Организация Объединенных Наций A/CONF.213/9

# Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию

Distr.: General
22 February 2009
Russian
Original: English

**Сальвадор, Бразилия, 12-19 апреля 2010 года**

Пункт 8 предварительной повестки дня*
**Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности**

## Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности

### Рабочий документ, подготовленный Секретариатом

## I. Введение

1. Тот факт, что киберпреступность занимает столь видное место в повестке дня двенадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, свидетельствует о неизменной актуальности и серьезности данной проблемы – несмотря на то, что дискуссии на эту тему ведутся уже почти полвека.

2. На протяжении последних 50 лет разрабатывались и обсуждались разнообразные подходы к решению проблемы киберпреступности. Однако решить ее до сих пор не удалось, отчасти из-за постоянного развития техники, вместе с которой меняются и методы совершения "киберпреступлений".

3. В 1960-1980 годах государствам пришлось столкнуться с новыми видами деяний – такими, как манипуляции с компьютерными системами и компьютерный шпионаж, – которые зачастую не подпадали под действующее

* A/CONF.213/1.

V.10-50384 (R)

уголовное законодательство. В то время главной темой дискуссий была разработка в этой связи соответствующих законодательных мер[1].

4. Появление в 1990-е годы графического интерфейса для работы с ЭВМ и последовавший за этим стремительный рост числа пользователей Интернета привели к возникновению новых проблем. Информация, на законных основаниях размещенная в сети в одной стране, стала доступной в любой точке земного шара, в том числе в странах, где ее публикация противоречит закону. Начала вызывать тревогу и такая особенность компьютерных сетей, как быстрота информационного обмена, создающая сложности прежде всего при расследовании преступлений транснационального характера[2].

5. В первом десятилетии двадцать первого века на передний план вышли новые, более изощренные методы совершения преступлений (такие как фишинг[3] и атаки с использованием бот-сетей[4]), а также технологии, еще сильнее затрудняющие получение сотрудниками правоохранительных органов необходимой следственной информации (например, протоколы голосовой связи по Интернету и "сетевые облака").

# II. Проблемы, связанные с киберпреступностью

## A. Неясность масштабов

6. Несмотря на технический прогресс и активные усилия по расследованию нарушений, масштабы использования информационных технологий в противозаконных целях остаются неизменными или даже растут. По данным некоторых провайдеров услуг электронной почты, от 75 до 90 процентов всех пересылаемых сообщений представляют собой спам[5]. Аналогичные цифры,

---

[1] См. Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1976) и Ulrich Sieber, *Computerkriminalität und Strafrecht* (Cologne, Karl Heymanns Verlag, 1977).

[2] О последствиях ускоренного обмена данными с точки зрения расследования киберпреступлений см.: Международный союз электросвязи. *Понимание киберпреступности: руководство для развивающихся стран* (Женева, 2009 год). Размещено по адресу http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

[3] Согласно определению, приведенному Международным союзом электросвязи в публикации *"Понимание киберпреступности: руководство для развивающихся стран"* (см. сноску 2), под фишингом понимаются действия, имеющие целью побудить жертву к раскрытию личной или секретной информации. Термин "фишинг" (от английского слова fishing, обозначающего рыбную ловлю – прим. пер.) изначально относился к рассылке по электронной почте сообщений, предназначенных для "выуживания" паролей и финансовых данных из "моря" пользователей Интернета. Сочетание букв "ph", используемое в латинском написании этого термина (phishing), соответствует особой орфографии, популярной среди хакеров.

[4] Бот-сеть – группа компьютеров, зараженных программой, которая позволяет посторонним лицам управлять ими удаленно. См. Clay Wilson, "Botnets, cybercrime and cyberterrorism: vulnerabilities and policy issues for Congress", Congressional Research Service Report RL32114, последняя версия от 29 января 2008 года, размещено по адресу www.fas.org/sgp/crs/terror/RL32114.pdf.

[5] В 2009 году Рабочая группа по борьбе со злоупотреблением рассылкой сообщений (http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf),

свидетельствующие о сохранении или возрастании объемов, публикуются и в отношении других, более распространенных видов противозаконной деятельности. Так, организация "Интернет уотч фаундейшн" в своем издании "Annual and Charity Report" за 2008 год приводит данные о практически не изменившемся с 2006 по 2008 год количестве коммерческих веб-сайтов, которые, согласно проверенной информации, используются для распространения детской порнографии.

7. Хотя статистические данные полезны для привлечения внимания к серьезному характеру данной проблемы или к ее дальнейшему усугублению, одна из главных трудностей борьбы с киберпреступностью заключается в отсутствии надежной информации о масштабах этого явления, а также о случаях ареста, привлечения к ответственности и наказания виновных. Криминальная статистика часто не содержит информации по отдельным видам преступлений, а те скудные сведения о последствиях киберпреступности, которые можно почерпнуть из публикуемых данных, как правило, недостаточно подробны для того, чтобы руководство могло составить достоверное представление о распространенности и масштабах таких правонарушений[6]. Отсутствие подобной информации затрудняет количественную оценку воздействия киберпреступности на жизнь общества и выработку стратегий решения данной проблемы[7].

8. Одна из причин нехватки статистической информации состоит в том, что объем финансовых потерь, вызванных действиями киберпреступников, и количество совершаемых ими правонарушений с трудом поддаются оценке. По данным из некоторых источников, убытки, причиняемые киберпреступностью коммерческим структурам и другим организациями в Соединенных Штатах Америки[8], оцениваются не менее чем в 67 млрд. долл. США в год. Вместе с тем нельзя с уверенностью считать корректными цифры, полученные путем экстраполяции результатов выборочного опроса[9]. Этот методологический упрек можно отнести не только к данным об убытках, но и к количеству зафиксированных правонарушений[10]. Неясным остается также то, какой процент потерпевших заявляют о совершенных против них киберпреступлениях. Хотя официальные органы, ведущие борьбу с киберпреступностью, призывают ее жертв сообщать о фактах преступлений, существует опасение, что некоторые из них, особенно в финансовом секторе (т.е. банки), не раскрывают такую информацию из опасения, что распространение негативных сведений подобного рода нанесет ущерб их репутации[11]. Если компания объявит, что ее сервер был взломан хакерами, то клиенты могут утратить к ней доверие, и в результате совокупные издержки и другие последствия по своей тяжести могут даже

---

представила информацию, согласно которой спам составляет до 85 процентов всех сообщений, пересылаемых по электронной почте.

[6] United States of America, Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO report GAO-07-705 (Washington, D.C., June 2007), p. 22; и Ian Walden, *Computer Crimes and Digital Investigations* (Oxford, Oxford University Press, 2007).

[7] Walden, *Computer Crimes and Digital Investigations*.

[8] United States, Federal Bureau of Investigation, *2005 FBI Computer Crime Survey*, p. 10.

[9] *Понимание киберпреступности: руководство для развивающихся стран* (см. сноску 2).

[10] Там же.

[11] Neil Mitchison and Robin Urry, "Crime and abuse in e-business", *IPTS Report*, vol. 57, September 2001.

превзойти потери, вызванные самой хакерской атакой. Кроме того, подвергающиеся таким атакам пользователи не всегда верят в способность правоохранительных органов найти виновных. С другой стороны, если не сообщать о правонарушениях и не привлекать преступников к ответственности, они могут пойти на новые преступления.

9. Еще одна трудность, связанная со статистическими выкладками, обусловлена зачастую неоднократным цитированием ненадежной или не поддающейся проверке информации. Одним из примеров являются статистические данные о коммерческих аспектах распространения детской порнографии в Интернете. В нескольких аналитических обзорах упоминалось, что ежегодный общемировой доход от детской порнографии в сети составляет 2,5 млрд. долл. США[12]. Однако источник, откуда была позаимствована эта цифра (www.toptenreviews.com), не содержит никакой информации о методах исследования, на котором она основана. При этом текст на веб-сайте данной компании ("Здесь Вы найдете всю информацию, нужную Вам, чтобы делать покупки с умом. Мы рекомендуем лучший товар в каждой из категорий. Наши сравнительные таблицы, новости, обзоры и видеоматериалы облегчают покупателям правильный выбор") заставляет серьезно усомниться в надежности приводимых ею сведений. В другом случае журналист "Уолл-стрит джорнал"[13], решивший в 2006 году проверить утверждение о том, что бизнес на детской порнографии приносит 20 млрд. долл. США в год, обнаружил, что два основных документа, в которых назывались суммы таких доходов в диапазоне от 3 до 20 млрд. долл. США (публикация Национального центра США по делам пропавших и эксплуатируемых детей и публикация Совета Европы), содержат ссылки на учреждения, где эти данные подтвердить не смогли.

## B. Транснациональный аспект

10. Киберпреступность носит в значительной степени транснациональный характер. Первоначально Интернет был задуман как сеть военного назначения с рассредоточенной архитектурой. Такая сетевая архитектура и возможность глобального доступа к соответствующим услугам часто придают киберпреступлениям международный аспект. Электронные письма с запрещенными материалами без труда пересылаются по адресам в целом ряде государств, даже когда их исходный отправитель и конечный получатель находятся в одной и той же стране, например, если отправитель либо получатель пользуются услугами зарубежного провайдера электронной почты. Тот факт, что клиентами некоторых популярных провайдеров, предоставляющих почтовые услуги бесплатно, являются миллионы людей на всей планете, дополнительно подчеркивает транснациональные масштабы киберпреступности.

11. Трудности расследования киберпреступлений, вытекающие из их транснационального характера, аналогичны тем, которые возникают в связи с

[12] Kim-Kwang Choo, Russel G. Smith and Rob McCusker, "Future directions in technology-enabled crime: 2007-09", Research and Public Policy Series, No. 78 (Canberra, Australian Institute of Criminology, 2007), p. 62; ECPAT International, *Violence against Children in Cyberspace* (Bangkok, 2005), p. 54; Council of Europe, *Organised Crime Situation Report 2005: Focus on the Threat to Economic Crime* (Strasbourg, December 2005), p. 41.

[13] Carl Bialik, "Measuring the child-porn trade", *Wall Street Journal*, 18 April 2006.

другими видами трансграничной преступности. В силу основополагающего принципа национального суверенитета, согласно которому расследования на территории других государств могут проводиться только с разрешения их властей, тесное сотрудничество между соответствующими государствами жизненно важно для раскрытия киберпреступлений. Еще одна серьезная трудность связана с крайней ограниченностью времени, которым располагает следствие в делах о киберпреступлениях. В отличие от запрещенных наркотиков, доставка которых к месту назначения может, в зависимости от используемых видов транспорта, занимать до нескольких недель, электронные сообщения передаются за считанные секунды, а для загрузки больших по объему файлов при достаточной скорости подключения требуется всего несколько минут.

12. Решающее значение имеют также своевременность и эффективность взаимодействия между государственными органами разных стран, поскольку следы киберпреступлений во многих случаях уничтожаются автоматически через короткое время. Затяжные формальности при этом могут сильно помешать расследованию.

13. Многие из существующих соглашений о взаимной правовой помощи по-прежнему предусматривают сложные и зачастую весьма длительные формальные процедуры. Крайне важной задачей представляется поэтому введение процедур ускоренного реагирования на соответствующие инциденты и запросы об оказании международного содействия.

14. Набор принципов для формирования правовой основы международного сотрудничества в области расследования киберпреступлений содержится, в частности, в главе III Конвенции Совета Европы о киберпреступности[14]. В этой главе говорится о растущем значении международного сотрудничества (ст. 23-35) и о целесообразности использования быстродействующих средств связи, включая факсимильную связь и электронную почту (пункт 3 ст. 25). Кроме того, каждой стороне Конвенции предлагается создать у себя контактный пункт, который должен ежедневно и в любое время суток реагировать на обращения государств за помощью (ст. 35). Другие возможные подходы изложены в проекте международной конвенции об усилении защиты от киберпреступности и терроризма, а также в подготовленной Международным союзом электросвязи (МСЭ) подборке материалов для разработки законодательства о киберпреступности.

## C. Различия в подходах на уровне национального законодательства

15. Одним из практических следствий сетевой архитектуры Интернета является то, что преступники не обязательно должны находиться в том месте, где ими совершаются киберпреступления. Поэтому ключевым аспектом предупреждения киберпреступности стала необходимость лишить преступников безопасного укрытия[15]. Пользуясь такими укрытиями, правонарушители чинят

[14] Council of Europe, *European Treaty Series*, No. 185. См. также "пояснительный доклад" к этой конвенции.

[15] Как Генеральная Ассамблея в своей резолюции 55/63, так и страны Большой восьмерки в принятых на совещании министров юстиции и внутренних дел этих стран в Вашингтоне,

препятствия расследованию. Хорошо известен пример с компьютерным червем "Love Bug", созданным на Филиппинах в 2000 году[16], которым, как сообщалось, были заражены миллионы компьютеров по всему миру[17]. При этом проведению следственных действий на месте мешало то, что на Филиппинах тогда отсутствовали надлежащие положения об уголовной ответственности за умышленную разработку и распространение вредоносного программного обеспечения.

16. Вопрос об уменьшении расхождений в законодательстве весьма актуален, так как режим взаимной правовой помощи во многих странах основывается на принципе двойной криминализации, согласно которому преследуемое деяние должно быть уголовно наказуемым как в государстве, обращающемся за помощью, так и в государстве, оказывающем ее[18]. Расследования в глобальных масштабах могут, как правило, проводиться лишь в отношении действий, влекущих за собой уголовную ответственность во всех затронутых ими странах. Хотя существует целый ряд преступлений, виновники которых могут быть привлечены к суду в любой стране мира, региональные особенности играют весьма важную роль. Например, круг материалов, публикация которых противоречит закону, является различным в разных странах[19], а это означает, что на сервере в одной стране могут легально размещаться материалы, запрещенные по законам другой[20].

17. Используемые сегодня во всем мире компьютеры и компьютерные сети в техническом отношении по существу не отличаются друг от друга. Если не

---

О.К., 10 декабря 1997 года принципах и плане действий по борьбе с высокотехнологичными преступлениями (размещены по адресу www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf), подчеркивали необходимость обеспечить, чтобы лица, преступно злоупотребляющие информационными технологиями, не могли укрываться где бы то ни было.

[16] United States, General Accountability Office, Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, testimony given before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, United States Senate, GAO report GAO/T-AIMD-00-181 (Washington, D.C., May 2000).

[17] "Police close in on Love Bug culprit" *BBC News*, 6 May 2000. Размещено по адресу http://news.bbc.co.uk/2/hi/science/nature/738537.stm.

[18] О принципе двойной криминализации при расследовании киберпреступлений см. Руководство Организации Объединенных Наций по предупреждению преступлений, связанных с использованием компьютеров, и борьбе с ними (*Международный обзор уголовной политики*, №№ 43 и 44 (издание Организации Объединенных Наций, в продаже под № R.94.IV.5)), стр. 269, и обзорный доклад Stein Schjølberg and Amanda Hubbard, "Harmonizing national legal approaches on cybercrime", p. 5, представленный на тематическом совещании МСЭ по вопросам компьютерной безопасности, проходившем в Женеве 28 июня 1 июля 2005 года.

[19] Различия в правовых подходах к регулированию контента являются одной из причин того, что некоторые аспекты размещения в сети запрещенных законом материалов не охвачены Конвенцией о киберпреступности, но рассматриваются в дополнительном протоколе. См. также *Понимание киберпреступности: руководство для развивающихся стран*, глава 2.5 (см. сноску 2).

[20] О различиях в национальных подходах к уголовной ответственности за детскую порнографию см., например, Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung* (Bonn, Forum Verlag Godesberg, 1999).

считать различных языковых версий и конструкции блоков сетевого питания, компьютеры и сотовые телефоны, продающиеся в Азии, практически идентичны тем, которые можно купить в Европе. Аналогичная ситуация сложилась и с Интернетом. Благодаря стандартизации сетевые протоколы, используемые в африканских странах, не отличаются от тех, которые действуют в США. Стандартизация позволяет людям всего мира пользоваться одними и теми же услугами через Интернет[21].

18. Ниже рассматриваются два различных подхода к транснациональным аспектам киберпреступности и расхождения в соответствующих правовых критериях.

### 1. Совместимость законодательства

19. Одним из возможных подходов к борьбе с киберпреступностью в ее транснациональном аспекте и развитию международного сотрудничества являются выработка и стандартизация соответствующего законодательства. В последние годы в разных регионах был применен ряд подходов к решению этой задачи.

20. В 2002 году Содружеством наций был разработан типовой закон о компьютерных и связанных с компьютерами преступлениях, имевший своей целью совершенствование законодательных норм государств – членов Содружества в области борьбы с киберпреступностью и углубление международного сотрудничества. Без этого для развития трансграничного сотрудничества в данной области членам Содружества наций потребовалось бы заключить между собой в общей сложности не менее 1 72 двусторонних договоров[22]. Типовой закон содержит положения по материальным вопросам уголовного права, а также процессуальные нормы и положения о международном сотрудничестве. Поскольку он имеет региональную ориентацию, обеспечиваемая этим законом согласованность распространяется только на государства – члены Содружества.

21. Европейским союзом также предприняты усилия по согласованию законодательства о киберпреступности, действующего в 27 его государствах-членах. Для этого были приняты, в частности, директива № 2000/31/ЕС Европейского парламента и Совета о некоторых правовых аспектах услуг информационного общества, таких как электронная торговля, на внутреннем рынке; рамочное решение Совета Европейского союза 2000/41/JHA о борьбе с мошенничеством и фальсификацией безналичных платежных средств; рамочное решение Совета Европейского союза 2004/68/JHA о борьбе с сексуальной эксплуатацией детей и детской порнографией; рамочное решение Совета

---

[21] О важности введения единых технических, равно как и правовых, стандартов см. Marco Gercke, "National, regional and international approaches in the fight against cybercrime", *Computer Law Review International*, 2008, p. 7.

[22] Richard Bourne, "2002 Commonwealth Law Ministers' Meeting: policy brief". Подготовлено к совещанию министров по вопросам законодательства стран Содружества, состоявшемуся в Кингстауне, Сент-Винсент и Гренадины, 18-21 ноября 2002 года (London, Institute of Commonwealth Studies, 2002), p. 9.

Европейского союза 2005/222/JHA об атаках на информационные системы[23]; директива 2006/24/EC Европейского парламента и Совета Европейского союза о сохранении данных, выработанных или обработанных в связи с предоставлением услуг электронной связи общего пользования или сетей связи общего пользования, и о внесении поправок в директиву 2002/58/EC; а также рамочное решение Совета Европейского союза 2008/919/JHA о внесении поправок в рамочное решение 2002/475/JHA о борьбе с терроризмом. В отличие от большинства других региональных мер, осуществление документов, принимаемых Европейским союзом, является обязательным для всех государств-членов. При всей действенности этих документов главным препятствием гармонизации соответствующих норм в странах ЕС до начала 2010 года была ограниченность его законодательных полномочий в области уголовного права[24]. Многообразие применявшихся подходов объяснялось тем, что органы ЕС могли заниматься согласованием норм национального уголовного законодательства лишь в отдельных областях[25]. Иная ситуация возникла после заключения Лиссабонского договора, изменившего ряд положений Договора о Европейском союзе и Договора об учреждении Европейского сообщества, в результате чего ЕС получил более весомые полномочия в том, что касается согласования в будущем законодательства о компьютерных преступлениях; это, однако, касается лишь 27 государств – членов ЕС.

22. Советом Европы разработаны три основных инструмента, направленные на согласование законодательства о киберпреступности. Самым известным из них является Конвенция о киберпреступности, разработанная в 1997-2001 годах. Она содержит положения по материальным вопросам уголовного права, процессуальные нормы и положения о международном сотрудничестве. По состоянию на декабрь 2009 года эта конвенция была подписана 46 государствами и ратифицирована 26 из них. Поскольку в ходе переговоров по Конвенции не удалось достичь согласия о введении уголовной ответственности за расизм и распространение материалов ксенофобского содержания, в 2003 году был принят Дополнительный протокол к Конвенции о киберпреступности, касающийся уголовной ответственности за действия расистского и ксенофобского характера, совершаемые с помощью компьютерных систем[26]. К декабрю 2009 года Дополнительный протокол подписали 34 государства[27] и ратифицировали 15 из

---

[23] Подробнее см. в: Marco Gercke, "The EU framework decision on attacks against information systems", *Computer und Recht*, 2005, pp. 468 ff.; и *Понимание киберпреступности: руководство для развивающихся стран* (см. сноску 2), стр. 99.

[24] Helmut Satzger, *Internationales und Europäisches Strafrecht* (Baden-Baden, Nomos, 2005), p. 84; и P.J.G. Kapteyn and Pieter Verloren van Themaat, *Introduction to the Law of the European Communities: After the Coming into Force of the Single European Act* (Boston, Kluwer Law International, 1989).

[25] О законодательстве стран Европейского союза по вопросам борьбы с киберпреступностью: Lorenzo Valeri and others, *Handbook of Legal Procedures of Computer Network Misuse in EU Countries* (Santa Monica, California, Rand Corporation, 2006).

[26] Council of Europe, *European Treaty Series*, No. 189. См. также "пояснительный доклад" к Дополнительному протоколу.

[27] Австрия, Албания, Армения, Бельгия, Босния и Герцеговина, бывшая югославская Республика Македония, Германия, Греция, Дания, Исландия, Канада, Кипр, Латвия, Лихтенштейн, Литва, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Республика Молдова, Румыния, Сербия, Словения, Украина, Финляндия, Франция, Хорватия, Черногория, Швейцария, Швеция, Эстония и Южная Африка.

них[28]. В 2007 году была открыта для подписания Конвенция Совета Европы о защите детей от эксплуатации и посягательств сексуального характера[29]. Она содержит конкретные положения об уголовной ответственности за обмен детской порнографией, а также за умышленное получение доступа к детской порнографии с использованием информационных и коммуникационных технологий (пункт 1 (f) статьи 20). К декабрю 2009 года ее подписали 38 государств[30] и ратифицировали три из них[31].

23. Кроме того, по итогам конференции, проведенной в Стэндфордском университете, США, в 1999 году, был разработан проект международной конвенции об усилении защиты от киберпреступности и терроризма; представители Американской ассоциации адвокатов вместе с другими экспертами подготовили проект подборки материалов МСЭ для разработки законодательства о киберпреступности.

## 2. Территориальное разделение

24. В теории техническая стандартизация влечет за собой последствия, выходящие далеко за рамки глобализации технологий и услуг, и может вести также к согласованию национальных законов. Однако, как показывают темпы ратификации Конвенции о киберпреступности и ход переговоров по Дополнительному протоколу к этой конвенции, принципы, заложенные в национальном законодательстве, изменяются намного медленнее, чем технические возможности. Это приводит к появлению другой тенденции, а именно подходов, направленных на территориальное разделение Интернета.

25. Хотя Интернет и не признает национальных границ, существуют способы ограничить доступ его пользователей к определенной информации[32]. Соответственно, идея о том, чтобы обязать провайдеров интернет-услуг блокировать доступ к веб-сайтам, содержащим детскую порнографию, стала привлекать к себе внимание правительств и международных организаций[33].

---

[28] Албания, Армения, Босния и Герцеговина, бывшая югославская Республика Македония, Дания, Кипр, Латвия, Литва, Норвегия, Румыния, Сербия, Словения, Украина, Франция и Хорватия.

[29] Council of Europe, *Treaty Series*, No. 201.

[30] Австрия, Азербайджан, Албания, Бельгия, Болгария, бывшая югославская Республика Македония, Германия, Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кипр, Литва, Лихтенштейн, Люксембург, Монако, Нидерланды, Норвегия, Польша, Португалия, Республика Молдова, Румыния, Сан-Марино, Сербия, Словакия, Словения, Соединенное Королевство, Турция, Украина, Финляндия, Франция, Хорватия, Черногория, Швеция и Эстония.

[31] Албания, Греция и Дания.

[32] Jonathan Zittrain, "A history of online gatekeeping", *Harvard Journal of Law and Technology*, vol. 19, No. 2 (2006), p. 253.

[33] Об обязанностях и возможных подходах в сфере фильтрации Интернета см. Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content", *Computer Law Review International*, 2007, pp. 89 ff.; Ulrich Sieber and Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?* (Berlin, Duncker and Humblot, 2008); W. Ph. Stol and others, *Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland* (The Hague, Boom Juridische Uitgevers, WODC, 2008); Tom Edwards and Gareth Griffith, "Internet censorship and mandatory filtering", *NSW Parliamentary Library Research Service*, E-Brief 5/08, November 2008; Jonathan Zittrain and Benjamin Edelman,

С технической точки зрения организации, предоставляющие доступ в Интернет, в принципе способны проверять, не значатся ли в "черном списке" интересующие пользователей веб-сайты, и если да – блокировать доступ к этим сайтам. Для этого могут использоваться различные технические решения – от манипулирования системой доменных имен до прокси-серверов и комбинированных подходов, сочетающих в себе разные элементы[34]. По данным организации "OpenNet Initiative", подобный контроль доступных пользователям материалов практикуется примерно в двух десятках стран[35]. В их число входят несколько европейских государств, включая Италию, Норвегию, Соединенное Королевство, Швейцарию и Швецию, а также такие страны, как Иран (Исламская Республика), Китай и Таиланд. Вопрос о введении обязательных положений на этот счет обсуждается также в Европейском союзе[36]. Сомнения по поводу данного подхода связаны с тем, что любые возможные на сегодняшний день технические меры можно тем или иным способом обойти, а также что, начав блокировать доступ к информации в Интернете, есть риск зайти слишком далеко[37]. Важность защиты основных прав подчеркивалась в рекомендации Комитета министров Совета Европы о мерах, способствующих соблюдению свободы выражения и свободы информации при применении интернет-фильтров.

## D. Организованная преступность

26. Хотя компьютерные преступления обычно совершаются в одиночку, организованные преступные группы также проявляют активность в этой сфере. Эта тенденция заслуживает особого внимания, так как открывает возможность применения документов, направленных на борьбу с организованной преступностью, – таких, как Конвенция Организации Объединенных Наций против транснациональной организованной преступности[38].

27. Когда речь заходит о киберпреступлениях в контексте организованной преступности, важно проводить различие между двумя основными формами

---

"Documentation of Internet filtering worldwide", October 2003, информация о проекте размещена по адресу http://cyber.law.harvard.edu/filtering.

[34] Обзор технических аспектов см. в Sieber and Nolde, *Sperrverfügungen im Internet*, pp. 50 ff.; Stol and others, *Filteren van kinderporno op internet*, pp. 10 ff.; Andreas Pfitzmann, Stefan Köpsell and Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*, Technical University of Dresden, размещено по адресу www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Richard Clayton, Steven J. Murdoch and Robert N. M. Watson, "Ignoring the Great Firewall of China". Доклад, представленный на 6-м Практикуме по технологиям защиты частной жизни, Кембридж, июнь 2006 года; Lori Brown Ayre, *Internet Filtering Options Analysis: An Interim Report*, подготовлено для InfoPeople Project, май 2001 года.

[35] Miklós Haraszti, "Preface", в книге *Governing the Internet: Freedom and Regulation in the OSCE Region*, C. Möller and A. Amouroux, eds. (Vienna, Organization for Security and Cooperation in Europe, 2007), pp. 5-6.

[36] Commission of the European Communities, "Proposal for a Council framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing framework decision 2004/68/JHA", document COM(2009) 135, Brussels, 25 March 2009.

[37] Подробнее о блокировании доступа в Интернет и о том, как это соотносится с основными свободами, см. Cormac Callanan and others, *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin, Aconite Internet Solutions, October 2009), chaps. 6 and 7.

[38] United Nations, *Treaty Series*, vol. 2225, No. 39574.

причастности организованных преступных группировок: использованием информационных технологий организованными преступными сообществами традиционного типа и деятельностью преступных групп, специализирующихся на совершении киберпреступлений[39].

28. Традиционные криминальные группировки, специально не занимающиеся преступной деятельностью в Интернете, используют информационные технологии для координации своих действий и для облегчения совершения других преступлений[40]. Целью применения ими таких технологий является повышение эффективности действий организованной преступной группы в традиционной для нее сфере. Речь может идти о переходе на электронные средства связи, что, например, позволяет организованным преступным сообществам прибегать к шифрованию сообщений и передавать информацию анонимно. Кроме того, Интернет может использоваться для освоения новых рынков: как выяснила Целевая группа по борьбе с организованной преступностью в Соединенном Королевстве, это уже позволило продавцам контрафактной и пиратской продукции значительно расширить сбыт своего товара[41].

29. Поступающая информация свидетельствует о тенденции традиционных организованных преступных групп осваивать новые виды криминальной деятельности в высокотехнологичных областях[42], включая торговлю "пиратским" программным обеспечением и другие формы нарушения авторских прав[43]. Однако организованная преступность нередко оказывается замешанной и в других видах киберпреступлений, таких как распространение детской порнографии[44] и преступления, связанные с личными данными. Применительно к осуществлению Конвенции против организованной преступности необходимо принимать во внимание следующие особенности организованных группировок, специализирующихся на киберпреступлениях:

---

[39] Kim-Kwang Raymond Choo, "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, No. 3 (September 2008), pp. 270-295. В этой статье Чу различает три категории организованных преступных групп, использующих информационные технологии для уклонения от мер контроля.

[40] Там же, p. 273; Eoghan Casey, *Digital Evidence and Computer Crime: Forenisc Science, Computers, and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 9.

[41] United Kingdom, Organised Crime Task Force, *Annual Report and Threat Assessment 2007: Organised Crime in Northern Ireland* (2007), p. 34. Размещено по адресу www.octf.gov.uk.

[42] United Kingdom, Serious Organised Crime Agency, *The United Kingdom Threat Assessment of Organised Crime: 2009/10*, p. 10. Размещено по адресу www.soca.gov.uk.

[43] Canada, Canadian Security Intelligence Service, "Transnational criminal activity: a global context", *Perpectives*, 17 August 2000, размещено по адресу www.csis-scrs.gc.ca/pblctns/prspctvs/200007-eng.asp; Choo, "Organised crime groups", p. 273 (см. сноску 40).

[44] Choo, "Organised crime groups", p. 281; European Police Office (Europol), "Child abuse in relation to trafficking in human beings", Serious Crime Overview, January 2008, p. 2; *Organised Crime Situation Report 2005*, p. 8; John Carr, *Child Abuse, Child Pornography and the Internet* (London, NCH, The Children's Charity, 2004), p. 17; Canada, Criminal Intelligence Service Canada, *Annual Report on Organized Crime in Canada 2007* (Ottawa, 2007), p. 4; "Annual report on organized crime in Greece for the year 2004", *Trends in Organized Crime*, vol. 9, No. 2 (2005), p. 5; Организация Объединенных Наций, Комиссия по правам человека, доклад Специального докладчика по вопросу о торговле детьми, детской проституции и детской порнографии (E/CN.4/2005/78), стр. 8.

a) группировки киберпреступников обычно имеют более свободную и гибкую структуру, допускающую привлечение некоторых лиц на временной основе[45];

b) группировки киберпреступников часто значительно уступают по размерам традиционным организованным преступным сообществам[46];

c) многие члены таких группировок общаются между собой исключительно в электронной форме, никогда не встречаясь лично.

# III. Противодействие киберпреступности

30. Для борьбы с киберпреступностью международные и региональные организации, правительства, правоохранительные органы и неправительственные организации используют различные средства, включая законодательные инициативы, меры правоохранительного характера и меры по созданию потенциала.

## A. Законодательство

31. Законодательство о киберпреступности в настоящее время разрабатывается в основном на национальном и региональном уровнях. В отличие от технической стандартизации процедур передачи данных, которые сегодня одинаковы повсюду в мире, никаких глобальных усилий по согласованию законодательства о киберпреступности до сих пор не предпринималось.

### 1. Пределы применения существующих документов

32. Эффективность региональных подходов, принятых в рамках Содружества наций, Экономического сообщества государств Западной Африки (ЭКОВАС), Европейского союза и Совета Европы, в глобальном масштабе невелика, так как они распространяются только на государства – члены соответствующих организаций. Наиболее широкой сферой применения на сегодняшний день обладает Конвенция о киберпреступности, признанная в качестве важного инструмента борьбы с этим видом преступлений и получившая поддержку различных международных организаций. Кроме того, к этой конвенции, согласно ее статье 37, может присоединиться любое государство, не являющееся членом Совета. В переговорах по Конвенции участвовали четыре таких государства (Канада, США, Южная Африка и Япония), три из которых (Канада, США и Япония) поддерживают тесные связи с Советом, имея в нем статус наблюдателей. К декабрю 2009 года Конвенцию подписали 46 государств[47]

---

[45] Choo, "Organised crime groups" p. 273 (см. сноску 40).

[46] Susan W. Brenner, "Organized cybercrime? How cybercrime may affect the structure of criminal relationships", North Carolina Journal of Law and Technology, No. 4 (2002), p. 27.

[47] Австрия, Азербайджан, Албания, Армения, Бельгия, Болгария, Босния и Герцеговина, бывшая югославская Республика Македония, Венгрия, Германия, Греция, Грузия, Дания, Канада, Кипр, Исландия, Ирландия, Испания, Италия, Латвия, Литва, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Республика Молдова, Румыния, Сербия, Словакия, Словения, Соединенное Королевство, Соединенные Штаты Америки, Украина,

(включая четыре не входящие в Совет государства, которые принимали участие в переговорах); на сегодняшний день Конвенция ратифицирована 26 государствами и одной страной, не являющейся членом Совета[48].

33. Действенность Конвенции о киберпреступности определяется не только числом государств, подписавших или ратифицировавших ее. Так, Аргентина, Ботсвана, Египет, Нигерия, Пакистан и Филиппины не присоединились к Конвенции официально, но взяли ее за образец при разработке некоторых законодательных актов. Однако по глобальным меркам число присоединившихся к Конвенции государств и темпы ее подписания и ратификации, несомненно, до сих пор оставляют желать лучшего. За девять лет, прошедшие с тех пор, как 23 ноября 2001 года Конвенцию подписали первые 30 стран, свои подписи под ней поставили лишь еще 16. После 2001 года к Конвенции не присоединилось ни одно государство, не являющееся членом Совета Европы, хотя пяти таким государствам (Доминиканской Республике, Коста-Рике, Мексике, Филиппинам и Чили) было предложено это сделать. Столь же медленно продвигается и процесс ратификации: в 2002 году Конвенцию ратифицировали два государства (Албания и Хорватия), в 2003 – еще два (Венгрия и Эстония), в 2004 – четыре (бывшая югославская Республика Македония, Литва, Румыния и Словения), в 2005 – три (Болгария, Дания и Кипр), в 2006 – семь (Армения, Босния и Герцеговина, Нидерланды, Норвегия, США, Украина и Франция), в 2007 – три (Исландия, Латвия и Финляндия), в 2008 – два (Италия и Словакия) и в 2009 – три (Германия, Республика Молдова и Сербия). Поскольку Конвенцию в большинстве случаев требуется не только ратифицировать, но и воплощать на практике, ее эффективность зависит от того, будет ли законодательство ратифицировавших Конвенцию государств полностью адаптировано к ее положениям. Необходимы также доказательства такой полной адаптации.

## 2. Глобальная дискуссия

34. Еще одним аспектом, характеризующим потенциальный вклад региональных договоренностей в глобальный процесс согласования действующих норм, является возможность участия в них государств, не входящих в региональные объединения. Несмотря на транснациональные масштабы киберпреступности, ее последствия по-разному ощущаются в разных регионах мира. Это особенно относится к развивающимся странам[49]. Упомянутые в пункте 32 региональные подходы не рассчитаны на широкое вовлечение государств, не являющихся членами соответствующих группировок. Даже Конвенция о киберпреступности, обладающая на сегодняшний день самым широким членским составом, ограничивает возможность участия в ней таких стран. В статье 37 этой конвенции указано, что государство, желающее к ней

---

Финляндия, Франция, Хорватия, Черногория, Чешская Республика, Швейцария, Швеция, Эстония, Южная Африка и Япония.

[48] Албания, Армения, Босния и Герцеговина, Болгария, бывшая югославская Республика Македония, Венгрия, Германия, Дания, Исландия, Италия, Кипр, Латвия, Литва, Нидерланды, Норвегия, Республика Молдова, Румыния, Сербия, Словакия, Словения, Соединенные Штаты Америки, Украина, Финляндия, Франция, Хорватия и Эстония.

[49] См., например, доклад Организации экономического сотрудничества и развития "*Spam Issues in Developing Countries"* (Paris, OECD, 2005), p. 4. Размещено по адресу http://www.oecd.org/dataoecd/5/47/34935342.pdf); а также *Понимание киберпреступности: руководство для развивающихся стран*, стр. 15 (см. сноску 2).

присоединиться, должно проконсультироваться со всеми государствами – участниками Конвенции и получить на это их единодушное согласие. Кроме того, правом участвовать в дискуссиях о возможных в будущем поправках к Конвенции обладают только ее стороны (ст. 44).

35. Опыт показывает, что государства, как правило, не склонны ратифицировать или присоединяться к конвенциям, в разработке и согласовании которых они не участвовали. Это относится к любым конвенциям, независимо от их содержания.

36. На всех четырех региональных подготовительных совещаниях к двенадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию звучали призывы к разработке международной конвенции о киберпреступности.

37. К этому же призывали участники совещаний руководителей национальных правоохранительных органов стран Африки, Ближнего и Среднего Востока и Европы, в ходе которых обсуждались проблемы Интернета, электронного сбора следственной информации, разработки законодательства и т.д. Делегаты совещаний, проводившихся в других регионах, приходили к выводу о том, что правоохранительные и судебные органы не обладают необходимой подготовкой и достаточным потенциалом для реагирования на новые явления в сфере киберпреступности, а также для сбора доказательств с помощью компьютерных технологий и их использования в целях подготовки к судебным процессам. Высказывалось единодушное мнение, что национальное законодательство отстало от жизни и нуждается в поправках, позволяющих вести расследования, привлекать преступников к ответственности и выносить им обвинительные приговоры на основании доказательств, полученных при помощи кибертехнологий. Налицо острая потребность в установлении единых правил и развитии сотрудничества на межгосударственном уровне, с тем чтобы органы власти могли принимать эффективные меры по привлечению преступников к суду в разных юрисдикциях. С призывами к разработке международного документа выступают также представители научных кругов[50].

### 3. Меры, необходимые в свете современных тенденций

38. Киберпреступность принимает все новые формы. В период разработки региональных документов, подобных типовому закону Содружества о компьютерных и связанных с компьютерами преступлениях и Конвенции о киберпреступности, о таких явлениях, как массированные атаки бот-сетей, фишинг и использование Интернета террористами, не было известно вовсе либо им не придавалось того значения, которое они имеют сегодня. Поэтому каких-либо специальных положений на этот счет не существует. В ходе региональных совещаний по подготовке к двенадцатому Конгрессу говорилось о необходимости учитывать эти новые явления, и особенно использование Интернета в террористических целях: от пропаганды, поддержания связи и финансирования терактов посредством сетевых платежей до сбора информации

[50] Joachim Vogel, "Towards a global convention against cybercrime". Доклад, представленный на Первой всемирной конференции по уголовному праву, Гвадалахара, Мексика, 19-23 ноября 2007 года; Stein Schjølberg and Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Oslo, E-dit, 2009).

о потенциальных целях. Эти явления, а также возможные правовые меры противодействия им неоднократно рассматривались Целевой группой по осуществлению контртеррористических мероприятий[51].

39. Если вопрос об охвате таких явлений материально-правовыми нормами уголовного законодательства часто удается решить путем применения положений о несанкционированном вмешательстве в работу систем или компьютерном подлоге, то применять процедурные механизмы, предусмотренные существующими региональными документами, намного труднее, особенно в условиях, когда интернет-технологии и характер предлагаемых сетевых услуг (например, социальных сетей) существенно изменились. Прослушивание разговоров, ведущихся с помощью голосовой связи через Интернет, приемлемость цифровых данных в качестве доказательств в суде, процедуры расследования дел, в которых применялись технологии шифрования или средства анонимной связи, – все это неотложные проблемы, для решения которых, однако, ничего не делается на региональном уровне и лишь в некоторых случаях предпринимаются усилия на уровне отдельных стран[52].

40. Заниматься этими вопросами весьма важно, поскольку традиционные следственные методы нередко оказываются бесполезными для раскрытия киберпреступлений. Примером может служить прослушивание телефонных разговоров. В последние десятилетия в распоряжении государств появились средства – такие, как электронная подслушивающая аппаратура, – которые позволяют следственным органам прослушивать разговоры, ведущиеся по мобильным и стационарным телефонам. Такой перехват обычных телефонных звонков, как правило, осуществляется через операторов телекоммуникационных сетей. Для того чтобы распространить эту практику на голосовые переговоры по Интернету, правоохранительным ведомствам необходимо установить контакты с провайдерами услуг голосовой интернет-связи. Однако последние могут сами быть практически не в состоянии обеспечить прослушивание подобных переговоров, если их услуги основаны на технологиях однорангового обмена[53], при которых передача данных осуществляется напрямую от одного собеседника другому[54]. Поэтому в дополнение к соответствующим правовым документам могут потребоваться и новые методы.

---

[51] См., например, Counter-Terrorism Implementation Task Force, "Report of the Working Group on Countering the Use of Internet for Terrorist Purposes", February 2009. Размещено по адресу www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf.

[52] Обзор различных национальных подходов к этим проблемам см. в публикации "*Понимание киберпреступности: руководство для развивающихся стран*", глава 6 (см. сноску 2).

[53] Технологии однорангового обмена позволяют абонентам сетей устанавливать прямую связь друг с другом вместо того, чтобы в обязательном порядке общаться по традиционной схеме через центральные сетевые серверы.

[54] О прослушивании правоохранительными органами голосовых переговоров, ведущихся по Интернету, см. Steven Bellovin and others, "Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP", 13 June 2006, размещено по адресу www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf; Matthew Simon and Jill Slay, "Voice over IP: forensic computing implications". Доклад, представленный на 4-й Австралийской конференции по компьютерной криминалистике, Перт, Австралия, декабрь 2006 года.

41. Возможность применения сложных современных методов расследования важна для раскрытия не только новых, но и более традиционных видов киберпреступлений, например связанных с детской порнографией. С середины 1990-х годов распространители и потребители детской порнографии получили доступ к сетевым услугам, которые используются ими все более активно[55]. Интернет стал основным каналом обмена детской порнографией. Проблемы, связанные с обнаружением детской порнографии и проведением соответствующих расследований, привлекли к себе внимание еще в 1990-е годы; они до сих пор не решены во многом из-за того, что преступникам удается применять изощренные технологии, затрудняющие работу следственных органов. Так, по данным одного из исследований, 6 процентов лиц, у которых была обнаружена детская порнография, пользовались шифрованием, 17 процентов использовали программы, защищенные паролями, 3 процента – программы, способные автоматически уничтожать компрометирующую информацию, и 2 процента – системы удаленного хранения файлов[56]. Кроме того, наблюдается смена технологий: если на ранних этапах развития Интернета обмен детской порнографией осуществлялся в основном с помощью обычных чатов с передачей сообщений через центральный сервер, то в последнее время для этого стали использоваться другие средства, такие как одноранговые сети[57].

## B. Потребности правоохранительных органов

42. Помимо надлежащей нормативной базы успешная работа правоохранительных органов в значительной степени зависит от наличия в руках следствия таких инструментов, как специальное программное обеспечение для криминалистических нужд (сбор доказательств, запись информации, вводимой с клавиатуры компьютера, расшифровка данных и восстановление уничтоженных файлов), а также для розыска по базам данных (например, с помощью хеш-функций файлов с известными кадрами детской порнографии). Несколько подобных инструментов созданы за последние годы и продолжают совершенствоваться[58]. Так, в Университетском колледже Дублина осуществляется исследовательский проект, получивший название "Автоматическая реконструкция событий для целей компьютерной

---

[55] United States, House of Representatives, "Sexual exploitation of children over the Internet" (2007), 109th Congress, p. 9.

[56] Janis Wolak, David Finkelhor and Kimberly J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study* (Alexandria, Virginia, National Center for Missing and Exploited Children, 2005), p. 9.

[57] United States, General Accountability Office, *File-Sharing Programs, Child Pornography is Readily Accessible over Peer-to-Peer Networks*, testimony before the Committee on Government Reform, House of representatives, GAO Report GAO-03-537T (Washington, D.C., March 2003); Gretchen Ruethling, "27 charged in international online child pornography ring", *New York Times*, 16 March 2006; Choo, "Organised crime groups", p. 282 (см. сноску 40); United Kingdom, Stockport Safeguarding Children Board, *Safeguarding Children in Stockport: Policy and Practice Handbook* (May 2008), p. 299, размещено по адресу http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf.

[58] См., например, исследовательский проект на тему "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis", осуществляемый в Университетском колледже Дублина (информация размещена по адресу htt://cci.ucd.ie/?q=node/33).

криминалистики и разбора случаев взлома систем" (информацию о проекте см. по адресу http://cci.ucd.ie/?q=node/33), а в США с декабря 2009 года внедряется новая технология отслеживания происхождения детской порнографии под названием PhotoDNA. Одной из главных проблем, связанных с созданием таких инструментов, остается координация усилий их разработчиков во избежание дублирования. В координации нуждается также деятельность сетей, объединяющих соответствующие контактные пункты (в частности, стран Большой восьмерки и Интерпола, а также сети, созданной в рамках Конвенции о киберпреступности).

## C. Создание потенциала

43. Проблема киберпреступности актуальна не только для развитых, но и для развивающихся стран. Согласно данным фонда "Девелопмент гейтуэй", в 2005 году развивающиеся страны опережали промышленно развитые государства по количеству пользователей Интернета[59]. В качестве позитивных признаков можно отметить недавнее принятие директивы о киберпреступности странами ЭКОВАС и проект основных положений законодательства о кибертехнологиях, представленный в рамках Восточноафриканского сообщества. Дальнейшая поддержка в этой сфере облегчила бы правоохранительным органам подготовку к борьбе с правонарушениями, которых можно ожидать, когда высокоскоростной доступ в Интернет станет более широко распространенным в развивающихся странах. В своей резолюции 64/179, озаглавленной "Укрепление программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в особенности ее потенциала в сфере технического сотрудничества", Генеральная Ассамблея обратила внимание на новые политические вопросы, отмеченные в докладе Генерального секретаря (A/64/123) – пиратство, киберпреступность, сексуальная эксплуатация детей и преступность в городах, и предложила ЮНОДК исследовать в рамках своего мандата пути и средства решения этих проблем.

## D. Подготовка кадров

44. Поскольку при расследовании киберпреступлений и судебном преследовании тех, кто их совершает, возникают совершенно особые проблемы, важно обеспечивать соответствующую подготовку сотрудников правоохранительных органов, прокуроров и судей. Как подчеркивалось на совещании группы экспертов ЮНОДК по киберпреступности, проходившем в Вене 6 и 7 октября 2009 года, большинство занимающихся этим международных и региональных организаций предпринимают шаги по профессиональной подготовке экспертов, участвующих в расследовании киберпреступлений, и по разработке необходимых учебных пособий[60].

---

[59] Информация размещена по адресу http://topics.developmentgateway.org/special/informationsociety.

[60] Например, Азиатско-тихоокеанская ассоциация экономического сотрудничества организовала несколько учебных мероприятий на темы борьбы с киберпреступностью,

# IV. Выводы и рекомендации

45. Расследование киберпреступлений и привлечение киберпреступников к ответственности – нелегкое дело для всех вовлеченных в эту работу учреждений. Ввиду сложного характера данной проблемы и непрекращающегося технического прогресса ключевой задачей остается непрерывная и все более широкая профессиональная подготовка сотрудников всех соответствующих органов. Как показала дискуссия в ходе состоявшегося в 2009 году совещания группы экспертов ЮНОДК по киберпреступности, организационно оформленная деятельность по созданию потенциала и надежное закрепление достигнутого – два важнейших критерия успеха будущих инициатив.

46. Для того чтобы преступникам стало негде укрываться, а также в целях дальнейшего развития международного сотрудничества, следует уделять внимание восполнению пробелов в действующем законодательстве и обеспечению непротиворечивости, последовательности и совместимости законодательных положений. Принимая во внимание важность гармонизации законодательства и необходимость учета результатов региональных подготовительных совещаний к двенадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, следует тщательно и в позитивном плане рассмотреть вопрос о разработке глобальной конвенции против киберпреступности.

47. Тем временем ЮНОДК как организация, определяющая стандарты в области предупреждения преступности и уголовного правосудия, будет служить площадкой для многосторонних контактов, центральное место в которых должно принадлежать развивающимся странам. ЮНОДК будет и впредь придерживаться всеобъемлющего, опирающегося на партнерство междисциплинарного подхода, объединяя свой доказанный на деле экспертный потенциал в том, что касается юридических, правоохранительных и технических аспектов противодействия преступности, с конкретными, весьма глубокими знаниями и навыками ключевых партнеров, уже ведущих борьбу с киберпреступлениями. ЮНОДК будет стремиться налаживать партнерские связи, мобилизуя имеющийся инструментарий и специалистов, в том числе со стороны частного сектора (и особенно провайдеров интернет-услуг), в целях решения проблемы в той или иной стране или регионе. Первоочередное внимание будет уделяться оказанию технической помощи нуждающимся в ней государствам-членам, с тем чтобы преодолеть дефицит возможностей и экспертной подготовки и придать борьбе с компьютерной преступностью стабильный и долговременный характер.

---

включая законодательство о киберпреступлениях; учебные занятия по правовой и технической тематике организовывались по линии Содружества наций; Совет Европы участвовал в проведении мероприятий по подготовке кадров в разных районах мира и подготовил специальные учебные материалы для судей; Европейский союз поддерживает работу по организации занятий и подготовке учебных пособий по киберпреступности для сотрудников правоохранительных органов своих государств-членов и провел несколько учебных мероприятий в Европе и за ее пределами; Интерполом был организован ряд учебных мероприятий для личного состава правоохранительных органов и подготовлены учебные пособия; МСЭ разработал учебные материалы по киберпреступности на всех языках Организации Объединенных Наций, обеспечил подготовку по общей тематике для участников нескольких региональных мероприятий, а также организовал специализированную подготовку для судей.

48. В конкретном плане ЮНОДК будет ставить перед собой следующие задачи: помогать государствам-членам в принятии законодательства, позволяющего эффективно расследовать компьютерные преступления и привлекать к ответственности преступников; расширять прикладные и технические знания судей, прокуроров и сотрудников правоохранительных органов по вопросам, связанным с киберпреступностью, путем их профессиональной подготовки, адаптации/разработки учебных пособий на темы расследования компьютерных преступлений и судебного преследования за них, и т.д.; обучать должностных лиц правоохранительных органов эффективному использованию механизмов международного сотрудничества в целях противодействия киберпреступности; повышать осведомленность гражданского общества и побуждать руководителей к объединению усилий по профилактике и пресечению киберпреступности; а также выявлять и распространять позитивный опыт и развивать государственно-частные партнерские инициативы в целях предупреждения киберпреступности и борьбы с ней.