Конференция участников Конвенции Организации Объединенных Наций против транснациональной организованной преступности

Distr.: General
18 August 2015
Russian
Original: English

Рабочая группа по вопросам международного сотрудничества
Вена, 27 и 28 октября 2015 года
Пункт 2 предварительной повестки дня*
Сбор электронных доказательств и обмен ими

Сбор электронных доказательств и обмен ими

Справочный документ, подготовленный Секретариатом

I. Введение

1. Преступления, сопряженные с электронными доказательствами, создают особые сложности для органов, которым поручено должным образом реагировать на них как на национальном уровне (законодатели, следователи, прокуроры и судьи), так и в рамках международного сотрудничества.

2. В целом электронные доказательства могут включать любые созданные или хранимые в цифровой форме данные во всех случаях, когда используется компьютер. К таким данным относится информация, вносимая ручным способом каким-либо лицом в электронное устройство; информация, вырабатываемая при вычислительной операции или реагировании каким-либо лицом на запрос, когда электронное устройство генерирует информацию в режиме автомата; или вырабатываемая и хранимая информация в тех случаях, когда устройство обрабатывает информацию в рамках своей матрицы. Таким образом, электронные доказательства представляют собой любую информацию, регистрируемую, генерируемую или хранимую в базах данных, операционных системах, прикладных программах, компьютерных моделях с экстраполированными результатами, электронных и голосовых почтовых сообщениях и даже командах, пребывающих в инертном состоянии в блоках памяти компьютера[1].

3. Настоящий документ был подготовлен Секретариатом в качестве справочного материала по ключевым концепциям и аспектам, касающимся

* CTOC/COP/WG.3/2015/1.

[1] Ireland Law Reform Commission, “Documentary and Electronic Evidence”, Consultation paper, December 2009, p. 8.

электронных доказательств, чтобы облегчить обсуждение Рабочей группой соответствующего пункта повестки дня ее совещания.

II. Сбор электронных доказательств и обмен ими: области для рассмотрения и принятия мер на национальном и международном уровнях

4. Учитывая тесную взаимосвязь между сбором электронных доказательств и обменом ими, внутреннее законодательство и региональные и международные соглашения или договоренности часто предусматривают следственные полномочия для осуществления сбора электронных доказательств и механизмы сотрудничества для обмена ими.

A. Сбор электронных доказательств

1. Национальные правовые системы

5. Обычно уголовно-процессуальное законодательство содержит положения о сборе и допустимости доказательств. Что касается доказательств в электронной форме, то компьютерные данные и электронные записи могут быть с легкостью изменены. Поэтому сбор электронных доказательств и обращение с ними должны осуществляться таким образом, чтобы гарантировать их целостность, подлинность и неизменность на протяжении всего периода времени с момента их сбора до использования в суде.

a) Правомочия осуществлять сбор электронных доказательств и оперировать ими

6. Важнейшую роль в сборе электронных доказательств играют полномочия национальных следственных органов. Как указано в подготовленном УНП ООН исследовании по киберпреступности, для эффективного проведения расследований и сбора электронных доказательств государства могут принять процессуальное законодательство, предоставляющее полномочия соответствующим правоохранительным органам. Возможен целый спектр полномочий на проведение расследований: от традиционных процессуальных полномочий, широко толкуемых общих следственных полномочий и общих полномочий на проведение расследований, связанных с применением методов киберкриминалистики, до всеобъемлющих следственных полномочий, применяемых для получения электронных доказательств[2].

7. В исследовании по киберпреступности отмечено также, что анализ правовой основы для полномочий на расследование преступлений, связанных с электронными доказательствами, свидетельствует о наличии самых разнообразных подходов на национальном уровне. Одну часть таких подходов

[2] UNODC, Comprehensive Study on Cybercrime: Draft – 2013 (УНП ООН, "Всестороннее исследование по киберпреступности: проект – 2013 год"), подготовленный УНП ООН документ для рассмотрения Группой экспертов для проведения всестороннего исследования по киберпреступности (www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf), Chapter 5, p. 125.

объединяет то, что "традиционные" полномочия могут истолковываться как применимые к виртуальным данным, а другую часть то, что для связанных с проникновением особых мер, например для расследований методами удаленной криминалистики, существуют юридические полномочия.

8. Тем не менее, несмотря на различия в юридических полномочиях, между государствами, представившими материалы для исследования по киберпреступности, по-видимому, существует довольно широкий консенсус относительно перечня следственных мероприятий, которые должны применяться для сбора электронных доказательств. Такие мероприятия могут включать оперативное обеспечение сохранности компьютерных данных; распоряжения о предоставлении хранимых данных о контенте; распоряжения о предоставлении хранимых данных о трафике; распоряжения о предоставлении информации о подписчиках; сбор данных о контенте в реальном времени; сбор данных о трафике в реальном времени; поиск компьютерных аппаратных средств или компьютерных данных; изъятие компьютерных аппаратных средств или компьютерных данных; трансграничный доступ к компьютерной системе или данным; и использование средств удаленной технико-криминалистической экспертизы[3].

9. 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 поставщики услуг интернета (ПУИ) играют важную роль в обеспечении доступности электронных доказательств. На способность ПУИ предоставлять соответствующим органам информацию в ходе расследований влияют также нормы внутреннего законодательства о неприкосновенности частной жизни. Например, государства могут вводить ограничения в отношении категорий данных, к которым может предоставляться доступ, устанавливать предельные сроки, предусматривать требования в отношении наличия достаточных оснований, а также надзор со стороны органов прокуратуры и судебных органов[4]. Вследствие существующих во внутреннем законодательстве норм, охраняющих неприкосновенность частной жизни, ПУИ должны отказывать в предоставлении информации о личных данных подписчика, данных о контенте и данных о трафике. Помимо норм внутреннего законодательства, международное право в области прав человека устанавливает определенные стандарты в отношении прав на неприкосновенность частной жизни лиц, в отношении которых правоохранительные органы проводят расследования.

10. Учитывая важную роль ПУИ в сборе электронных доказательств, Совет Европы принял "Руководящие принципы сотрудничества между правоохранительными органами и поставщиками услуг Интернета в борьбе с киберпреступностью". Эти руководящие принципы призваны содействовать выстраиванию надлежащего взаимодействия правоохранительных органов и

---

[3] Примеры норм внутреннего законодательства, касающихся этих следственных мероприятий, приведены в разделах Cybercrime Repository (http://cybrepo.unodc.org) и SHERLOC (http://sherloc.unodc.org).

[4] Cybercrime Study, Chapter 5, p. 134.

ПУИ при решении проблем киберпреступности. Эти руководящие принципы являются гибкими и могут применяться в любой стране в соответствии с внутренним законодательством и при соблюдении основополагающих прав граждан. Правоохранительным органам и ПУИ рекомендуется, в частности, участвовать в обмене информацией; содействовать привитию культуры сотрудничества; разработать письменно оформленный порядок взаимодействия; рассмотреть возможность установления официальных партнерских отношений; и защищать основополагающие права граждан[5].

b) Наращивание потенциала правоохранительных органов и систем уголовного правосудия в области обращения с электронными доказательствами

11. Электронные доказательства по своей природе являются легко разрушаемыми. При ненадлежащем обращении или изучении они могут быть изменены, повреждены или уничтожены. Поэтому для документирования, сбора, сохранения и анализа такого рода доказательств следует принимать особые меры предосторожности. При несоблюдении таких мер электронные доказательства могут прийти в негодность или могут быть сделаны неверные выводы.

12. В этой связи 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 цифровые доказательства все более широко используются при расследовании "обычных" преступлений, правоохранительным органам, возможно, необходимо 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, также испытывают растущую потребность в приобретении и использовании таких базисных навыков, которые используются для составления обоснованного экспертно-криминалистического описания устройств для электронного хранения данных.

13. Поскольку при совершении преступлений, сопряженных с электронными доказательствами, широко используются технологические новшества, такие как анонимизирующие сети, криптостойкое шифрование и виртуальные валюты, следователям также придется использовать новые стратегии. Например, правоохранительным органам, возможно, следует активизировать партнерские отношения с научно-исследовательскими группами, которые занимаются разработкой технических методологий в таких областях, как

[5] Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, размещены на сайте www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

характеризация и анализ операций с виртуальной валютой[6]. Кроме того, следователям, возможно, необходимо учитывать то, каким образом специальные методы расследования, такие как слежка, секретные операции, использование осведомителей и проведение контролируемых поставок в случае продажи запрещенных товаров через интернет, могут использоваться вместе с интернет-расследованиями и методами цифровой криминалистической экспертизы для сбора деликатных и легко разрушаемых электронных доказательств. В целом очевидно, что наращивание потенциала правоохранительных органов и органов уголовного правосудия в области борьбы с киберпреступностью и/или преступлениями, сопряженными с электронным доказательствами, будет постоянным и непрерывным процессом, учитывая, что продолжают быстро появляться новые технологии и новые методы совершения преступлений[7].

c) Роль специальных структур или подразделений по борьбе с киберпреступностью: внутригосударственные подходы

14. Создание национальных правоохранительных органов, специализирующихся на расследовании киберпреступлений и/или преступлений, сопряженных с электронными доказательствами, становится широко распространенной практикой и имеет важнейшее значение для содействия сбору и анализу электронных доказательств и обмену ими. Такая специализация в первую очередь обусловлена особым характером киберпреступности, в связи с которым существуют определенные трудности, касающиеся квалификации преступлений, применимости законов и сбора и анализа доказательств. В этой связи эффективность деятельности в области предупреждения преступности и уголовного правосудия в рамках борьбы с киберпреступностью будет непосредственно зависеть от технической квалификации и потенциала правоохранительных органов[8]. Кроме того, по мере все более широкого применения в повседневной жизни электронных устройств, интернета и глобальных средств связи использование электронных доказательств, таких как текстовые сообщения, сообщения по электронной почте и данные просмотра интернета, становится общепринятой практикой при проведении многих обычных уголовных расследований[9]. В результате все более необходимым становится также то, чтобы правоохранительные органы на всех уровнях (местном или национальном) располагали по меньшей мере базовыми возможностями для расследования киберпреступлений.

---

[6] См., например, Sarah Meiklejohn and others, “A fistful of bitcoins: characterizing payments among men with no names”, in *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2013).

[7] Тринадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, подготовленный Секретариатом справочный документ к семинару-практикуму 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия и появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество, A/CONF.222/12, пункты 37 и 38.

[8] Cybercrime Study, Chapter 5, p. 152.

[9] См. сноску 7 выше, A/CONF.222/12, пункт 16.

15. В исследовании проблем киберпреступности наиболее часто упоминается такая деятельность по оказанию технической помощи, как обучение методам расследования кибепреступлений. Из стран, которым требуется помощь, 60 процентов указали на то, что в помощи нуждаются правоохранительные органы[10]. Государства, представившие материалы для исследования по киберпреступности, сообщили также о том, что во многих случаях местные полицейские участки передают дела, связанные с киберпреступлениями, в специальный правоохранительный орган, занимающийся такими делами на государственном уровне[11].

16. 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 и надлежащего сбора и анализа 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, могущих вызывать особую обеспокоенность государства, как надругательство над детьми в режиме онлайн, преступления с использованием личных данных, мошенничество и аферы в интернете и т.д.

d) Приемлемость электронных доказательств в судах

17. Собранные и представленные электронные доказательства в принципе должны быть приемлемы в рамках уголовного судопроизводства. Доказательственное право традиционно полагалось на бумажную документацию, хотя при этом устные показания и физические предметы всегда были частью судебных разбирательств. Однако все большее значение в уголовном производстве приобретают электронные доказательства, что вызывает прежде неизвестные проблемы, и в этой связи обзорное исследование по киберпреступности было призвано отразить национальные правовые подходы к вопросу допустимости таких доказательств в судах по уголовным делам.

18. В этом контексте 85 процентов представивших ответы стран сообщили о допустимости электронных доказательств в уголовном производстве. Большинство стран, признающих допустимость электронных доказательств, сообщили, что такие доказательства рассматриваются в том же порядке, что и вещественные доказательства. Менее 40 процентов стран сообщили о существовании юридически значимых различий между электронными и вещественными доказательствами. Лишь несколько стран сообщили о существовании специальных законов, касающихся доказательности, которые регулируют использование электронных доказательств. Действующие в этих странах законы охватывают такие области, как юридические гипотезы, касающиеся собственности или авторства электронных данных и документов, а

[10] Cybercrime Study, Executive Summary, p. xxiii.
[11] Cybercrime Study, Chapter 5, p. 118.

также обстоятельств, при которых электронные доказательства могут считаться подлинными[12].

2. Международное сотрудничество

19. В связи с преступлениями, сопряженными с цифровыми доказательствами, возникают особые задачи в сфере международного сотрудничества. Учитывая, что электронные доказательства характеризуются неустойчивостью, для международного сотрудничества в деле борьбы с киберпреступностью требуется своевременное реагирование и способность запрашивать проведение специальных следственных мероприятий, включая обеспечение сохранности и предоставления данных поставщиками услуг из частного сектора. К проблемам, часто встречающимся при запросе таких данных у других стран, относятся задержки с реагированием на запросы, отсутствие гибкости и готовности реагировать у органа, у которого запрашиваются доказательства, форма, в которой доказательства предоставляются запрашивающему государству и которая не всегда может использоваться в уголовном производстве, и отличие определений составов уголовных преступлений в разных государствах[13].

20. Несмотря на то что существует ряд форм неофициального сотрудничества между правоохранительными органами, включая сети "24/7", для получения экстерриториальных электронных доказательств страны по-прежнему в значительной степени полагаются на традиционные официальные судебные механизмы, в частности двусторонние документы о взаимной правовой помощи, при этом более 70 процентов стран используют официальные просьбы о взаимной правовой помощи[14]. Срок получения ответа на такие просьбы, связанные с расследованием киберпреступлений, обычно составляет около 150 дней. Такие сроки зачастую могут превышать срок хранения данных поставщиком услуг или могут позволить преступникам полностью уничтожить важнейшие электронные доказательства.

21. Поэтому для обеспечения эффективного международного сотрудничества по делам, связанным с электронными доказательствами, необходимы механизмы оперативного сохранения данных в ожидании решения вопроса о дальнейших следственных мероприятиях. Развитию международного сотрудничества в делах, связанных с электронными доказательствами, могут также способствовать общие подходы к составлению просьб о предоставлении определенных видов доказательств, включая сетевые доказательства, журналы соединений и сделанные криминалистами копии содержимого памяти.

22. В некоторых действующих многосторонних документах предусмотрены механизмы, призванные облегчить доступ к данным для правоохранительных органов, например круглосуточно действующие контактные центры по

---

[12] Cybercrime Study, Chapter 6, pp. 165-167.

[13] Подготовленное УНП ООН сравнительное исследование Current practices in electronic surveillance in the investigation of serious and organized crime (Современная практика электронного наблюдения при расследовании серьезных и организованных преступлений), p. 9 (www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf).

[14] Cybercrime Study, Executive Summary, p. xxv.

обеспечению помощи в расследовании киберпреступлений, трансграничный доступ с соответствующего согласия к хранящимся компьютерным данным или к общедоступным данным и безотлагательные просьбы об оказании взаимной помощи.

23. Так, согласно Конвенции Совета Европы о киберпреступности постоянно и круглосуточно работающие контактные центры содействуют применению или, если это допускается внутригосударственным правом или практикой, непосредственно применяют следующие меры: i) оказание технической консультативной помощи; ii) обеспечение сохранности данных; и iii) сбор доказательств, предоставление законной информации и установление нахождения подозреваемых лиц.

24. Ряд международных соглашений регулируют вопросы, касающиеся сбора электронных доказательств. Например, в Конвенции Совета Европы о киберпреступности указано, что сфера применения процессуальных норм, изложенных в Конвенции, охватывает полномочия и процедуры в отношении сбора доказательств в электронной форме совершения уголовного преступления.

25. В типовом проекте закона о кибербезопасности (2011 год) Общего рынка Восточной и Южной Африки (КОМЕСА) содержатся положения, имеющие отношение к ПУИ. Эти положения касаются обязательств по мониторингу (статья 17), добровольного предоставления информации (статья 17(b)), уведомлений об удалении контента (статья 16), ответственности поставщиков услуг доступа (статья 12), записи в кэш-память (статья 13), хостинга (статья 14) и провайдеров гиперссылок/поисковых программ (статья 15). Кроме того, аналогичные, хотя и меньшие по количеству, чем в типовом законе КОМЕСА, положения содержатся также в директиве 2000/31/ЕС Европейского союза и в типовых законодательных актах МСЭ/КАРИКОМ/КСЭ, касающихся i) киберпреступности/электронных преступлений и ii) электронных доказательств.

26. Правоохранительные органы могли бы неофициально сотрудничать с целью получения электронных доказательств из других стран. Такое сотрудничество может облегчить принятие различных мер для получения экстерриториальных доказательств, включая поиск и изъятие; обеспечение сохранности компьютерных данных; распоряжения о предоставлении компьютерных данных; сбор данных в реальном времени; применение средств удаленной технико-криминалистической экспертизы; и прямой доступ для правоохранительных органов к экстерриториальным данным[15].

27. 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 таких структур, как Глобальный инновационный комплекс Интерпола[16] и Европейский центр по борьбе с

[15] Cybercrime Study, Chapter 5, pp. 126-133.

[16] www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

киберпреступностью (ЕЦК)[17] Европейского полицейского управления (Европол). Другие формы и инициативы, например Глобальная конференция по киберпространству, также предоставляют странам возможность рассматривать инновационные меры в области международного сотрудничества в борьбе с киберпреступностью.

28. Применение "облачных" технологий также создает дополнительные трудности для международного сотрудничества, поскольку все более широкой становится практика переноса компьютерных услуг в территориально рассредоточенные серверы и центры данных, вследствие чего трудно определить местонахождение электронных доказательств[18]. Так, пользователь Google может получать доступ к данным, которые хранятся или обрабатываются в Северной Америке, Юго-Восточной Азии, Северной или Западной Европе[19].

B. Обмен электронными доказательствами

1. Национальные правовые системы

29. Внутреннее законодательство некоторых государств регулирует вопросы обмена доказательствами в рамках международного сотрудничества. Например, во многих государствах существует внутреннее законодательство о взаимной помощи в области уголовного правосудия, которое можно использовать также применительно к обмену электронными доказательствами.

2. Международное сотрудничество

30. Для содействия обмену электронными доказательствами между разными правовыми системами государства могут заключать двусторонние, региональные и международные соглашения. В таких соглашениях могут содержаться положения, касающиеся помощи в обеспечении сохранности компьютерных данных, помощи в получении доступа к компьютерным данным и в изъятии, сборе и раскрытии компьютерных данных; трансграничного доступа к компьютерным данным; предоставления незапрашиваемой информации и обмена информацией; и общих просьб об оказании взаимной правовой помощи (ВПП)[20]. Содержащиеся в таких соглашениях положения являются основными источниками права, которые охватывают как права, так и обязательства сторон этих соглашений, тем самым определяя для сторон юридически обязывающие условия. Однако не все государства нуждаются в формальной договорной основе для сотрудничества в судебной сфере и обмена электронными доказательствами, а напротив, могут оказывать помощь, руководствуясь принципами взаимности или вежливости.

31. Обзор региональных и международных соглашений свидетельствует об использовании государствами различных форм обмена электронными доказательствами. Такие формы сотрудничества предусматривают применение

---

[17] www.europol.europa.eu/ec3.
[18] Cybercrime Study, Chapter 7, p. 216.
[19] Cybercrime Study, Chapter 7, pp. 216-217.
[20] Cybercrime Study, Annex 3, pp. 273-274.

общих принципов международного сотрудничества; оказание взаимной правовой помощи в целом; механизмы оперативного оказания помощи; помощь в обеспечении сохранности компьютерных данных; помощь в изъятии/обеспечении доступности/сборе/раскрытии компьютерных данных; предоставление трансграничного доступа к данным; и предоставление незапрашиваемой информации/обмен информацией. Вышеупомянутые формы сотрудничества предусмотрены в следующих соглашениях:

Организация Объединенных Наций, Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии (2000 год);

Содружество Независимых Государств, Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации (2001 год);

Совет Европы, Конвенция о киберпреступности и Дополнительный протокол к Конвенции о киберпреступности, касающийся криминализации актов расистского и ксенофобного характера, совершенных через компьютерные системы (2001 год);

Совет Европы, Конвенция о защите детей от эксплуатации и посягательств сексуального характера (2007 год);

Экономическое сообщество западноафриканских государств (ЭКОВАС), Проект директивы о борьбе с киберпреступностью в рамках ЭКОВАС (2009 год);

Лига арабских государств, Конвенция о борьбе с преступлениями в области информационных технологий (2010 год);

Шанхайская организация сотрудничества, Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (2010 год);

Общий рынок Восточной и Южной Африки (КОМЕСА), Проект типового закона о кибербезопасности (2011 год);

Африканский союз, Проект конвенции о создании правовой основы для обеспечения кибербезопасности в Африке (2012 год);

Европейский союз, Рамочное решение 2001/413/ЈНА Совета о борьбе с мошенничеством и фальсификацией безналичных платежных средств (2001 год);

Европейский союз, Рамочное решение 2005/222/ЈНА Совета об атаках на информационные системы (2005 год);

Европейский союз, Окончательное предложение COM (2010) 517 в отношении Директивы Европейского парламента и Совета об атаках на информационные системы, отменяющей Рамочное решение 2005/222/ЈНА Совета (2010 год).

32. Для обмена электронными доказательствами прежде всего используются традиционные механизмы сотрудничества, например официальные просьбы о ВПП. Процедуры ВПП регулируются рядом двусторонних, региональных и

международных соглашений. Положения, касающиеся ВПП, содержатся во многих из вышеперечисленных региональных и международных документах о киберпреступности. Процедуры и порядок обращения с просьбами о ВПП преимущественно определяются региональными и двусторонними соглашениями. К числу региональных соглашений о ВПП относятся, например, Договор о взаимной правовой помощи в уголовных делах Ассоциации государств Юго-Восточной Азии (АСЕАН) 2004 года и принятая Советом Европы Европейская конвенция о взаимной правовой помощи в уголовных делах между государствами – членами Европейского союза 2000 года.

33. Следует учитывать, что электронные доказательства по своему характеру часто являются неустойчивыми и легко подвергаются пагубному воздействию, а официальные механизмы сотрудничества не всегда обеспечивают оперативное принятие требуемых в отношении таких доказательств мер. В этой связи возможно также использование неофициальных механизмов сотрудничества и особенно сетей "24/7", которые располагают значительным потенциалом для придания динамизма такому неофициальному сотрудничеству или даже содействия, на более позднем этапе, официальному сотрудничеству. Вместе с тем набор возможных следственных действий в рамках неофициального сотрудничества может быть весьма различным. Фактором, существенно препятствующим обмену электронными доказательствами в рамках неофициального сотрудничества, является то, что во многих странах в контексте уголовного производства запрещено использовать доказательства, полученные по неофициальным каналам[21].

34. Страны, представившие материалы для исследования по киберпреступности и использующие неофициальное сотрудничество, сообщили о том, что применение соответствующих механизмов зависит от наличия компетентных и хорошо организованных иностранных служб-партнеров. Страны отметили также, что неофициальное сотрудничество между правоохранительными органами является более вероятным в том случае, если регулируются каким-либо соглашением. В этой связи ряд стран сообщили о том, что неофициальное сотрудничество опирается на региональные и двусторонние соглашения и осуществляется на основе использования сетей, созданных международными и региональными организациями и учреждениями; при содействии посольств и консульств; а также на основе использования частных сетей, объединяющих сотрудников правоохранительных органов.

35. С этой целью статья 27 Конвенции Организации Объединенных Наций против транснациональной организованной преступности содержит положения, касающиеся сотрудничества между правоохранительными органами, и рекомендует государствам рассматривать возможность заключения двусторонних или многосторонних соглашений или договоренностей о сотрудничестве между различными правоохранительными органами. Кроме того, государства принимают также различные законы о сотрудничестве между

[21] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, Chapter 4, p. 47 (см. ниже), размещено на www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

правоохранительными органами, в том числе об обмене информацией, совместном проведении расследований, электронном наблюдении или других формах наблюдения и т.д.

36. Некоторые страны сообщают о непосредственном сотрудничестве между полицейскими службами, тогда как другие страны осуществляют неофициальное сотрудничество прежде всего по каналам Интерпола. Бюро Интерпола, расположенные в 190 странах, часто связаны с национальными правоохранительными органами[22]. Благодаря этому бюро могут поддерживать неофициальные отношения, что повышает вероятность успешного применения альтернатив официальным процедурам международного сотрудничества.

37. Существует ряд трудностей на пути осуществления как официальных, так и неофициальных процедур сотрудничества в использовании электронных доказательств в сфере уголовного правосудия, которые могут препятствовать как сбору таких доказательств, так и обмену ими. Следует отметить, в частности, различия в сфере охвата положений о сотрудничестве, содержащихся в многосторонних и двусторонних документах, отсутствие обязательства представлять ответ в течение определенного срока, большое число неофициальных сетей правоохранительных органов и различия в гарантиях сотрудничества[23].

III. Средства, разработанные Управлением Организации Объединенных Наций по наркотикам и преступности

38. За последние несколько лет УНП ООН подготовило ряд документов, в которых с различных точек зрения и в рамках различных дисциплин и мандатов рассматривается тема электронных доказательств. В этой связи документы УНП ООН охватывают спектр взаимодополняющих знаний, получению которых часто способствуют широкие консультации с государствами-членами и соответствующими заинтересованными сторонами. Инструментарий УНП ООН – от основанного на исследованиях анализа конкретных форм преступности до электронных платформ, предоставляющих прямой доступ к материалам правового характера, – предлагает многогранный набор информационно-справочных документов, касающихся сбора электронных доказательств и обмена ими.

39. Хотя ни один из подготовленных УНП ООН материалов не посвящен исключительно электронным доказательствам, существует ряд руководств/исследований/документов УНП ООН, имеющих отношение к обсуждаемой теме, обзор которых представлен ниже.

---

[22] Cybercrime Study, Chapter 7, p. 187.

[23] Cybercrime Study, Chapter 7, pp. 197-215.

A. Исследования, подготовленные Управлением Организации Объединенных Наций по наркотикам и преступности во исполнение резолюций Организации Объединенных Наций

40. Во исполнение соответствующих мандатов Экономического и Социального Совета Управление Организации Объединенных Наций по наркотикам и преступности за последние несколько лет провело следующие исследования, которые касаются, в частности, сбора электронных данных и обмена ими в контексте конкретных видов преступлений: a) Справочник по преступлениям с использованием личных данных[24]; и b) Исследование влияния новых информационных технологий на совершение надругательств над детьми и их эксплуатацию[25] (далее именуемое "Исследованием по проблеме надругательства над детьми и их эксплуатации").

41. Во исполнение резолюций 65/230 и 67/189 Генеральной Ассамблеи УНП ООН оказывало секретариатскую и техническую поддержку совещаниям межправительственной группы экспертов открытого состава по проведению всестороннего исследования проблем киберпреступности. В этой связи УНП ООН, используя информацию, предоставленную государствами-членами, подготовило проект всеобъемлющего исследования по киберпреступности, которое цитируется и на которое даются ссылки в различных частях настоящего справочного документа.

1. Справочник по преступлениям с использованием личных данных

42. Во исполнение резолюций 2007/20 и 2009/22 Экономического и Социального Совета о международном сотрудничестве в деле предупреждения и расследования случаев экономического мошенничества и преступлений с использованием личных данных, а также преследования и наказания за такие деяния УНП ООН в 2011 году выпустило Справочник, посвященный некоторым вопросам права и политики, касающимся преступлений с использованием личных данных, включая вопросы сбора и использования электронных данных и информации. Основная цель Справочника заключается в том, чтобы изложить различные варианты и соображения, которые необходимо принимать во внимание при решении вопросов внутреннего режима уголовного правосудия (типология преступлений, подходы к криминализации и защита жертв), конкретные задачи в области международного сотрудничества по уголовно-правовым вопросам и возможности для взаимодействия и партнерства между государственным и частным секторами, прежде всего в контексте предупреждения преступлений с использованием личных данных. Сочетание в Справочнике исследований и практических материалов позволяет осветить различные аспекты и параметры сложных проблем, связанных с этим видом преступности.

43. Справочник охватывает разнообразные вопросы и предназначен для законодателей, разработчиков политики, сотрудников прокуратуры и правоохранительных органов и практикующих юристов, а также других

---

[24] www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

[25] См. сноску 21.

заинтересованных сторон, включая представителей соответствующих международных и межправительственных организаций, частного сектора и академических кругов.

44. Справочник может быть полезен также при осуществлении программ технической помощи и мероприятий по созданию потенциала с целью расширения экспертных знаний при решении правовых, институциональных и оперативных вопросов, связанных с преступлениями с использованием личных данных как нового вида преступлений.

45. Кроме того, в содержащемся в Справочнике практическом руководстве по международному сотрудничеству в борьбе с преступлениями с использованием личных данных приводится обзор вопросов, касающихся транснациональных аспектов преступлений с использованием личных данных, а также базовая информация и руководящие принципы в отношении оптимальных подходов к просьбам о международном сотрудничестве в этой области, в том числе на основе соответствующих примеров конкретных дел.

2. Исследование влияния новых информационных технологий на совершение надругательств над детьми и их эксплуатацию

46. Во исполнение резолюции 2011/33 Экономического и Социального Совета, озаглавленной "Предупреждение, защита и международное сотрудничество в области борьбы с использованием новых информационных технологий для надругательства над детьми и/или их эксплуатации", УНП ООН опубликовало в 2015 году Исследование влияния новых информационных технологий на совершение надругательств над детьми и/или их эксплуатацию (первоначально было представлено Комиссии по предупреждению преступности и уголовному правосудию на ее двадцать третьей сессии в мае 2014 года). Подготовленное УНП ООН исследование основано на открытых источниках информации по этой проблеме, а также на результатах работы неофициального совещания группы экспертов УНП ООН по этой теме, которое было проведено в Вене 23-25 сентября 2013 года и в работе которого приняли участие эксперты из международных организаций, представители правоохранительных органов, другие соответствующие специалисты-практики и представители научных кругов. Исследование содержит соответствующую справочную информацию по следующим вопросам:

a) новые определения и термины;

b) типология преступлений;

c) наиболее распространенные типы и формы соответствующего поведения;

d) основные виды информационно-коммуникационных технологий, которые облегчают совершение некоторых видов преступлений, таких как надругательство над детьми и их эксплуатация;

e) портрет и техническая квалификация правонарушителя;

f) факторы риска виктимизации;

g) характер таких материалов, как фотографии, негативы, слайды, журналы, книги, рисунки, кинофильмы, видеокассеты и компьютерные диски или файлы; и

h) типы устройств и платформ, используемых в преступных целях, например: мобильные телефоны, службы удаленного хранения данных, которые включают интегрированную технологию шифрования, технологию "облачных" вычислений и такие новые прикладные программы, как Snap Chat и Wickr, которые позволяют пользователям распространять временные изображения, исчезающие через несколько секунд после получения.

47. Кроме того, глава III исследования посвящена расследованию случаев надругательства над детьми и их эксплуатации с использованием информационно-коммуникационных технологий.

48. В исследовании подробно рассмотрены вопросы доступности и применения на практике связанных с изображениями компьютерных программ и технологий, которые позволяют правоохранительным органам идентифицировать и спасать неидентифицированных жертв, фигурирующих в опубликованных в сети материалах, а также проводить криминалистические исследования путем сопоставления цифровых материалов подозреваемых с изображениями в базах данных. В исследовании содержится полезная информация об инновационных технологиях, используемых для снижения информационной избыточности в рамках следственных действий и при этом служащих интересам защиты жертв. К таким технологиям относятся, в частности:

"PhotoDNA" компании Microsoft: бесплатная компьютерная программа, используемая для создания подобной отпечатку пальца уникальной подписи на цифровом изображении, которую можно сравнивать с подписями других изображений и находить копии этого изображения;

базы данных изображений, демонстрирующих надругательства, которые содержат информацию об идентифицированных и неидентифицированных жертвах[26]; и

действующая под эгидой Интерпола Международная база данных изображений сексуальной эксплуатации детей: используется для идентификации и спасения прежде не идентифицированных жертв на основе применения современных компьютерных программ сравнения изображений с целью нахождения связи между жертвами и местами.

49. Вышеупомянутые технические новшества используются также поставщиками услуг интернета для алгоритмического поиска и удаления со своих серверов материалов, связанных с сексуальными надругательствами над детьми.

50. Кроме того, в исследовании рассказывается о такой области криминалистики, как цифровая криминалистика, которая занимается

[26] Например, базы данных, созданные Интерполом и расположенным в Соединенных Штатах Америки Национальным центром по проблеме исчезнувших и эксплуатируемых детей (НЦИЭД).

восстановлением и исследованием образуемых компьютерами электронно-цифровых следов. В этой связи в исследовании сообщается о типах компьютерных данных и электронных сообщений, которые могут иметь отношение к преступному деянию, о всевозможных форматах и системах, используемых для занесения данных в файлы, а также о средствах, применяемых для анализа данных.

51. В исследовании рассматривается также использование в криминалистических исследованиях программ автоматизированного поиска. Особое внимание обращено на использование таких программных средств для того, чтобы легко и оперативно находить сайты и контент, которые помечены распространенными ключевыми словами.

52. В исследовании рассматриваются также достигнутые за прошедшее десятилетие успехи в разработке и применении технических и программных средств, позволяющих оперативно находить соответствующие данные в тысячах индивидуальных баз данных, финансовой документации, образцах ДНК, образцах звучания, видеоклипах, картах, поэтажных планах, донесениях агентурной разведки и социальных сетях. С помощью этих средств соответствующие данные сплетаются, образуя точную, ясную и полезную траекторию и создавая условия для концептуального анализа связей.

53. Кроме того, в исследовании рассматриваются особенности и приемлемость методов расследования шпионской деятельности применительно к преступлениям с использованием интернета.

3. Проект всеобъемлющего исследования по киберпреступности

54. В главе 6 проекта всеобъемлющего исследования по киберпреступности подробно рассматривается тема электронных доказательств в сфере уголовного правосудия, начиная с необходимости выявления, сбора и анализа электронных доказательств с помощью методов цифровой криминалистики. В этой главе приводится анализ приемлемости и порядка использования электронных доказательств в судебных процессах, а также показано, как различные сложности в подготовке обвинительных заключений способны влиять на эффективность функционирования системы уголовного правосудия. В ней изложены также потребности в укреплении потенциала правоохранительных органов и органов уголовного правосудия и дан обзор проводимых и требуемых мероприятий по оказанию технической помощи.

55. Кроме того, некоторые аспекты, касающиеся электронных доказательств, рассматриваются с точки зрения обеспечения правопорядка и международного сотрудничества. В этой связи в главе 5 (Правоприменительная деятельность и расследования) рассматриваются такие вопросы, как изучение, использование, хранение и сохранение электронных данных, которые могут быть представлены в качестве электронных доказательств; сбор данных в реальном времени; средства дистанционной криминалистики; прямой доступ правоохранительных органов к экстерриториальным данным; права человека и следственные мероприятия правоохранительных органов и получение данных у частных поставщиков услуг. С другой стороны, в главе 7 (Международное сотрудничество) рассматриваются такие вопросы, как получение экстерриториальных доказательств из "облачных" хранилищ и у поставщиков

услуг с уделением внимания вопросу местоположения данных; доступ к экстерриториальным данным в ходе сбора доказательств, получение данных у экстерриториальных поставщиков услуг.

B. Средства, разработанные Управлением Организации Объединенных Наций по наркотикам и преступности, для использования в контексте деятельности по оказанию технической помощи

56. В связи с осуществлением программ УНП ООН по оказанию технической помощи потребовалось разработать практические пособия, в которых тема электронных доказательств рассматривается с точки зрения специалистов-практиков. В этой связи участники второго Межрегионального совещания по обмену опытом запрашивания и предоставления цифровых доказательств в рамках расследований и уголовного преследования по делам, связанным с организованной преступностью[27], сформулировали для следователей и прокуроров ряд основных рекомендаций относительно запрашивания электронных/цифровых данных/доказательств у других стран.

57. Набор основных рекомендаций содержит практические советы по запрашиванию электронных доказательств у других стран, которые предусматривают, в частности, получение электронных доказательств из открытых источников или непосредственно у поставщиков услуг интернета, компании которых учреждены или зарегистрированы в запрашивающей стране в качестве дочерних компаний, расположенных за границей ПУИ; обеспечение сохранности электронных доказательств до направления просьбы об их раскрытии; направление просьбы, по возможности, непосредственно ПУИ и направление копии просьбы в следственный орган или прокуратуру запрашиваемой страны; проведение консультаций с подразделением по борьбе с киберпреступностью по техническим аспектам просьбы.

58. Во исполнение резолюции 7/4 Конференции участников Конвенции Организации Объединенных Наций против транснациональной организованной преступности УНП ООН продолжает разрабатывать инструменты для осуществления международного сотрудничества, включая Программу составления просьб об оказании взаимной правовой помощи. В этой связи УНП ООН организовало ряд неофициальных совещаний группы экспертов для анализа и обсуждения вопроса о модернизации этой программы и для обсуждения направлений ее использования в будущем.

59. На последнем неофициальном совещании группы экспертов в мае 2015 года участники договорились о включении в модернизированную программу модуля, посвященного цифровым доказательствам, который может быть полезен государствам при запрашивании помощи относительно этого вида доказательств. В этой связи эксперты поделились опытом запрашивания и

[27] Тбилиси, Грузия, 9-11 декабря 2014 года. Это пособие было разработано в рамках инициативы УНП ООН по созданию и укреплению Сети прокуроров и центральных органов стран происхождения, транзита и назначения с целью борьбы с транснациональной организованной преступностью в Центральной Азии и на Южном Кавказе.

получения их странами цифровых доказательств, в том числе сообщили о том, используются ли типовые образцы просьб о предоставлении цифровых доказательств и существуют ли стандартные подходы к описанию цифровых доказательств. Совещание сформулировало рекомендации относительно возможного формата и структуры модуля, посвященного цифровым доказательствам, уделив особое внимание различным видам цифровых доказательств, таким как данные устройства, сетевые данные, сведения об абонентах и данные о контенте. Работа над модернизированной версией Программы составления просьб об оказании взаимной правовой помощи будет завершена после проведения следующего неофициального совещания группы экспертов в Вене 22 и 23 октября 2015 года.

C. Платформы управления знаниями Управления Организации Объединенных Наций по наркотикам и преступности

1. Распространение электронных ресурсов и законов о борьбе с преступностью (ШЕРЛОК)

60. УНП ООН продолжало работать над развитием информационно-справочного портала ШЕРЛОК, задачей которого является распространение правовой документации по преступности. На портале ШЕРЛОК осуществляется сбор материалов по различным видам преступлений и смежным темам, в том числе по электронным доказательствам. По состоянию на 18 августа 2015 года портал располагает 44 документами, содержащими нормоустанавливающие стандарты, касающиеся электронных доказательств.

2. Хранилище данных по киберпреступности

61. Помимо портала ШЕРЛОК УНП ООН создало хранилище данных по киберпреступности, которое является центральной базой данных о законодательстве и накопленном опыте, в целях содействия постоянной оценке потребностей и потенциала систем уголовного правосудия, а также оказанию и координации технической помощи.

62. Хранилище, созданное в 2015 году на основе предоставляемой и обновляемой государствами-членами информации, является первым доступным глобальным хранилищем информации о законах, прецедентах и извлеченных уроках, касающихся киберпреступности и электронных доказательств. В разноплановые задачи хранилища входит, в частности: содействие использованию законодателями базы данных по законодательству при разработке законов, касающихся киберпреступности или электронных доказательств; содействие международному сотрудничеству путем оказания помощи сотрудникам правоохранительных органов и прокуратуры в определении положений законодательства о киберпреступности, которые применимы в других государствах-членах; и предоставление пользователям примеров передового опыта в области предупреждения и расследования киберпреступлений и преследования за их совершение. Функции центрального органа не всегда указываются или закрепляются в национальных нормативных актах о взаимной правовой помощи. В тех случаях, когда национальное законодательство содержит такие положения, оно может предусматривать

назначение правительственного учреждения в качестве центрального органа, включать перечень его функций и в отдельных случаях содержать защитную оговорку, подтверждающую, что данный закон не ограничивает полномочия органа составлять или получать просьбы или сотрудничать с иностранным государством по другим каналам или иным способом. Например, в законе о правовой помощи одной из европейских стран предусмотрено, что центральный орган "1) получает запросы об оказании помощи...; 2) обеспечивает прямо или через [другие] органы выполнение просьб...; 3) препровождает просьбы об оказании помощи, а также 4) обеспечивает перевод документов".

IV. Выводы и рекомендации

63. Рабочая группа по вопросам международного сотрудничества, возможно, пожелает рекомендовать Конференции участников:

a) просить Секретариат в сотрудничестве с соответствующими межправительственными организациями и в случае наличия внебюджетных средств подготовить справочник по сбору электронных доказательств и обмену ими;

b) просить Секретариат в рамках его усилий по обновлению методических пособий, касающихся международного сотрудничества, включать в них тему электронных доказательств;

c) просить государства-члены уведомить Секретариат о существовании специальных подразделений и структур по борьбе с киберпреступностью для включения этой информации в справочник по центральным национальным органам.