обмене ими (CTOC/COP/WG.3/2015/2), пункт 19.

[11] Ход обсуждений на втором совещании Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенном в Вене 25–28 февраля 2013 года, резюме Докладчика, UNODC/CCPCJ/EG.4/2017/3, пункт 25.

Этот вопрос по-прежнему остается открытым, и к настоящему времени достичь консенсуса по нему не удалось.

Возможные меры реагирования

53. Механизмы международного сотрудничества можно еще более улучшить путем изучения вопроса о возможных способах ускорения процедуры оказания взаимной правовой помощи. Другие решения могут заключаться в укреплении сотрудничества между правоохранительными органами и продолжении многостороннего диалога по вопросам транснационального доступа к компьютерным данным. В частности, введение отдельного режима доступа к сведениям об абонентах, как это определено в пункте 3 статьи 18 Конвенции Совета Европы о киберпреступности, в зависимости от типа запрашиваемых данных, может в значительной степени способствовать повышению эффективности оказания взаимной правовой помощи в таких вопросах, как киберпреступность и электронные доказательства[12].

54. Оптимизации процессов оказания взаимной правовой помощи, в том числе предоставлению электронных доказательств, могут способствовать такие новаторские решения, как включение модуля электронных доказательств в переработанную версию Программы составления просьб об оказании взаимной правовой помощи УНП ООН. Однако в то же время правоохранительные органы могут испытывать растущую потребность в нахождении новаторских методов сотрудничества в области проведения транснациональных расследований киберпреступлений. Особенно важным в этом отношении может оказаться участие в координации и поддержке транснациональных расследований, в том числе в содействии обмену информацией, в отношениях между национальными правоохранительными органами и такими структурами, как Глобальный инновационный комплекс Международной организации уголовной полиции (Интерпол) и Европейский центр по борьбе с киберпреступностью Европейского полицейского управления (Европол).

55. К прочим возможным решениям относятся: создание отдельных подразделений по борьбе с киберпреступностью в рамках центральных органов; мониторинг и изучение материалов судебных дел, связанных с оказанием взаимной правовой помощи, на предмет оперативности и эффективности, в том числе посредством ведения статистической информации, касающейся просьб об оказании взаимной правовой помощи, в том числе применительно к электронным доказательствам; более частое обращение к сотрудничеству между полицейскими органами в качестве полезного дополнения к другим формам оказания взаимной правовой помощи в целях обеспечения своевременного реагирования на просьбы об оказании помощи; проведение целенаправленной и более интенсивной подготовки кадров в целях расширения объемов предоставления взаимной правовой помощи, сотрудничества между полицейскими органами и других форм международного сотрудничества по таким вопросам, как киберпреступность и электронные доказательства; расширение обмена информацией и опытом между ежедневно и круглосуточно действующими сетями координаторов; и выделение ресурсов на уровне национальных органов, на которые возложена задача по выполнению просьб о взаимной правовой помощи, а также повышение координации их действий с центральными органами в целях своевременного реагирования.

[12] См. Council of Europe, Cybercrime Convention Committee, Cloud Evidence Group, “Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY”, document T-CY (2016)5, p. 13.

Вопросы для обсуждения

56. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Как повысить оперативность процедур оказания взаимной правовой помощи в делах, связанных с киберпреступностью и электронными доказательствами? Какие существуют наилучшие виды практики и какие проблемы возникают на пути сотрудничества между полицейскими органами при получении электронных доказательств за границей?

b) Какими примерами государства могут проиллюстрировать, как активизация обмена информацией на региональном и международном уровнях способствовала укреплению потенциала для выявления и оценки рисков, а также эффективного и своевременного реагирования на них?

c) Как должны подготавливаться, передаваться и обрабатываться международные запросы о сохранении электронных доказательств? Какой опыт был получен в рамках сотрудничества между публичным и частным секторами в этой области?

G. Предупреждение киберпреступности

Существующие проблемы

57. Издержки и трудности, связанные с расследованием и уголовным преследованием киберпреступлений, свидетельствуют о том, что выгоды от усилий по сотрудничеству в области предупреждения киберпреступности могут быть значительными. В частности, центральным элементом в деле предупреждения киберпреступности является публично-частное партнерство. Поставщики услуг могут содействовать предупреждению киберпреступности посредством a) хранения данных пользователей, доступ к которым сотрудники правоохранительных органов могут получить при наличии ордера в целях использования таких данных в ходе расследования киберпреступлений; и b) проведения активной фильтрации Интернет-сообщений и контента в целях предупреждения киберпреступлений, до того как те будут совершены. После анализа этих двух мер в контексте свободы слова выяснилось, что в связи с ними возникают многочисленные проблемы.

58. При обсуждении роли поставщиков услуг в деле предупреждения киберпреступности, возможно, потребуется рассмотреть вопрос о их ограниченных полномочиях как субъектов частного сектора. Во-первых, стратегии поставщиков зачастую часто меняются и характеризуются отсутствием предсказуемости для сотрудников правоохранительных органов, а также для потребителей. Поставщики услуг могут изменить свою стратегию в одностороннем порядке в любое время без предварительного уведомления сотрудников правоохранительных органов. В дополнение к этому стратегии и практика значительно варьируются не только от поставщика к поставщику, но также в отношении разных государств-членов. Поставщик может отвечать на многочисленные просьбы от одной страны, но совсем не отвечать или только отвечать на некоторые просьбы от другой, при этом практика другого поставщика может быть диаметрально противоположной[13].

59. Во-вторых, ход полицейских расследований киберпреступлений может затруднять гарантии защиты данных, которые требуют удалять персональные данные, если они более не требуются для тех целей, для которых они были собраны. Таким образом, хотя законы о хранении данных могут представлять прагматический подход к обеспечению того, чтобы операторы связи могли играть более

[13] Ibid., “Criminal justice access to data in the cloud: Cooperation with ‘foreign’ service providers”, (T-CY (2016)2), p. 22.

значительную роль в предупреждении киберпреступности посредством расширения объемов сотрудничества с правоохранительными органами, важно, чтобы такие законы осуществлялись с соблюдением должных процессуальных гарантий и обеспечивали защиту личных данных. Необходимо учитывать стандарты и нормативные положения о защите данных, в том числе общий регламент Европейского союза по защите данных[14].

60. Научное сообщество сталкивается с серьезной проблемой, связанной с заполнением большого числа пробелов, которые существуют и продолжают появляться в знаниях о киберпреступности, в частности о сексуальной эксплуатации детей и надругательствах над ними с использованием ИКТ. При условии наличия устойчивого финансирования, а это во многих юрисдикционных системах представляет собой значительную проблему, научные организации могут выполнять разнообразные функции в деле предупреждения киберпреступности, в том числе посредством обучения и профессиональной подготовки специалистов, разработки законодательной базы и политики, а также подготовки технических стандартов и выработки решений.

Возможные меры реагирования

61. К числу успешных видов практики в области предупреждения киберпреступности относятся принятие законов, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, создание прочной базы знаний и сотрудничество между органами власти, общинами, частным сектором и государствами. Исключительно важно обеспечивать помощь в разработке и совершенствовании методов предупреждения, обмен информацией об извлеченных уроках и наилучших видах практики и обмен информацией, необходимой для разработки методов предупреждения и обеспечения их эффективности.

62. Информационно-просветительские кампании и инициативы, в том числе кампании по вопросам новых угроз и кампании, ориентированные на конкретные целевые группы, например детей, были отмечены в качестве важного компонента стратегий по предупреждению киберпреступности[15]. Инициатива «Образование во имя правосудия», один из основных компонентов Глобальной программы по осуществлению Дохинской декларации, проводимой в рамках УНП ООН, включает в себя подготовку и распространение материалов по борьбе с киберпреступностью для детей и молодежи в начальных, средних и высших учебных заведениях.

63. Гражданское общество может играть жизненно важную роль, помогая детям понять и преодолеть онлайн-риски, что имеет особенно большое значение в контексте усилий по предупреждению случаев надругательства над детьми и их эксплуатации с использованием ИКТ. Такие методы, как просвещение и оказание превентивной психосоциальной помощи, признаются в качестве важного элемента защиты детей от надругательства над ними и их эксплуатации с использованием ИКТ. Просветительские инициативы позволяют детям, их семьям и другим лицам, осуществляющим уход, понимать и правильно оценивать риски, связанные с ИКТ[16].

64. Существует ряд моделей публично-частного партнерства, например между правоохранительными органами и операторами связи, способствующих предупреждению киберпреступности. Многие из них построены на обмене информацией на основе четких правил, доверия, ограниченного членства и поощрения взаимной выгоды и ответной реакции. Кроме того, будет расти роль частного

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*Official Journal of the European Union*, L 119, 4 May 2016, pp. 1–88).

[15] См. *Study on the Effects of New Information Technologies*, p. 54.

[16] Ibid., p. 54.

сектора в деле выявления и блокирования, среди прочего, онлайн-материалов, связанных с сексуальными надругательствами над детьми, до того, как клиенты смогут получить к ним доступ[17].

65. Правительства могут избрать четкий и перспективный подход, который будет заключаться в сотрудничестве с теми, кто в будущем будет оказывать влияние на предпринимательскую и рабочую среду, с тем чтобы все заинтересованные стороны могли более точно прогнозировать изменения в области преступной деятельности и неправомерного использования технологий. В этой связи чрезвычайно важно продолжать расширять знания о поведении современного киберпреступника посредством анализа оперативных данных, криминологического исследования и методов профилирования в целях более эффективного использования имеющихся ресурсов и заблаговременного определения характеристик будущих коммуникационных технологий, уязвимых с точки зрения эксплуатации в преступных целях.

Вопросы для обсуждения

66. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие примеры могут привести государства относительно эффективных стратегий по предупреждению киберпреступности в том, что касается соответствующих заинтересованных участников? По каким критериям определяется и оценивается успех?

b) Каким образом научные учреждения, частный сектор и неправительственные организации могут наиболее эффективно содействовать формированию знаний, разработке законодательства и стратегий в области киберпреступности и обмениваться ими?

c) Какой опыт получили государства-члены в области обеспечения баланса между защитой данных и эффективностью расследования киберпреступлений?

H. Наращивание потенциала и техническая помощь

Существующие проблемы

67. Важнейшую роль играет наращивание потенциала на уровне национальных правоохранительных органов и систем уголовного правосудия. Хотя большинство стран приступили к созданию специализированных структур для расследования киберпреступлений и преступлений, сопряженных с электронными доказательствами, во многих странах эти структуры не получают достаточного финансирования и страдают от отсутствия достаточных возможностей. Поскольку электронные доказательства крайне необходимы при расследовании киберпреступлений, правоохранительным органам, возможно, требуется проводить четкое различие между возможностями следователей по киберпреступлениям и возможностями лабораторий цифровой криминалистики, а также установить для них четкую сферу ответственности. Оперативные сотрудники правоохранительных органов, возможно, испытывают растущую потребность в приобретении и использовании таких базисных навыков, которые используются для составления обоснованного экспертно-криминалистического описания устройств для электронного хранения данных.

68. В целом очевидно, что наращивание потенциала правоохранительных органов и органов уголовного правосудия в области борьбы с киберпреступностью будет постоянным и непрерывным процессом, учитывая, что продолжают

[17] См., например, The Netclean Report 2017, доступный по https://www.netclean.com/netclean-report-2017.

быстро появляться новые технологии и новые методы совершения преступлений.

Возможные меры реагирования

69. Техническая помощь и сотрудничество имеют важное значение для обеспечения обмена информацией об эффективных следственных методах, опыте и новых технологиях. Государства-члены, возможно, пожелают расширить обмен информацией о новых подходах к расследованию сложных случаев финансового мошенничества через Интернет, онлайнового незаконного оборота наркотиков или использования виртуальных валют для отмывания денег, что позволит создать условия для срочного приобретения сотрудниками правоохранительных органов во многих странах навыков, необходимых для борьбы с возникающими угрозами, связанными с киберпреступностью.

70. При наличии в правоохранительных органах специальных структур или подразделений по борьбе с киберпреступностью государствам легче концентрировать в одном месте ограниченные ресурсы для освоения специальных методов расследования, а также для сбора и анализа достаточных электронных доказательств, в том числе для проведения цифровой криминалистической экспертизы. В то же время такие структуры и подразделения могут обучать сотрудников местных правоохранительных органов, координировать принимаемые на национальном уровне меры по противодействию киберпреступности, содействовать взаимодействию партнеров, участвующих в расследованиях, и собирать информацию о таких формах киберпреступности, которые могут вызывать особую обеспокоенность государства.

71. В соответствии с резолюцией 65/230 Генеральной Ассамблеи и резолюциями 22/7 и 22/8 Комиссии по предупреждению преступности и уголовному правосудию УНП ООН в рамках его Глобальной программы борьбы с киберпреступностью было поручено помогать государствам-членам в их усилиях по противодействию киберпреступности посредством наращивания потенциала и оказания технической помощи. В рамках этой Программы УНП ООН оказывает, главным образом в развивающихся странах, целенаправленную техническую помощь в деле наращивания потенциала, предупреждения преступлений и повышения уровня осведомленности, а также в деле международного сотрудничества и анализа в вопросах борьбы с киберпреступностью. УНП ООН также оказывает, по просьбе и в рамках своего мандата, законодательную помощь нуждающимся в ней государствам-членам.

72. Так, например, УНП ООН разработало курс подготовки инструкторов для расследований, связанных с криптовалютами, и организует его в различных регионах. Цель курса состоит в укреплении потенциала сотрудников правоохранительных органов, аналитиков, прокуроров и судей в области криптовалют, отслеживания биткойнов в рамках финансовых расследований, локализации информационных ресурсов и международного сотрудничества по изучению материалов судебных дел.

Вопросы для обсуждения

73. Комиссия, возможно, пожелает рассмотреть следующие вопросы для дальнейшего обсуждения:

a) Какие аспекты мер и стратегий, связанных с киберпреступностью, являются приоритетными для оказания технической помощи и наращивания потенциала, в частности, с учетом меняющегося характера киберпреступности, а также новых и появляющихся угроз, связанных с ней?

b) Какие уроки были извлечены из обмена информацией об успешных следственных методах, опыте и новых технологиях в качестве примера сотрудничества в деле оказания технической помощи?

c) Как можно наилучшим образом налаживать и продвигать взаимодействие и сотрудничество между международными организациями, оказывающими техническую помощь в вопросах киберпреступности, в целях результативного и устойчивого оказания государствам-членам, нуждающимся в помощи, услуг в области наращивания потенциала?

IV. Устранение существующих пробелов: путь вперед

74. Международное сообщество прилагает все больше усилий в целях лучшего понимания угроз, которые создает киберпреступность, и реагирования на них. Тем не менее крайне необходимо проделать дополнительную работу, поскольку сохраняются серьезные проблемы в области разработки и осуществления всеобъемлющих, скоординированных, устойчивых и эффективных мер по борьбе с киберпреступностью.

75. Содействуя проведению тематического обсуждения на своей двадцать седьмой сессии, Комиссия в ходе обсуждения соответствующего пункта повестки дня будет служить в качестве платформы для обмена информацией, наилучшими видами практики и извлеченными уроками, обеспечивая разработку эффективных мер реагирования и содействуя применению соответствующих международных документов или стандартов в области борьбы с киберпреступностью.

76. При рассмотрении дальнейших действий по решению проблем, создаваемых киберпреступностью, и дальнейших шагов по разработке соответствующих мер реагирования Комиссия, возможно, пожелает уделить пристальное внимание обсуждению тех областей действующих национальных правовых и институциональных рамок, которые, как считается, представляют наибольшую опасность, а также обсуждению приоритетных областей, в которых государства-члены сталкиваются с наибольшими трудностями.

77. Комиссия может рассмотреть вопрос о том, чтобы рекомендовать государствам-членам активизировать усилия по наращиванию потенциала и укрепить нормативно-правовую базу, в частности, при пересмотре действующих национальных стратегий, законов и институциональных рамок с целью определения новых или измененных законодательных положений, институциональных рамок и практических методов, которые могли бы содействовать укреплению их потенциала в деле преодоления текущих или возникающих угроз, связанных с киберпреступностью.

78. Комиссия может определить — и установить их приоритетность — те области технической помощи, которыми УНП ООН могло бы заняться в тесном сотрудничестве и координации с другими соответствующими сторонами, на основе соответствующих мандатов, в целях оказания государствам-членам более эффективной поддержки во внедрении национальной политики, законодательства и институционального потенциала для решения текущих и возникающих проблем, связанных с киберпреступностью.

79. Кроме того, Комиссия, возможно, пожелает предложить УНП ООН содействовать поддержанию связи с другими межправительственными органами по противодействию киберпреступности и осуществлению мер, принимаемых в системе уголовного правосудия, с целью предупреждения киберпреступности и борьбы с ней, включая Конференцию участников Конвенции об организованной преступности и ее Рабочую группу по вопросам международного сотрудничества, в рамках их соответствующих мандатов и надлежащим образом.