Организация Объединенных Наций E/CN.15/2013/24

Экономический и Социальный Совет

Distr.: General
5 March 2013
Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Двадцать вторая сессия
Вена, 22-26 апреля 2013 года
Пункт 7 предварительной повестки дня*
Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения

Содействие деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала

Доклад Генерального секретаря

Резюме

Настоящий доклад был подготовлен во исполнение резолюции 20/7 Комиссии по предупреждению преступности и уголовному правосудию, озаглавленной "Содействие деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала". В нем содержатся краткая информация о деятельности Управления Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) в сфере оказания государствам-членам технической помощи и помощи в наращивании потенциала, а также краткий обзор мероприятий, осуществленных ЮНОДК в целях обеспечения поддержки группы экспертов по проведению всестороннего исследования проблемы киберпреступности, и резюме проекта исследования проблемы киберпреступности.

* E/CN.15/2013/1.

V.13-80775 (R) 110313 250313

I. Введение

1. Настоящий доклад был подготовлен во исполнение резолюции 20/7 Комиссии по предупреждению преступности и уголовному правосудию, озаглавленной "Содействие деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала".

2. В этой резолюции Комиссия просила Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК), в сотрудничестве с государствами-членами, соответствующими международными и региональными организациями и, в соответствующих случаях, частным сектором, продолжать оказывать государствам, по их просьбе, техническую помощь и помощь в подготовке кадров с учетом национальных потребностей, особенно в вопросах предупреждения, выявления и расследования киберпреступлений во всех формах и преследования за их совершение, без ущерба для работы и итогов совещаний группы экспертов по проведению всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора.

3. Кроме того, Комиссия приняла к сведению итоги первого совещания группы экспертов (см. E/CN.15/2011/19) и просила ЮНОДК укреплять сотрудничество в области борьбы с киберпреступностью с государствами-членами и соответствующими организациями, такими как Международная организация уголовной полиции (Интерпол), Европейское полицейское управление, Международный союз электросвязи (МСЭ), Европейская комиссия, Совет Европы, Шанхайская организация сотрудничества и Содружество Независимых Государств, а также частным сектором, включая компьютерные компании и поставщиков Интернет-услуг.

II. Деятельность Управления Организации Объединенных Наций по наркотикам и преступности по оказанию государствам технической помощи и помощи в подготовке кадров в сотрудничестве с государствами-членами, международными и региональными организациями и частным сектором

4. В 2012 году ЮНОДК завершило разработку Глобальной программы борьбы с киберпреступностью, предусматривающей применение целостного подхода с упором на: a) организации обучения сотрудников правоохранительных органов и работников системы уголовного правосудия методам проведения расследований и применяемым в уголовном правосудии подходам к борьбе с киберпреступностью; b) предупреждении преступлений в киберпространстве и повышении уровня осведомленности о проблеме киберпреступности; c) расширении сотрудничества в области борьбы с киберпреступностью на национальном, региональном и международном уровнях и d) сборе данных, изучении и анализе связей между организованной преступностью и киберпреступлениями. В рамках этой программы ЮНОДК

призвано принимать меры по содействию устойчивому и долгосрочному наращиванию потенциала, в том числе посредством проведения учебных занятий в сотрудничестве с целым рядом партнеров, включая МСЭ, организации частного сектора и научных экспертов.

5. Все запланированные в рамках Глобальной программы борьбы с киберпреступностью мероприятия призваны содействовать наращиванию долгосрочных устойчивых национальных потенциалов для предупреждения преступлений в киберпространстве и борьбы с ними. Предусмотренные Программой мероприятия будут осуществляться в первую очередь ЮНОДК в качестве исполнительного учреждения при дополнительной поддержке МСЭ и других соответствующих партнеров, в случае необходимости, и согласно обсуждаемой области деятельности, запросам правительств и соответствующему мандату.

6. В мае 2011 года ЮНОДК подписало с МСЭ меморандум о взаимопонимании с целью осуществления сотрудничества в деле оказания технической помощи в области борьбы с киберпреступностью и обеспечения кибербезопасности в рамках соответствующих мандатов каждой из организаций.[1] В соответствии с этим меморандумом ЮНОДК вместе с МСЭ занимались оказанием технической помощи по просьбе государств. В этом контексте ЮНОДК основное внимание уделяло аспектам киберпреступности, связанным с предупреждением преступности и уголовным правосудием, в то время как МСЭ выполняло работу по укреплению кибербезопасности, в том числе путем содействия обеспечению защиты важнейших объектов инфраструктуры от нападений, совершаемых с использованием компьютеров.

7. В своей резолюции 2011/33, озаглавленной "Предупреждение, защита и международное сотрудничество в области борьбы с использованием новых информационных технологий для надругательства над детьми и/или их эксплуатации", Экономический и Социальный Совет просил ЮНОДК провести исследование, которое способствовало бы выявлению, описанию и оценке влияния новых информационных технологий на совершение надругательств над детьми и их эксплуатацию, принимая во внимание соответствующие данные, собранные группой экспертов. В этой резолюции Совет также просил ЮНОДК подготовить и провести оценку потребностей государств в подготовке кадров в области расследования преступлений против детей, совершаемых с использованием новых информационно-коммуникационных технологий, и на основе результатов этого исследования разработать программу подготовки кадров и оказания технической помощи в целях содействия государствам-членам в повышении эффективности борьбы с такими преступлениями.

8. В 2011 году и в первой половине 2012 года ЮНОДК осуществило обзор документации в целях изучения влияния новых информационных технологий на совершение надругательств над детьми и их эксплуатацию и предприняло предварительные шаги по оценке потребностей государств в области подготовки кадров. В соответствии с резолюцией 2011/33 Экономического и Социального Совета доклад о выполнении резолюции должен быть представлен на рассмотрение Комиссии на ее двадцать третьей сессии в 2014 году.

---

[1] См. www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

9. В апреле и мае 2012 года ЮНОДК организовало семинары в Найроби для 10 стран Восточной и Южной Африки, Бейруте для 12 стран Западной Азии и Бангкоке для 11 стран Юго-Восточной и Южной Азии. Семинары позволили получить информацию о потребностях этих стран в технической помощи в области борьбы с киберпреступностью. Семинары продемонстрировали: a) необходимость обеспечения базовой подготовки лиц, ответственных за разработку политики и принятие решений, в целях придания более приоритетного характера вопросам киберпреступности; b) необходимость дальнейшей разработки механизмов официального и неофициального международного сотрудничества между сотрудниками правоохранительных органов и работниками прокуратуры; c) необходимость совершенствования доступа к программным и аппаратным средствам проведения судебной экспертизы и обучения работе с ними в целях проведения расследований киберпреступлений и d) необходимость содействия налаживанию партнерских связей между государственным и частным секторами с целью укрепления мер по предупреждению киберпреступности. В настоящее время ЮНОДК, опираясь на результаты работы этих семинаров, изучает возможные пути оказания технической помощи странам Восточной и Южной Африки в рамках Глобальной программы борьбы с киберпреступностью вместе с соответствующими партнерами, включая МСЭ.

10. Представители ЮНОДК участвовали в совещаниях с ведущими мировыми поставщиками электронных услуг с целью достижения дальнейшего прогресса в обеспечении поддержки со стороны частного сектора и его привлечения к осуществлению Глобальной программы борьбы с киберпреступностью. Программа предусматривает налаживание тесного сотрудничества с партнерами из частного сектора и соответствующими межправительственными организациями в целях содействия реализации программ по наращиванию потенциала. Программа также призвана способствовать установлению рабочих отношений между правоохранительными органами и местными отделениями ведущих мировых поставщиков электронных услуг, включая организацию мировыми поставщиками услуг для сотрудников специализированных правоохранительных органов по борьбе с киберпреступностью презентаций, посвященных корпоративным процедурам и требованиям к соблюдению надлежащих судебных процедур, а также способам облегчения потоковой передачи стратегической информации об угрозах правоохранительным органам ведущими мировыми поставщиками услуг по обеспечению кибербезопасности.

11. В феврале 2012 года в Панаму по просьбе ее правительства в целях дальнейшего наращивания национального потенциала в области борьбы с киберпреступностью была направлена миссия по проведению первоначальной оценки. Миссия, которая была организована совместными усилиями штаб-квартиры ЮНОДК и регионального отделения для стран Центральной Америки и Карибского бассейна, вместе с межведомственной правительственной рабочей группой провела работу по рассмотрению и пересмотру законодательных рамок для борьбы с киберпреступностью. Рабочая группа, в состав которой входят представители национальных органов и лица, формирующие общественное мнение, а также представители субъектов частного сектора, была создана с целью разработки в Панаме законодательства о борьбе с киберпреступностью. Были проведены консультации в целях

согласования широкого и всеобъемлющего подхода к борьбе с киберпреступностью в этой стране. Власти Панамы также выразили заинтересованность в применяемом МСЭ и ЮНОДК совместном подходе и поддержке, которая может быть им оказана в деле укрепления защиты важных объектов инфраструктуры Панамы.

12. Кроме того, в 2012 году в интересах дальнейшего укрепления сотрудничества и повышения уровня информированности о киберпреступлениях ЮНОДК организовало в Исламской Республике Иран по ее просьбе практикум с целью проведения учебных занятий по вопросам киберпреступности для 80 сотрудников правоохранительных органов и должностных лиц министерства юстиции. В целях расширения международного сотрудничества в области борьбы с киберпреступностью также были проведены совещания с представителями местного отделения Интерпола, сотрудниками полиции по борьбе с киберпреступностью и работниками юстиции.

III. Деятельность Управления Организации Объединенных Наций по наркотикам и преступности в области укрепления сотрудничества с государствами-членами, межправительственными организациями и частным сектором

13. С целью дальнейшего укрепления сотрудничества в области борьбы с киберпреступностью на всех уровнях ЮНОДК продолжало принимать участие в качестве наблюдателя в консультациях Комитета участников Конвенции Совета Европы о киберпреступности, проводившихся в рамках Конвенции Совета Европы о киберпреступности, и в ежегодной конференции "Октопус".

14. ЮНОДК также принимало участие в качестве партнера в осуществлении принятой Содружеством инициативы по борьбе с киберпреступностью, в контексте которой ЮНОДК занималось изысканием путей улучшения сотрудничества между ЮНОДК и партнерами по инициативе. Кроме этого, ЮНОДК участвовало в качестве наблюдателя в работе Европейской группы по подготовке и обучению в области борьбы с киберпреступностью и сотрудничало с Организацией по безопасности и сотрудничеству в Европе в рамках ее ежегодного совещания полицейских экспертов.

IV. Деятельность Управления Организации Объединенных Наций по наркотикам и преступности, направленная на обеспечение поддержки группы экспертов по проведению всестороннего исследования проблемы киберпреступности

15. Первое совещание группы экспертов по проведению всестороннего исследования проблемы киберпреступности состоялось в Вене 17-21 января 2011 года. На этом совещании группа экспертов рассмотрела и утвердила подборку тем и методологию исследования (см. E/CN.15/2011/19). Методология исследования предусматривала распространение вопросника среди государств-членов, межправительственных организаций и представителей частного сектора и научных учреждений. Сбор информации в соответствии с согласованной методологией проводился ЮНОДК в период с февраля по июль 2012 года[2].

16. В июне 2012 года вопросник был направлен всем государствам-членам, с тем чтобы они представили свои замечания. После того, как были получены замечания государств, ЮНОДК завершило работу над вопросником и распространило его через веб-портал для сбора данных. С целью получения от государств-членов подтверждения правильности отдельных аспектов собранной и проанализированной информации ЮНОДК направило всем государствам краткий обзор их законодательных положений в области борьбы с киберпреступностью, с тем чтобы они представили свои замечания и, в случае необходимости, внесли исправления. В ноябре 2012 года ЮНОДК провела консультации с экспертами, назначенными каждой из региональных групп, относительно предварительного анализа результатов, полученных на основании заполненных государствами-членами вопросников. На основе ответов на вопросник, полученных от государств-членов, частного сектора и научных и межправительственных организаций, ЮНОДК подготовило проект исследования для рассмотрения группой экспертов.

17. Второе совещание группы экспертов состоялось 25-28 февраля 2013 года[3]. На этом совещании группа экспертов приняла к сведению и рассмотрела всестороннее исследование проблемы киберпреступности, подготовленное ЮНОДК под эгидой группы экспертов. Группа экспертов отметила, что в ходе совещаний, равно как и в исследовании, были учтены мнения и различные подходы государств к предупреждению киберпреступности и борьбе с этим явлением. В ходе обсуждений, посвященных исследованию проблемы киберпреступности, отмечалась

---

[a] Текст раздела IV первоначально был опубликован в неотредактированном справочном документе (UNODC/CCPCJ/EG.4/2013/2); в настоящем докладе он приводится в отредактированном виде согласно установленным Секретариатом стандартам.

[2] Информация была получена от 69 государств-членов со следующим распределением по регионам: Азия (19), Америка (13), Африка (11), Европа (24) и Океания (2). Информация была получена от 40 организаций частного сектора, 17 научных организаций и 11 межправительственных организаций. Секретариат изучил также свыше 500 документов, находящихся в открытом доступе.

[3] Итоги совещания приводятся в документе UNODC/CCPCJ/EG.4/2013/3.

широкая поддержка деятельности по наращиванию потенциала и оказанию технической помощи, а также роль ЮНОДК в этой связи. Высказывались различные мнения относительно содержания исследования и представленных в нем выводов и вариантов возможных действий. Группа экспертов обсудила пути продвижения вперед и рекомендовала Комиссии продолжить обсуждение исследования на ее двадцать второй сессии.

18. Резюме всестороннего исследования, которое приводится ниже, было подготовлено ЮНОДК по поручению группы экспертов. Выводы и варианты возможных действий, содержащиеся в исследовании и резюме, были сформулированы ЮНОДК на основе полученной эмпирическим путем информации и не призваны служить в качестве рекомендаций[4].

A. Резюме всестороннего исследования проблемы киберпреступности, подготовленное Управлением Организацией Объединенных Наций по наркотикам и преступности

1. Подключение к глобальной сети и киберпреступность

19. В 2011 году по меньшей мере 2,3 миллиарда человек или более одной трети от общей численности населения планеты имели доступ к Интернету. Более 60 процентов всех пользователей Интернета находятся в развивающихся странах, причем 45 процентов всех пользователей Интернета составляют лица в возрасте до 25 лет. По оценкам, к 2017 году доступ к мобильному широкополосному Интернету получат до 70 процентов от общей численности населения мира. К 2020 году количество сетевых устройств ("Интернет вещей") будет в шесть раз превосходить численность населения, что полностью изменит нынешнее представление об Интернете. В сверхподключенном к сети мире будущего будет трудно представить себе какое-либо "компьютерное преступление", а, возможно, и вообще любое преступление, которое не сопровождалось бы электронными доказательствами, связанными с подключением к интернет-протоколу.

20. Определения киберпреступности главным образом зависят от того, в каких целях этот термин будет использоваться. Основу киберпреступности составляют ограниченное число деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем. Однако, если этим не ограничиваться, то в отношении деяний, предполагающих использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда, включая формы преступлений, связанных с использованием персональных данных, и деяния, связанные с хранящейся в компьютере информацией (все они входят в более широкое понятие "киберпреступности"), не так легко найти всеобъемлющее юридическое определение. В отношении преступлений, составляющих основу киберпреступности, некоторые определения необходимы. Однако наличие определения киберпреступности не столь важно

[4] Полный текст исследования представляется только на английском языке, как это отмечается в документе E/CN.15/2013/CRP.5.

для других целей, таких как определение диапазона специальных следственных полномочий и возможностей в области международного сотрудничества, которые в большей степени касаются обнаружения электронных доказательств совершения любого преступления, а не нахождения широкого, искусственного определения концепции "киберпреступности".

2. Глобальная картина киберпреступности

21. Во многих странах резкий всплеск в количестве подсоединений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне правоохранительные органы в своих ответах на вопросник отмечают рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. По оценкам, свыше 80 процентов киберпреступлений совершаются в той или иной форме организованной деятельности, со сложившимися черными рынками киберпреступности в области цикла создания вредоносных программ, компьютерных вирусов, управления бот-сетями, сбора персональных и финансовых данных, продажи данных и получения денег за финансовую информацию. Для совершения киберпреступлений более не требуется обладание сложными навыками или знание сложных методов. Особенно в контексте развивающихся стран появилась субкультура молодых людей, занимающихся финансовым мошенничеством при помощи компьютеров, многие из которых начинают заниматься киберпреступностью в конце подросткового возраста.

22. В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием содержащейся в компьютере информации, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем. Однако государственные органы и предприятия частного сектора по-разному воспринимают относительный риск и угрозу. В настоящее время статистические данные о преступности, регистрируемые полицией, не являют собой прочной основы для межстрановых сравнений, хотя такие статистические данные часто важны для разработки политики на национальном уровне. Две трети стран считают свои системы полицейской статистики недостаточными для того, чтобы регистрировать киберпреступность. Показатели киберпреступности, регистрируемые полицией, зависят не столько от непосредственного уровня преступности, сколько от уровня развития страны и специализированных возможностей полиции.

23. Более надежную основу для сравнения представляют собой опросы на тему виктимизации. Они свидетельствуют о том, что виктимизация частных лиц в результате киберпреступности значительно выше, чем в случае "обычных" форм преступности. Показатели виктимизации в отношении мошенничества с кредитными картами в режиме "онлайн", кражи персональных данных, ответов на попытку фишинга и несанкционированного

доступа к учетным записям электронной почты составляют от 1 до 17 процентов среди пользователей Интернета в 21 стране мира, в отличие от типичных показателей в отношении краж со взломом, ограблений и краж автомобиля, составляющих для этих же стран менее 5 процентов. Показатели виктимизации, связанной с киберпреступностью, выше в странах с низким уровнем развития, что подчеркивает необходимость укрепления профилактической работы в этих странах.

24. Предприятия частного сектора в Европе сообщают об аналогичных показателях виктимизации – от 2 до 16 процентов – в отношении таких деяний, как нарушение данных в результате вторжения или фишинга. Наиболее широко используемые для совершения этих преступлений уголовные средства, такие как бот-сети, имеют глобальный охват. В 2011 году во всем мире свыше одного миллиона индивидуальных IP-адресов функционировали в качестве серверов управления бот-сетями. Серьезную озабоченность для правительств также представляет содержание Интернета. Предназначенные для удаления материалы включают детскую порнографию и высказывания на почве ненависти, а также содержание данных, связанное с диффамацией и критикой правительства, что вызывало в ряде случаев озабоченность в отношении соблюдения прав человека. Почти 24 процента общего объема глобального потока данных в Интернете представляют собой, по оценкам, нарушение авторских прав, причем наиболее высокий уровень загрузки материалов совместного пользования ("peer-to-peer" или "P2P") отмечается в странах Африки, Южной Америки и Западной и Южной Азии.

3. Законодательство в области киберпреступности

25. Юридические меры играют ключевую роль в предупреждении и противодействии киберпреступности. Такие меры необходимы во всех областях, включая криминализацию, процессуальные полномочия, юрисдикцию, международное сотрудничество и ответственность и обязательства компаний, предоставляющих услуги Интернета. На национальном уровне как существующие, так и новые (или планируемые) законы в области киберпреступности наиболее часто касаются криминализации, что свидетельствует о том, что основной упор делается на установлении конкретного состава преступлений применительно к основным киберпреступлениям. Однако страны все шире признают необходимость принятия законов в других областях. По сравнению с существующим законодательством в новых или планируемых законах по противодействию киберпреступности более часто рассматриваются следственные действия, вопросы юрисдикции, электронных доказательств и международного сотрудничества. Менее половины представивших ответы стран всего мира считают свои уголовно-процессуальные системы достаточными, хотя за этим скрываются большие региональные различия. В то время как более двух третей стран Европы сообщают о том, что их законодательство является достаточным, в Африке, Северной и Южной Америке, Азии и Океании картина прямо противоположная: там свыше двух третей стран считают законодательство лишь частично достаточным или вообще недостаточным. Лишь половина стран, указавших на недостаточность своего законодательства, также сообщили о новых или планируемых законах, что подчеркивает настоятельную необходимость укрепления законодательства в этих регионах.

26. За последнее десятилетие наблюдается значительная активность в принятии международных и региональных документов, направленных на противодействие киберпреступности. Они включают как обязательные для выполнения, так и необязательные документы. Можно выделить пять групп документов, в которые входят документы, разработанные в контексте или под эгидой: a) Совета Европы или Европейского союза, b) Содружества Независимых Государств или Шанхайской организации сотрудничества, c) межправительственных африканских организаций, d) Лиги арабских государств и e) Организации Объединенных Наций. Все эти документы в значительной степени обогащают друг друга, в том числе в части, касающейся концепций и подходов, разработанных в Конвенции Совета Европы о киберпреступности. Анализ статей 19 многосторонних документов, имеющих отношение к киберпреступности, показывает, что в них присутствуют общие основные положения, но также имеются и значительные расхождения в рассматриваемых в них основных областях.

27. Во всем мире 82 страны подписали или ратифицировали тот или иной обязательный для выполнения документ о киберпреступности[5]. Многосторонние документы о киберпреступности не только обеспечивают формальное участие в них и их осуществление, но и оказывают косвенное влияние на национальное законодательство благодаря их использованию в качестве образца государствами, не являющимися их участниками, или за счет влияния законодательства государств-участников на другие страны. Участие в многостороннем документе о киберпреступности соотносится с ощущением большей достаточности национального уголовного и процессуального законодательства, что свидетельствует о том, что нынешние положения многосторонних документов в этих областях в целом считаются эффективными. Более 40 представивших информацию стран считают Конвенцию Совета Европы о киберпреступности наиболее часто используемым многосторонним документом при разработке законодательства в области противодействия киберпреступности. В целом, многосторонние документы из других "групп" использовали примерно в два раза меньше стран.

28. В целом, одна треть отвечающих стран сообщила, что их законодательное положение было высоко, или очень высоко, согласовано со странами, рассматриваемыми как важное в целях международного сотрудничества. Однако здесь имеются региональные различия, и более высокая степень согласованности наблюдается в Северной и Южной Америке и в Европе. Это может объясняться использованием в некоторых регионах многосторонних договоров, которые по своей природе призваны играть определенную роль в обеспечении согласованности. Возможно, существует корреляция между фрагментацией на международном уровне и разнообразием положений национальных законодательств с точки зрения криминализации киберпреступлений, юрисдикционных основ и механизмов сотрудничества, с

---

[5] Один или несколько из следующих документов: Конвенцию Совета Европы о киберпреступности, Конвенцию о борьбе с преступлениями в области информационных технологий Лиги арабских государств, Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации или Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества.

одной стороны, и наличием разных документов по противодействию киберпреступности, имеющих различный тематический и географический охват, с другой. В настоящее время и в документах, и в регионах находят отражение различия, вызванные базовыми правовыми и конституционными расхождениями, включая различия в понимании прав и конфиденциальности.

4. Криминализация

29. Информация об уголовном законодательстве в области киберпреступности собиралась при помощи вопросника, подготовленного для целей проведения исследования, а также посредством анализа основных источников с использованием имеющейся информации о законодательстве стран, собранной Секретариатом[6]. В вопроснике, подготовленном для целей проведения исследования, были выделены 14 деяний, которые обычно включаются в понятие киберпреступности[7]. Страны-респонденты сообщили о том, что эти 14 деяний широко криминализованы, за явным исключением преступлений, связанных со спамом, и, в некоторой степени, преступлений, связанных со средствами неправомерного использования компьютеров, преступлений, связанных с расизмом и ксенофобией, а также использования Интернета с целью завлечения или "груминга" детей. Это отражает определенный базовый консенсус в отношении подлежащих наказанию видов деяний, связанных с киберпреступностью. Страны сообщили о нескольких дополнительных преступлениях, не упомянутых в вопроснике. Они главным образом касались данных, хранящихся в компьютере, включая криминализацию непристойных материалов, азартных игр в режиме онлайн и онлайновых незаконных рынков, таких как рынки торговли наркотиками и людьми. В том что касается указанных 14 деяний, страны сообщили, что в отношении основных киберпреступлений против конфиденциальности, целостности данных и доступности компьютерных систем применяются специальные преступления в области киберпреступности. В отношении других форм киберпреступности чаще использовались правонарушения общего характера (непосредственно не связанные с киберпреступностью). В то же время применительно к деяниям, связанным с использованием компьютера в целях вторжения в частную жизнь, мошенничества или подлога, а также преступлениям, касающимся персональных данных, как сообщается, применяются оба подхода.

---

[6] Было проанализировано исходное законодательство 97 государств-членов, в том числе 56 государств, ответивших на вопросник, со следующим региональным распределением: Азия (24), Северная и Южная Америка (22), Африка (15), Европа (30) и Океания (6).

[7] Незаконный доступ к компьютерной системе; незаконный доступ, перехват или получение компьютерных данных; незаконное вмешательство в данные или вмешательство в систему; производство, распространение или хранение средств неправомерного использования компьютеров; нарушение конфиденциальности или мер защиты данных; компьютерное мошенничество или подлог; компьютерные преступления, связанные с использованием личных данных; компьютерные преступления, касающиеся авторских прав и товарных знаков; компьютерные преступления, связанные с причинением личного вреда; компьютерные преступления, связанные с расизмом или ксенофобией; использование компьютера с целью производства, распространения или хранения детской порнографии; использование компьютера для завлечения или "груминга" детей; и использование компьютера для содействия террористическим преступлениям.

30. Хотя в отношении общих областей криминализации существует довольно высокая степень консенсуса, детальный анализ положений существующих законов свидетельствует о том, что подходы различаются. Преступления, связанные с незаконным доступом к компьютерным системам и данным различаются в зависимости от объекта преступления (данные, система или информация) и в зависимости от криминализации "просто" доступа как такового или требования дополнительного умысла, такого как причинение убытков или повреждения. Различаются подходы к необходимости наличия умысла в составе преступления и в зависимости от криминализации вмешательства в функционирование компьютерных систем или данные. В большинстве стран вмешательство должно быть преднамеренным, в то время как в других странах предусматривается и вмешательство по неосторожности. В том что касается вмешательства в компьютерные данные, деяния, представляющие собой вмешательство, охватывают деяния от повреждения или удаления до изменения, блокировки, ввода или передачи данных. Криминализация незаконного перехвата данных различается в зависимости от того, касается ли правонарушение перехвата только не предназначенных для общего пользования данных или не ограничивается им, а также в зависимости от того, ограничивается ли преступление перехватом при помощи "технических средств". Не во всех странах криминализированы средства неправомерного использования компьютеров. В тех странах, где они криминализированы, имеются различия в зависимости от того, связано ли преступление с хранением, распространением или использованием программного обеспечения (такого как вредоносные программы) и/или компьютерных кодов доступа (например, паролей потерпевшей стороны). С точки зрения международного сотрудничества такие различия могут влиять на обоюдное признание странами соответствующего деяния преступлением.

31. В ряде стран приняты положения в отношении конкретных киберпреступлений: компьютерного мошенничества, подлога и использования персональных данных. В других странах используются общие положения в отношении мошенничества или кражи либо за основу берутся преступления, отражающие составные элементы деяния, такие как незаконный доступ, вмешательство в данные и подлог в случае преступлений, связанных с использованием персональных данных. Весьма широкое распространение получила криминализация правонарушений, связанных с содержанием данных, особенно преступлений, касающихся детской порнографии. Однако существуют расхождения в определении термина "ребенок", ограничениях, касающихся "визуальных" материалов или исключения имитируемых материалов, а также в отношении охватываемых деяний. Хотя в подавляющем большинстве стран, например, охватывается изготовление и распространение детской порнографии, в области криминализации хранения и доступа наблюдаются более широкие вариации. Что касается компьютерных правонарушений, связанных с авторскими правами и товарными знаками, страны чаще всего сообщают, что в случае деяний, совершенных умышленно и в коммерческих масштабах, они применяют общие уголовные преступления.

32. Рост популярности социальных сетей и содержания Интернета, генерированного пользователями, заставил многие страны принять меры нормативного характера, в том числе в области уголовного права, что стало причиной призывов к уважению прав на свободу самовыражения.

Представившие ответы страны сообщают о различной степени ограничения свободы выражения мнения, в том числе в отношении диффамации, неуважения, угроз, подстрекательства к ненависти, оскорбления религиозных чувств, непристойных материалов и подрыва государственных устоев. Социально-культурный элемент некоторых ограничений находит отражение не только в национальном законодательстве, но и в многосторонних документах. Так, в некоторых региональных документах по противодействию киберпреступности предусмотрены правонарушения общего характера в отношении нарушения общественной морали, порнографических материалов и религиозных или семейных принципов или ценностей.

33. Международное право в области прав человека действует как меч и щит, предусматривая необходимость криминализации (ограниченного числа) крайних форм выражения мнения, но в то же время защищая другие формы. Поэтому государства, являющиеся участниками соответствующих международных документов в области защиты прав человека, обязаны вводить некоторые запреты на свободу выражения мнения, в том числе в отношении подстрекательства к геноциду, ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию, подстрекательства к терроризму и пропаганды войны. Что касается других государств, концепция "свободы усмотрения" дает странам возможность гибкого подхода при определении границ приемлемости выражения мнения в соответствии с их собственной культурой и правовыми традициями. Тем не менее, на определенной стадии будет применимо международное право в области прав человека. Так, в случае уголовных законов о диффамации, неуважении к властям и оскорблении, распространяющихся на выражение мнения в Интернете, придется убедительно доказывать, что эти меры являются соразмерными, целесообразными и минимально интрузивными. В тех случаях, когда в одной стране содержание данных является незаконным, а в другой стране его производство и распространение разрешены, государствам потребуется сосредоточить внимание на мерах уголовного правосудия в отношении лиц, осуществляющих доступ к содержанию данных в пределах национальной юрисдикции, а не в отношении содержания данных, произведенного за пределами страны.

5. Деятельность правоохранительных органов и проведение расследований

34. Свыше 90 процентов стран-респондентов сообщают, что правоохранительным органам становится известно о деяниях в области киберпреступности из сообщений частных лиц или организаций, ставших жертвами такой деятельности. По оценкам стран-респондентов, полиция получает сообщения о виктимизации в результате киберпреступности в одном проценте случаев или более. В одном глобальном обследовании частного сектора указано, что 80 процентов частных лиц, ставших жертвами киберпреступности, в полицию о преступлении не сообщают. Тот факт, что люди редко обращаются в полицию, объясняется тем, что они не знают о виктимизации и о механизмах сообщения информации, ощущают стыд или неловкость в связи с тем, что они стали жертвами преступников, а корпорации опасаются возможного репутационного риска. Государственные органы стран всех регионов мира сообщают об инициативах, направленных на повышение уровня представления информации о совершении преступлений, в том числе о

системах, позволяющих сообщать о преступлениях по Интернету и горячим телефонным линиям, кампаниях по повышению информированности общественности, контактах с частным сектором и активизации информационно-пропагандистской деятельности полиции и обмене информацией. Однако меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться среднесрочными и долгосрочными тактическими расследованиями в отношении рынков преступности и разработчиков преступных схем. Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах и при обмене мгновенными сообщениями и пользовании материалами совместного пользования ("P2P"). Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских преступных методов, сложностями в получении доступа к электронным доказательствам и с внутренними ограничениями в отношении ресурсов, потенциала и материально-технических возможностей. Подозреваемые часто используют технологии анонимизации и запутывания следов, и новые технологии быстро получают распространение в преступном мире благодаря онлайновым преступным рынкам.

35. Для расследования киберпреступлений правоохранительным органам необходимо использовать как традиционные, так и новые методы работы полиции. В то время как некоторые следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежит пространственный, ориентированный на предметы подход, трудно применять в ситуациях, связанных с хранением электронных данных и потоками данных в режиме реального времени. В вопроснике, подготовленном в целях проведения исследования, указывались десять методов расследования киберпреступлений начиная с таких полномочий общего характера, как проведение обыска и выемки, до специализированных методов, таких как сохранение компьютерных данных[8]. Чаще всего страны сообщали о наличии полномочий общего характера (не специально предназначенных для киберпреступлений) в отношении всех следственных мероприятий. Ряд стран также сообщили о наличии законодательных положений, касающихся непосредственно киберпреступности, в частности с целью оперативного обеспечения сохранности компьютерных данных и получения хранимых данных подписчика. Многие страны сообщили об отсутствии юридических полномочий в отношении применения более продвинутых мер, таких как удаленная компьютерно-техническая экспертиза. Хотя традиционные процессуальные полномочия могут применяться в ситуациях, связанных с

[8] Обыск компьютерного аппаратного обеспечения или компьютерных данных; выемка компьютерного аппаратного обеспечения или компьютерных данных; распоряжение о предоставлении информации о подписчиках; распоряжение о предоставлении хранимых данных о потоках информации; распоряжение о предоставлении хранимых данных о содержании; сбор в режиме реального времени данных о потоках информации; сбор в режиме реального времени информации о содержании данных; оперативное обеспечение сохранности компьютерных данных; использование удаленной компьютерно-технической экспертизы; и трансграничной доступ к компьютерной системе или данным.

киберпреступлениями, во многих случаях такой подход может также привести к возникновению правовой неопределенности и поставить под сомнение законность сбора доказательств и таким образом допустимость доказательств. В целом, национальные подходы к полномочиям по расследованию киберпреступлений являются менее единообразными, чем подход к криминализации многих киберпреступлений.

36. Независимо от правовой формы полномочий по проведению расследований все представившие ответы органы используют право производства обыска и выемки для физического изъятия компьютерного оборудования и получения компьютерных данных. Большинство стран также используют распоряжения в целях получения хранимых компьютерных данных от поставщиков услуг Интернета. Однако, за исключением европейских стран, около одной трети государств сообщают о том, что третьи стороны в расследовании трудно заставить предоставлять информацию. Около трех четвертей стран используют специальные следственные меры, такие как сбор данных в режиме реального времени или оперативное обеспечение сохранности данных. Для применения следственных мер обычно требуется минимальное количество первоначальных доказательств или сообщение о киберпреступлении. Для применения более интрузивных мер, таких как меры, связанные со сбором данных в режиме реального времени или доступом к содержанию данных, часто необходимо соблюдение более жесткого критерия, например, наличие свидетельства совершения серьезного деяния или доказательства вероятной причины или разумных оснований.

37. Особенно сложным является взаимодействие между правоохранительными органами и поставщиками услуг Интернета. Поставщики услуг располагают информацией об абонентах, счетами-фактурами, некоторыми журналами связи, информацией о местоположении (например, поставщики услуг мобильной связи имеют информацию с антенн сотовой связи) и содержании данных – все это может представлять собой важнейшие электронные доказательства совершения преступления. Обязательства, предусмотренные национальным законодательством, и политика в области хранения и раскрытия данных в частном секторе значительно различаются в зависимости от страны, отрасли и вида данных. Страны сообщают, что чаще всего получение доказательств от поставщиков услуг осуществляется на основе судебных распоряжений. Однако в некоторых случаях правоохранительным органам удается напрямую получить сохраненные данные об абоненте, данные о трафике и даже информацию о содержании данных. В этой связи организации частного сектора часто сообщают как о базовой политике соблюдения надлежащей правовой процедуры в вопросах раскрытия данных, так и о добровольном выполнении в определенных обстоятельствах прямых запросов правоохранительных органов. Неофициальные отношения между правоохранительными органами и поставщиками услуг, о существовании которых сообщают более половины всех представивших ответы стран, помогают в процессе обмена информацией и укреплении доверия. Ответы свидетельствуют о необходимости нахождения баланса между конфиденциальностью и соблюдением процессуальных норм, позволяющего своевременно раскрывать доказательства, с тем чтобы частный сектор не превратился в непреодолимое препятствие при проведении расследований.

38. Расследование киберпреступлений неизменно сопряжено с соображениями обеспечения неприкосновенности частной жизни в соответствии с положениями международного права в области прав человека. Согласно нормам в области прав человека в законодательстве достаточно ясно должны быть изложены обстоятельства, при которых власти имеют право применять те или иные следственные действия, и должны существовать надлежащие и эффективные гарантии недопущения злоупотреблений. Страны сообщают о том, что национальное законодательство защищает право на неприкосновенность частной жизни, а также о ряде ограничений и гарантий в связи с проведением расследований. Однако в случае проведения транснациональных расследований из-за расхождений в уровне защиты возникает непредсказуемость в отношении возможности доступа к данным со стороны иностранных правоохранительных органов и потенциальные юрисдикционные пробелы в режимах защиты неприкосновенности частной жизни.

39. Свыше 90 процентов ответивших на вопросник стран приступили к созданию специализированных структур для расследования киберпреступлений и преступлений, связанных с электронными доказательствами. Однако в развивающихся странах на эту деятельность выделяется недостаточно ресурсов, и ощущается недостаточность потенциала. В странах с низким уровнем развития в полиции значительно меньше специалистов: примерно 0,2 специалиста на 100 000 пользователей Интернета в стране. В развитых странах этот показатель от двух до пяти раз выше. Согласно полученной информации, семьдесят процентов специализированных сотрудников правоохранительных органов в менее развитых странах не обладают необходимыми навыками работы с компьютером и не имеют оборудования, и только половина сотрудников проходят подготовку более чем один раз в год. Свыше половины представивших ответы стран Африки и одна треть стран Северной и Южной Америки сообщают, что правоохранительные органы не располагают достаточными ресурсами для расследования киберпреступлений. На общемировом уровне картина, вероятно, еще хуже. В рамках проведения данного исследования ответы, к примеру, представили лишь 20 процентов из 50 наименее развитых стран в мире. Все представившие ответы страны Африки и более 80 процентов стран Северной и Южной Америки, Азии и Океании сообщили, что они нуждаются в технической помощи. Наиболее часто упоминалась необходимость оказания технической помощи в такой области, как общие методы расследования киберпреступлений. Из стран, нуждающихся в помощи, 60 процентов указали, что в помощи нуждаются правоохранительные органы.

6. Электронные доказательства и меры в области уголовного правосудия

40. Доказательства представляют собой средства, при помощи которых в ходе судебного разбирательства устанавливаются факты, касающиеся виновности или невиновности лица. Электронные доказательства – это все средства такого рода, существующие в электронной (или цифровой) форме. Они могут представлять собой хранимые или временные данные. Они могут существовать в виде компьютерных файлов, передач, журналов, метаданных или сетевых данных. Судебная цифровая экспертиза предполагает восстановление зачастую неустойчивой и легко подверженной искажению информации, которая может

иметь доказательную ценность. Методы судебной экспертизы включают создание копий хранимой и удаленной информации по принципу "бит в бит", "блокировку записи" в целях недопущения внесения изменений в исходные данные и использование криптографических хэш-кодов или цифровых подписей, которые показывают наличие изменений в информации. Почти все страны сообщили о наличии определенных возможностей в области судебной цифровой экспертизы. В то же время многие страны-респонденты, представляющие все регионы, отмечают нехватку судебных экспертов, различия в возможностях, имеющихся на федеральном уровне и на уровне субъектов федерации, отсутствие инструментов для проведения судебной экспертизы и задержки из-за огромного количества данных, которые необходимо проанализировать. Половина стран сообщают, что подозреваемые пользуются шифрованием, что затрудняет и задерживает получение доступа к такого рода доказательствам без ключа расшифрования. В большинстве стран анализом электронных доказательств занимаются правоохранительные органы. Однако прокурорам необходимо изучить и понять электронные доказательства, чтобы доказать свою версию в суде. Все страны Африки и одна треть стран в других регионах сообщают о том, что прокуратура не располагает для этого достаточными ресурсами. У сотрудников прокуратуры навыки работы с компьютером обычно ниже, чем у следователей. Во всем мире около 65 процентов стран-респондентов сообщают о той или иной форме специализации сотрудников прокуратуры в вопросах киберпреступности. Лишь 10 процентов стран сообщают о наличии специализированных судебных служб. Подавляющее большинство дел о киберпреступности рассматривают судьи, не являющиеся специалистами в этой области, которые в 40 процентах стран-респондентов не проходят никакого обучения по вопросам, связанным с киберпреступностью. Особо приоритетную задачу представляет собой подготовка сотрудников судебной системы в области законодательства по борьбе с киберпреступностью, сбора доказательств и базового и углубленного компьютерного обучения.

41. Свыше 60 процентов стран, представивших ответы, не проводят юридического различия между электронными доказательствами и вещественными доказательствами. Хотя подходы различаются, многие страны считают это оптимальной практикой, поскольку такой подход обеспечивает достаточную допустимость доказательств наряду со всеми другими видами доказательств. Ряд неевропейских стран не признают электронные доказательства вообще, в результате чего судебное преследование киберпреступлений, равно как и любых других преступлений, доказательством которых является электронная информация, невозможно. В то время как обычно в странах не имеется отдельных правил доказывания в отношении электронных доказательств, ряд стран назвали следующие принципы: правило наилучших доказательств, относимость доказательств, правило в отношении показаний с чужих слов, подлинность и целостность – все они могут быть непосредственно применимы к электронным доказательствам. Многие страны подчеркивают сложность отнесения деяний на счет конкретного лица и отмечают, что это часто зависит от косвенных доказательств.

42. Ввиду проблем, с которыми приходится сталкиваться следователям правоохранительных органов и сотрудникам прокуратуры, показатели привлечения лиц, виновных в совершении киберпреступлений, к судебной

ответственности низки. Число подозреваемых, выявленных в связи с зарегистрированными полицией преступлениями, связанными с детской порнографией, сопоставимо с ситуацией в отношении других преступлений сексуального характера, однако, доля подозреваемых в совершении таких зарегистрированных полицией преступлений, как незаконный доступ и компьютерное мошенничество или подлог, составляет лишь 25 подозреваемых на 100 преступлений. Очень немногие страны смогли представить данные о числе лиц, подвергнутых преследованию в судебном порядке, или осужденных. Однако данные в отношении киберпреступлений в одной стране показывают, что соотношение числа осужденных и зарегистрированных преступлений значительно ниже, чем в случае других "обычных" преступлений.

7. Международное сотрудничество

43. Страны, представившие ответы на вопросник, подготовленный в целях проведения исследования, сообщают, что от 30 до 70 процентов киберпреступлений носят транснациональный характер и связаны с вопросами проведения транснациональных расследований, суверенитета, юрисдикции, экстерриториальных доказательств и необходимостью международного сотрудничества. Киберпреступления приобретают транснациональный характер в том случае, если какой-либо элемент или существенное последствие преступления проявляются на территории другой страны или если часть совершения преступления происходит на территории другой страны. Международное право предусматривает ряд оснований для юрисдикции в отношении таких деяний, в том числе различные виды юрисдикции по территориальному принципу и юрисдикции на основе гражданства. Некоторые из этих оснований закреплены в многосторонних документах по предупреждению киберпреступности. Хотя все страны Европы считают, что национальное законодательство обеспечивает достаточную основу для криминализации и преследования экстерриториальных киберпреступлений, около одной трети до более чем половины стран в других регионах мира указывают, что правовая база является недостаточно развитой. В законодательстве многих стран нашла отражение идея о том, что для признания территориальной юрисдикции внутри страны должно быть совершено не обязательно "все" преступление. Территориальная привязка может быть произведена в отношении элементов или последствий деяния, а также места нахождения компьютерных систем или данных, используемых для совершения преступления. В случае возникновения юрисдикционных конфликтов они обычно разрешаются с помощью проведения между странами официальных и неофициальных консультаций. Пока что ответы стран не свидетельствуют о какой-либо необходимости в дополнительных формах юрисдикции в отношении некоего условного измерения "киберпространства". Напротив, формы юрисдикции по территориальному признаку и на основе гражданства почти всегда способны обеспечить достаточную связь между киберпреступлениями и хотя бы одним государством.

44. Формы международного сотрудничества включают выдачу, оказание взаимной правовой помощи, взаимное признание иностранных судебных решений и неофициальное сотрудничество между органами полиции различных стран. Ввиду неустойчивого характера электронных доказательств в

рамках международного сотрудничества в уголовных вопросах в области киберпреступности необходимо своевременное представление ответов и наличие возможности обращаться с просьбой о проведении специализированных следственных действий, таких как сохранение компьютерных данных. В вопросах получения экстерриториальных доказательств в контексте дел, связанных с киберпреступлениями, преобладают традиционные формы сотрудничества: свыше 70 процентов стран, представивших ответы, сообщают, что они используют для этих целей официальные просьбы об оказании взаимной правовой помощи. В рамках такого официального сотрудничества в случае почти 60 процентов просьб в качестве правовой основы используются двусторонние документы. Многосторонние документы используются в 20 процентах случаев. Время представления ответов в рамках официальных механизмов составляет, согласно полученной информации, порядка нескольких месяцев в случае просьб как о выдаче, так и об оказании взаимной правовой помощи – такой срок создает проблемы в деле сбора неустойчивых электронных доказательств. Шестьдесят процентов стран Африки, Северной и Южной Америки и Европы и 20 процентов стран Азии и Океании сообщают о наличии каналов для направления срочных просьб. Однако неизвестно, насколько такие просьбы позволяют сократить срок представления ответа. Примерно две трети из представивших ответы стран имеют возможность прибегать к различным видам неофициального сотрудничества, хотя политика в отношении использования таких механизмов существует лишь в немногих странах. Существенным потенциалом в деле сокращения срока представления ответов обладают инициативы в области неофициального сотрудничества и содействия официальному сотрудничеству, таких как круглосуточные сети. Однако они используются в недостаточной мере – на них приходится около 3 процентов общего числа дел о киберпреступности, с которыми имеют дело правоохранительные органы представивших ответы стран.

45. Официальные и неофициальные каналы сотрудничества предназначены для регулирования процесса получения согласия государства на проведение иностранными правоохранительными органами расследований, затрагивающих суверенитет государства. Однако следователи, сознательно или бессознательно, все чаще обращаются к экстерриториальным данным в процессе сбора доказательств, не испрашивая согласия государства, в котором физически находятся эти данные. Эта ситуация возникает, в частности, в связи с облачными компьютерными технологиями, предполагающими хранение данных в нескольких центрах данных в различных географических точках. Хотя "местонахождение" данных технически может быть установлено, оно приобретает все более искусственный характер, вплоть до того, что даже традиционные просьбы об оказании взаимной правовой помощи будут часто направляться в страну места нахождения поставщика услуг, а не страну, в которой физически расположен центр данных. Иностранные правоохранительные органы могут использовать прямой доступ к экстерриториальным данным в тех случаях, когда следователи используют существующее "живое" подключение с устройства подозреваемого или когда следователи используют полученное законным образом разрешение на доступ к данным. Следователи правоохранительных органов иногда могут получать данные от экстратерриториальных поставщиков услуг посредством

неофициального прямого запроса, хотя поставщики услуг обычно требуют соблюдения надлежащей правовой процедуры. В соответствующих положениях о "трансграничном" доступе, содержащихся в Конвенции о киберпреступности Совета Европы и Конвенции о преступлениях в области информационных технологий Лиги арабских государств, такие ситуации учитываются не в полной мере, поскольку упор в них делается на "согласие" лица, правомочного раскрывать данные, и предполагается, что в момент доступа к данным или получения данных известно место их нахождения.

46. Ввиду нынешней ситуации в области международного сотрудничества возникает риск образования страновых группировок, в рамках которых существуют необходимые полномочия и процедуры для сотрудничества между входящими в их состав странами, но которые по отношению ко всем другим странам ограничиваются "традиционными" видами международного сотрудничества, не учитывающими особенности электронных доказательств и глобальный характер киберпреступности. Это особенно касается сотрудничества при проведении расследований. Отсутствие общего подхода, в том числе в рамках существующих многосторонних договоров в области киберпреступности, означает, что могут возникать трудности в выполнении просьб о принятии таких мер, как оперативное обеспечение сохранности данных в странах, не входящих в число стран, несущих международные обязательства в отношении обеспечения такого механизма и его задействования в случае поступления запроса. Включение таких полномочий в проект Конвенции о кибербезопасности Африканского союза может в некоторой степени способствовать ликвидации этого пробела. Во всем мире расхождения в сфере охвата положений в отношении сотрудничества, содержащихся в многосторонних и двусторонних документах, отсутствие обязательства представлять ответ в течение определенного срока, отсутствие договоренности о допустимом прямом доступе к экстерриториальным данным, большое число неофициальных сетей правоохранительных органов и различия в гарантиях сотрудничества представляют собой серьезные проблемы в деле обеспечения эффективного международного сотрудничества в области электронных доказательств по уголовным делам.

8. Предупреждение киберпреступности

47. Предупреждение преступности состоит из стратегий и мер, направленных на снижение риска совершения преступлений и нейтрализацию потенциально вредных последствий для частных лиц и общества. Почти 40 процентов представивших ответы стран сообщают о наличии национального законодательства или политики в области предупреждения киберпреступности. Еще в 20 процентах стран ведется разработка инициатив. Страны отмечают, что к числу оптимальных видов практики в области предупреждения киберпреступности относятся принятие законов, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно-просветительская деятельность, создание прочной базы знаний и сотрудничество между органами государственного управления, общинами, частным сектором и на международном уровне. Более половины стран сообщают о наличии стратегий противодействия киберпреступности. Во многих случаях стратегии противодействия киберпреступности являются неотъемлемой частью стратегий обеспечения кибербезопасности. Примерно в

70 процентах всех национальных стратегий, о которых была предоставлена информация, присутствуют компоненты, связанные с информационно-пропагандистской деятельностью, международным сотрудничеством и потенциалом правоохранительных органов. В том что касается координации, ответы свидетельствуют о том, что чаще всего ведущими учреждениями в области борьбы с киберпреступностью являются правоохранительные органы и органы прокуратуры.

48. Обследования, в том числе проведенные в развивающихся странах, показывают, что большинство индивидуальных пользователей Интернета в настоящее время принимают основные меры предосторожности. Представившие ответы правительства, организации частного сектора и научные учреждения подчеркивают сохраняющееся значение информационно-просветительских кампаний, в том числе кампаний по вопросам новых угроз и кампаний, ориентированных на конкретные целевые группы, например, детей. Наибольшая эффективность обучения пользователей достигается в случае сочетания обучения с системами, которые помогают пользователям безопасным образом достичь своих целей. Если затраты пользователей превышают непосредственную получаемую ими выгоду, у людей пропадает стимул применять меры безопасности. Организации частного сектора также сообщают, что осведомленность пользователей и сотрудников должна являться частью комплексного подхода к обеспечению безопасности. Указываются следующие основополагающие принципы и оптимальные виды практики: ответственность за повышение осведомленности, политика и практические меры в области управления рисками, руководство на уровне советов директоров и профессиональная подготовка сотрудников. Две трети респондентов из числа организаций частного сектора провели оценку риска киберпреступности, и большинство сообщают об использовании таких технологий обеспечения кибербезопасности, как межсетевая защита, сохранение цифровых доказательств, идентификация содержания данных, обнаружение вторжений и контроль и мониторинг системы. В то же время была выражена озабоченность тем, что малые и средние предприятия либо не принимают достаточных мер для защиты систем или ошибочно считают, что они не станут мишенью преступников.

49. Важную роль в предупреждении киберпреступности играет нормативно-правовая база – как в отношении частного сектора в целом, так и в отношении поставщиков услуг в частности. Почти в половине стран приняты законы о защите данных, которые предусматривают требования в отношении защиты и использования персональных данных. Некоторые из этих режимов содержат конкретные требования к поставщикам услуг Интернета и другим поставщикам электронных средств связи. Хотя законы о защите данных требуют удалять персональные данные, если они более не требуются, в некоторых странах сделаны исключения для целей уголовных расследований, согласно которым поставщики услуг Интернета обязаны хранить определенные виды данных в течение определенного срока. Во многих развитых странах имеются также правила, требующие от организаций в случае утечки данных уведомлять частных лиц и регулирующие органы. Поставщики услуг Интернета обычно несут ограниченную ответственность как "простые каналы передачи" данных. Модификация передаваемого содержания данных повышает степень ответственности, равно как и фактическое или

предполагаемое знание о незаконной деятельности. С другой стороны, оперативное принятие мер после получения уведомления снижает степень ответственности. Несмотря на наличие технических возможностей, позволяющих поставщикам услуг фильтровать содержание Интернета, при ограничении доступа к Интернету должны соблюдаться критерии предсказуемости и соразмерности, предусматриваемые международным правом в области прав человека, которое защищает право искать, получать и передавать информацию.

50. Центральным элементом в деле предупреждения киберпреступности является государственно-частное партнерство. О наличии такого партнерства сообщают более половины всех стран. Это партнерство в равной степени создается как на основании неофициальных договоренностей, так и на юридической основе. Чаще всего партнерские отношения устанавливаются с организациями частного сектора, за ними следуют научные учреждения и международные и региональные организации. Партнерские отношения в основном используются для облегчения обмена информацией об угрозах и тенденциях, а также для деятельности по предупреждению киберпреступности и принятия мер в конкретных случаях. В контексте некоторых государственно-частных партнерств организации частного сектора применяют упреждающий подход к проведению расследований и обращению в судебные органы для борьбы с киберпреступностью. Такие меры дополняют усилия правоохранительных органов и могут помочь снизить причиняемый жертвам ущерб. Научные организации выполняют 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 нахождения решений. В университетах работают и используют имеющиеся возможности эксперты по киберпреступности, различные группы реагирования на компьютерные инциденты и специализированные научно-исследовательские центры.

B. Резюме основных выводов исследования

51. Основные выводы, сделанные по итогам всестороннего исследования проблемы киберпреступности, включают следующее:

a) возможно, существует корреляция между фрагментацией усилий на международном уровне и различиями в национальных законах о противодействии киберпреступности, с одной стороны, и наличием различных документов с разным тематическим и географическим охватом, с другой. Хотя в документах совершенно справедливо отражены социально-культурные и региональные различия, расхождения в степени процессуальных полномочий и положениях, касающихся международного сотрудничества, могут привести к возникновению групп сотрудничающих между собой стран, что не всегда целесообразно ввиду глобального характера киберпреступности;

b) применение традиционных средств официального международного сотрудничества в вопросах противодействия киберпреступности в настоящее время не позволяет обеспечить своевременное реагирование, необходимое для

получения неустойчивых электронных доказательств. Поскольку преступления все чаще связаны с электронными доказательствами, разбросанными по всему миру, эта проблема будет касаться не только киберпреступности, но и всех преступлений в целом;

c) в мире облачных вычислений и центров данных необходимо по-новому подойти к концепции роли "местонахождения" доказательств, в том числе с целью достижения консенсуса по вопросам, касающимся прямого доступа правоохранительных органов к экстерриториальным данным;

d) анализ доступных национальных нормативно-правовых баз свидетельствует о недостаточной унификации "основных" правонарушений, связанных с киберпреступностью, полномочий по проведению расследований и допустимости электронных доказательств. Международное право в области прав человека представляет собой важную внешнюю точку отсчета в вопросах криминализации и процессуальных требований;

e) сотрудники правоохранительных органов, прокуратуры и судебных органов в развивающихся странах нуждаются в долгосрочной, устойчивой, всеобъемлющей технической поддержке и помощи для расследования киберпреступлений и противодействия киберпреступности;

f) во всех странах необходимо наращивать усилия по предупреждению киберпреступности на основе комплексного подхода, предусматривающего дальнейшее повышение осведомленности, создание отношений партнерства между государственными и частными организациями и интеграцию стратегий противодействия киберпреступности в более широкую проблематику обеспечения кибербезопасности.

C. Резюме содержащихся в исследовании вариантов возможных действий

52. Представленные в исследовании варианты возможных действий были разработаны ЮНОДК на основе полученных от стран ответов на включенный в вопросник, подготовленный в целях проведения исследования, вопрос относительно возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или других мер по противодействию киберпреступности, а также с учетом его основных выводов. В исследовании делается вывод, что варианты возможных действий могут включать одну или несколько из следующих мер[9]:

a) разработку международных типовых положений по криминализации базовых деяний в области киберпреступности с целью оказания государствам помощи в ликвидации безопасных убежищ путем согласования единообразных составов преступлений;

b) разработку международных типовых положений о полномочиях в области использования электронных доказательств при проведении расследований с целью оказания помощи государствам в обеспечении

[9] Более подробная информация приводится в документе UNODC/CCPCJ/EG.4/2013/2.

необходимых процессуальных средств для расследования преступлений, связанных с электронными доказательствами;

c) разработку типовых положений по вопросу о юрисдикции с целью заложить единую эффективную основу в отношении юрисдикции в уголовных вопросах, связанных с киберпреступностью;

d) разработку типовых положений по международному сотрудничеству в области использования электронных доказательств с целью включения их в двусторонние и многосторонние документы, включая пересмотренный Типовой договор Организации Объединенных Наций о взаимной правовой помощи, в соответствии с рекомендациями, изложенными в Руководстве для дискуссии тринадцатого Конгресса по предупреждению преступности и уголовному правосудию;

e) разработку многостороннего документа по международному сотрудничеству в области использования электронных доказательств в уголовных делах с целью создания международного механизма, обеспечивающего своевременное сотрудничество в деле сохранения и получения электронных доказательств;

f) разработку всеобъемлющего многостороннего документа о противодействии киберпреступности с целью выработки международного подхода в области криминализации, процессуальных полномочий, юрисдикции и международного сотрудничества;

g) укрепление международных, региональных и национальных партнерских отношений, в том числе с частным сектором и научными учреждениями, с целью оказания эффективной технической помощи в области предупреждения и противодействия киберпреступности в развивающихся странах.

V. Рекомендации в отношении содействия деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала

53. Комиссия может пожелать, в частности, с учетом деятельности ЮНОДК, о которой говорится в разделе II настоящего доклада, обратиться к ЮНОДК с просьбой продолжать оказывать государствам-членам техническую помощь в борьбе с киберпреступностью, и настоятельно призвать государства-члены предоставить для этого внебюджетные ресурсы с целью обеспечения долгосрочного устойчивого наращивания потенциала в области борьбы с киберпреступностью в развивающихся странах.