Организация Объединенных Наций E/CN.15/2011/19

Экономический и Социальный Совет

Distr.: General
2 March 2011
Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Двадцатая сессия
Вена, 11-15 апреля 2011 года
Пункт 6 предварительной повестки дня*
Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения

Доклад межправительственной группы экспертов открытого состава о всестороннем исследовании проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора

Записка Секретариата

1. В соответствии с пунктом 9 резолюции 65/230 Генеральной Ассамблеи межправительственная группа экспертов открытого состава, учрежденная Комиссией согласно пункту 42 Салвадорской декларации о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развития в изменяющемся мире (резолюция 65/230 Генеральной Ассамблеи, приложение), провела свое совещание в Вене с 17 по 21 января 2011 года. В соответствии со своим мандатом группа экспертов обсудила вопрос о

> всестороннем исследовании проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых и других мер по противодействию киберпреступности.

* E/CN.15/2011/1.

V.11-80328 (R)

2. В пункте 11 своей резолюции 65/230 Генеральная Ассамблея просила межправительственную группу экспертов открытого состава представить Комиссии доклад о ходе ее работы. Соответственно, группа экспертов рассмотрела и приняла приложенные к настоящему докладу итоговые документы под названиями "Подборка тем для рассмотрения в рамках всестороннего исследования последствий киберпреступности и ответных мер по борьбе с ней" (приложение I) и "Методология исследования" (приложение II), которые препровождаются Комиссии для рассмотрения на ее двадцатой сессии.

3. После утверждения "Подборки тем для рассмотрения в рамках всестороннего исследования последствий киберпреступности и ответных мер по борьбе с ней" (приложение I) представитель Колумбии выступил с нижеизложенным заявлением и просил включить его в доклад межправительственной группы экспертов открытого состава:

"1. В ходе совещания межправительственной группы экспертов открытого состава многие делегации выразили обеспокоенность тем фактом, что новые информационно-коммуникационные технологии часто противоправно используются в террористических целях. В этом контексте представитель Секретариата рассказал о работе Управления Организации Объединенных Наций по наркотикам и преступности в связи с этой проблемой и, в частности, в связи с неправомерным использованием Интернета. С учетом того, что исследование проблемы киберпреступности должно носить всесторонний и комплексный характер, в его рамках потребуется рассмотреть все вызвавшие обеспокоенность моменты. Поэтому чрезвычайно важно, чтобы все аспекты взаимосвязей между терроризмом и киберпреступностью были охвачены в исследовании. Террористические организации используют эти технологии самыми различными способами, например:

a) в пропагандистских целях;

b) для сбора информации;

c) в качестве инструмента обучения;

d) для организации незаконной деятельности;

e) для распространения информации в целях вербовки и подстрекательства;

f) для целей обеспечения хранения и передачи информации;

g) для самостоятельных атак на компьютерные системы.

2. В интересах консенсуса Колумбия выражает согласие с предложениями делегации Аргентины по этому предмету, однако просит отметить в докладе межправительственной группы экспертов открытого состава о работе ее первого совещания следующее:

a) применительно к пункту 12 подборки тем для рассмотрения в рамках всестороннего исследования последствий киберпреступности и ответных мер по борьбе с ней (см. приложение I) ссылка на перечень

деяний, признанных уголовно наказуемыми, включает, согласно пониманию Колумбии, состав терроризма;

b) применительно к названию, предшествующему пункту 18 этого документа, вызовы, создаваемые киберпреступностью, также включают, согласно пониманию Колумбии, состав терроризма;

c) Колумбия также выражает надежду, что в исследовании будет охвачено рассмотрение возможного противоправного использования террористами тех инструментов, которые могут использоваться для совершения киберпреступлений, как об этом упомянуто в пункте 25 этого документа".

Приложение I

Подборка тем для рассмотрения в рамках всестороннего исследования последствий киберпреступности и ответных мер по борьбе с ней

1. Введение

1. В ходе двенадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, состоявшегося в 2010 году, государства-члены более или менее подробно обсудили проблему киберпреступности и предложили Комиссии по предупреждению преступности и уголовному правосудию созвать совещание межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер по борьбе с ней. Эта рекомендация была принята Комиссией по предупреждению преступности и уголовному правосудию, а затем Экономическим и Социальным Советом в его резолюции 2010/18 и Генеральной Ассамблеей в ее резолюции 65/230.

2. В соответствии с пунктом 42 Салвадорской декларации о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире в рамках всестороннего исследования должны быть рассмотрены:

> проблема киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или других мер по противодействию киберпреступности.

3. Таким образом, в пункте 42 Салвадорской декларации определены различные существенные аспекты, которые должны быть рассмотрены в рамках этого исследования (проблема киберпреступности, национальное законодательство, наилучшие виды практики, техническая помощь и международное сотрудничество), а также его подход (ответные меры со стороны государств-членов, международного сообщества и частного сектора) и основная цель (изучение возможных путей укрепления существующих и выработки предложений в отношении новых ответных мер).

4. В целях выработки структуры исследования эти три аспекта (вопросы существа, подход и основная цель) были представлены как 12 тем в соответствии с поставленной в Декларации задачей. Эти 12 тем сгруппированы ниже по категориям.

Проблема киберпреступности (темы 1-3)

5. В Салвадорской декларации отмечено, что в рамках исследования следует подробно изучить проблему киберпреступности. В целях всеобъемлющего изучения связанных с киберпреступностью проблем были определены три основные области, которые следует подробно проанализировать:

a) феномен киберпреступности (тема 1);

b) статистическая информация (тема 2);

c) вызовы, создаваемые киберпреступностью (тема 3).

Правовые меры по противодействию киберпреступности (темы 4-9)

6. В Салвадорской декларации содержится призыв к исследованию правовых мер по противодействию киберпреступности, включая обмен информацией о национальном законодательстве, наилучших видах практики и международном сотрудничестве. В дополнение к общим аспектам согласования законодательства определены конкретные области принятия правовых ответных мер:

a) общие подходы к законодательству (тема 4);

b) криминализация (тема 5);

c) процессуальные полномочия (тема 6);

d) международное сотрудничество (тема 7);

e) гарантии и условия, включая защиту основополагающих прав человека и личных данных;

f) уважение принципа суверенного равенства государств и невмешательства в дела других государств;

g) электронные доказательства (тема 8);

h) роли и ответственность поставщиков услуг и частного сектора (тема 9).

Потенциал в области предупреждения преступности и уголовного правосудия и другие меры по противодействию киберпреступности (тема 10)

7. В Салвадорской декларации говорится об исследовании не только правовых мер по противодействию киберпреступности, но и, более широко, о других мерах противодействия.

Международные организации (тема 11)

8. В Салвадорской декларации содержится призыв к проведению анализа ответных мер со стороны государств-членов, международного сообщества и частного сектора. Вопросы, касающиеся принимаемых международным сообществом правовых ответных мер, рассмотрены в рамках раздела, посвященного правовым мерам по противодействию киберпреступности, тогда как включение отдельного раздела, касающегося ответных мер со стороны

международного сообщества, позволит проанализировать аспекты более общего характера, в частности взаимосвязи между региональным и международным подходами.

Техническая помощь (тема 12)

9. С учетом воздействия киберпреступности на развивающиеся страны и необходимости единообразного и скоординированного подхода к борьбе с киберпреступностью техническая помощь должна рассматриваться в рамках всестороннего исследования как отдельная тема.

II. Подробный обзор тем

Тема 1. Феномен киберпреступности

Общая информация

10. Компьютерная преступность и, более конкретно, киберпреступность – термины, используемые для обозначения конкретной категории преступных деяний. Связанные с этой категорией преступных деяний вызовы включают не только широкий круг уже подпадающих под эту категорию правонарушений, но и быстро формирующиеся новые методы совершения преступлений.

Возникновение и развитие компьютерной преступности и киберпреступности

11. В 60-х годах прошлого века, когда появились первые транзисторные вычислительные системы и популярность компьютеров начала расти[1], уголовно наказуемым признавалось, главным образом, физическое повреждение компьютерных систем и хранящихся на них данных[2]. В 70-х годах произошел переход от традиционных имущественных преступлений против компьютерных систем[3] к новым формам преступности[4], в частности противоправному использованию компьютерных систем[5] и манипуляциям[6] с электронными данными[7]. Переход от личного заключения сделок к заключению сделок при помощи компьютеров способствовал

---

[1] О связанных с этим проблемах см. R. T. Slivka and J. W. Darrow, "Methods and problems in computer security", *Rutgers Journal of Computers and the Law*, vol. 5, No. 2 (1976), pp. 217-269.

[2] McLaughlin, "Computer crime: the Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, vol. 2, 1978, pp. 217 ff.

[3] Gemignani, "Computer crime: the law in ‘80", *Indiana Law Review*, vol. 13, 1980, p. 681.

[4] McLaughlin, "Computer crime: the Ribicoff Amendment".

[5] Freed, *Materials and Cases on Computer and Law* (n.p., 1971), p. 65.

[6] Bequai, "The electronic criminals: how and why computer crime pays", *Barrister*, vol. 4, 1977, pp. 8 ff.

[7] *Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976)*, vol. XV, Collected Studies in Criminological Research (Strasbourg, Council of Europe, 1977), pp. 225 ff.; United States of America, *Staff Study of Computer Security in Federal Programs: Committee on Government Operations – United States Senate* (Washington, D.C., United States Government Printing Office, 1977).

возникновению еще одной новой формы преступности – компьютерного мошенничества[8]. В 80-х годах популярность персональных компьютеров продолжала расти и впервые в истории управление многими важнейшими объектами инфраструктуры стало осуществляться при помощи компьютерных технологий[9]. Одним из побочных эффектов распространения компьютерных систем стало повышение интереса к программному обеспечению, что привело к появлению первых форм торговли "пиратскими" программными продуктами и преступлений, связанных с патентами[10]. Кроме того, появление компьютерных сетей позволило преступникам получать доступ к тем или иным компьютерным системам, не присутствуя при этом на месте преступления[11]. Появление в 90-е годы графического интерфейса (Всемирная сеть World Wide Web) и последовавший за этим стремительный рост числа пользователей Интернета привели к возникновению новых методов совершения преступных деяний. Так, например, если детские порнографические материалы распространялись путем физического обмена печатной продукцией и видеозаписями, то теперь такие материалы распространяются через веб-сайты и Интернет-службы[12]. Компьютерные преступления, как правило, совершались на местном уровне, однако с появлением Интернета электронная преступность приобрела транснациональный характер. В первом десятилетии XXI века на передний план вышли новые, более изощренные методы совершения преступлений, такие как "фишинг"[13], атаки с использованием "бот-сетей"[14], а

---

[8] McLaughlin, "Computer crime: the Ribicoff Amendment" (см. сноску 2 выше); Bequai, "Computer crime: a growing and serious problem", *Police Law Quarterly*, vol. 6, 1977, p. 22.

[9] E. A. Glynn, "Computer abuse: the emerging crime and the need for legislation", *Fordham Urban Law Journal*, vol. 12, No. 1 (1983-1984), p. 73.

[10] BloomBecker, "The trial of computer crime", *Jurimetrics Journal*, vol. 21, 1981, p. 428; W. Schmidt, "Legal proprietary interests in computer programs: the American experience", *Jurimetrics Journal*, vol. 21, 1981, pp. 345 ff.; M. Dunning, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, No. 3 (1982), pp. 273 ff.; Weiss, "Pirates and prizes: the difficulties of protecting computer software", *Western State University Law Review*, vol. 11, 1983, pp. 1 ff.; R. P. Bigelow, "The challenge of computer law", *Western England Law Review*, vol. 7, No. 3 (1985), p. 401; G. Thackeray, "Computer-related crimes: an outline", *Jurimetrics Journal*, vol. 25, No. 3 (1985), pp. 300 ff.

[11] Yee, "Juvenile computer crime: hacking – criminal and civil liability", *Comm/Ent Law Journal*, vol. 7, 1984, pp. 336 ff.; "Who is calling your computer next? Hacker!", *Criminal Justice Journal*, vol. 8, 1985, pp. 89 ff.; A. M. Wagner, "The challenge of computer-crime legislation: how should New York respond?", *Buffalo Law Review*, vol. 33, No. 3 (1984), pp. 777 ff.

[12] "Child pornography", theme paper prepared for the Second World Congress against Commercial Sexual Exploitation of Children, Yokohama, Japan, 12-20 December 2001, p. 17; "Sexual exploitation of children over the Internet", report prepared for the use of the Committee on Energy and Commerce, United States, House of Representatives, 109th Congress, January 2007, p. 9.

[13] Под термином "фишинг" ("phishing") понимается действие, имеющее целью побудить жертву к раскрытию личной или секретной информации. Этот термин (созвучный английскому слову "fishing" ("рыбная ловля" – прим. пер.) изначально относился к рассылке по электронной почте сообщений, предназначенных для "выуживания" паролей и финансовых данных из "моря" пользователей Интернета. Замена буквы "f" буквами "ph" в написании этого термина соответствует особой орфографии, популярной среди хакеров. Более подробно об этом см. Международный союз электросвязи, "Понимание киберпреступности – Руководство для развивающихся стран" (Женева, 2009 год), раздел 2.8.4.

[14] "Бот-сеть" – краткий термин, обозначающий группу компьютеров, зараженных программой, которая позволяет посторонним лицам управлять ими удаленно. Более

также новые методы использования технологий, в частности, речевая связь по Интернету (IP-телефония) (VoIP)[15] и "облачные вычисления" ("cloud computing")[16], которые затрудняют деятельность правоохранительных органов.

Сфера охвата исследования

12. При рассмотрении данной темы в рамках исследования основное внимание будет сосредоточено на самом явлении киберпреступности (меры противодействия этому феномену рассматриваться не будут):

a) анализ феномена киберпреступности с учетом деяний, охватываемых существующими правовыми рамочными документами;

b) перечень деяний, признанных уголовно наказуемыми;

c) перечень деяний, которые пока не признаются уголовно наказуемыми;

d) обзор многосоставных преступлений (таких, как "фишинг") и прогнозирование тенденций;

e) перечень соответствующих дел;

f) изучение важности определения киберпреступности.

Тема 2. Статистическая информация

Общая информация

13. Статистика преступлений является основой для обсуждений и принятия решений политическими деятелями и представителями научных кругов[17]. Кроме того, доступ к точной информации об истинных масштабах киберпреступности позволит правоохранительным органам совершенствовать стратегии борьбы с киберпреступностью, предотвращать возможные атаки и обеспечивать принятие и осуществление более целенаправленного и эффективного законодательства.

подробно об этом см. Clay Wilson, "Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress", Congressional Research Service Report RL32114, 2007, p. 4.

[15] M. Simon and J. Slay, "Voice over IP: forensic computing implications", paper prepared for the fourth Australian Digital Forensics Conference, Perth, 4 December 2006.

[16] Cristos Velasco San Martin, "Jurisdictional aspects of cloud computing", paper presented at the Council of Europe Octopus Interface Conference: Cooperation against Cybercrime, Strasbourg, 10-11 March 2009; M. Gercke, "Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden", in *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger and A. Wiebe, eds., Oldenburger Tagungsbände (Edewecht, Germany, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), pp. 499 ff.

[17] P. A. Collier and B. J. Spaul, "Problems in policing computer crime", *Policing and Society*, vol. 2, No. 4 (1992), p. 308.

Нынешнее положение дел в области сбора статистических данных о киберпреступности

14. Информацию о масштабах преступности, как правило, получают на основе анализа данных статистики преступлений и обследований[18]. Однако использование обоих видов источников при разработке программных рекомендаций сопряжено с некоторыми сложностями. Прежде всего, сбор статистических данных о преступности, как правило, осуществляется на национальном уровне, и такие данные не отражают международные масштабы этой проблемы. Теоретически можно было бы объединить данные различных государств, однако из-за различий в законодательстве и процедурах регистрации преступлений такой подход не позволил бы получить достоверную информацию[19]. Для того чтобы объединить и сравнить национальные статистические данные, они должны быть в определенной мере сопоставимыми[20], а в случае киберпреступности такие данные пока несопоставимы. Даже если киберпреступления регистрируются, то их не всегда выделяют в отдельную категорию[21].

15. Во-вторых, статистические данные могут содержать информацию только о тех преступлениях, которые были выявлены и зарегистрированы[22]. В частности, в отношении киберпреступности высказываются опасения, что далеко не все такие преступления зарегистрированы[23]. Предприятия, возможно, опасаются, что распространение негативных сведений о совершенных против них киберпреступлениях может нанести ущерб их

---

[18] О растущей важности статистических данных о преступности см. D. A. Osborne and S. C. Wernicke, *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, New York, Haworth Press, 2003), pp. 1 ff.

[19] В этом контексте см. *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report No. 5, interim report (London, United Kingdom Statistics Authority, December 2009), p. 9. Размещено по адресу www.statisticsauthority.gov.uk.

[20] A. Alvazzi del Frate, "Crime and criminal justice statistics challenges", in *International Statistics on Crime and Justice*, S. Harrendorf, M. Heiskanen and S. Malby, eds., HEUNI Publication Series, No. 64 (Helsinki, European Institute for Crime Prevention and Control, affiliated with the United Nations, 2010), p. 168. Размещено по адресу www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[21] "Computer crime", Parliamentary Office of Science and Technology, *Postnote*, No. 271, October 2006, p. 3.

[22] О связанных с этим трудностях см. M. E. Kabay, "Understanding studies and surveys of computer crime", June 2009. Размещено по адресу www.mekabay.com/methodology/crime_stats_methods.pdf.

[23] "Федеральное бюро расследований Соединенных Штатов просило компании не замалчивать случаи "фишинговых" атак или атак на информационные системы компаний, а сообщать о них властям, с тем чтобы они были более информированы о преступной деятельности в Интернете. Наша проблема заключается в том, что некоторые компании со всей очевидностью гораздо более обеспокоены утратой репутации, чем последствиями успешной хакерской атаки", – пояснил исполняющий обязанности руководителя Нью-йоркского отделения ФБР Марк Мершин. См."FBI wants to know more about hacker attacks", *Heise News*, 27 October 2006. Размещено по адресу www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html. См. также "Comments on computer crime: Senate Bill S. 240", *Memphis State University Law Review*, 1980, p. 660.

репутации[24]. Если компания объявит, что ее сервер был взломан хакерами, то клиенты могут утратить к ней доверие, и в результате совокупные издержки по своей тяжести могут даже превзойти потери, вызванные самой хакерской атакой. С другой стороны, если не сообщать о правонарушениях и не привлекать преступников к ответственности, они могут пойти на новые преступления. Потерпевшие не всегда верят в способность правоохранительных органов найти виновных[25] и, возможно, не видят смысла в сообщении о таких правонарушениях[26]. Поскольку автоматизация кибератак позволяет киберпреступникам разрабатывать стратегии получения крупной прибыли в результате многочисленных атак, направленных на получение небольшого количества денежных средств (что происходит в случае мошеннических действий с предоплатой)[27], непредставление информации о таких преступлениях может привести к серьезным последствиям. В случаях, когда потерпевшие лишаются лишь небольшого количества денег, они, возможно, предпочтут не проходить длительных процедур регистрации таких преступлений в правоохранительных органах. На практике о таких преступлениях сообщают в основном тогда, когда речь идет о наиболее крупных финансовых потерях[28].

Сфера охвата исследования

16. Изучение данной темы будет предусматривать следующее:

a) сбор самых последних данных статистики, обследований и анализов, касающихся распространения и масштабов киберпреступности;

b) анализ ценности статистических данных для разработки программных рекомендаций;

---

[24] См. N. Mitchison and R. Urry, "Crime and abuse in e-business", in *IPTS Report*, No. 57, 2001, pp. 18-22; Collier and Spaul, "Problems in policing computer crime" (см. сноску 17 выше), p. 310.

[25] См. Collier and Spaul, "Problems in policing computer crime" (см. сноску 17 выше), p. 310; R. G. Smith, "Investigating cybercrime: barriers and solutions", paper prepared for the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p. 2. Размещено по адресу www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx.

[26] На деле газеты и телевизионные каналы при освещении успешных расследований совершаемых в Интернете преступлений ограничиваются такими впечатляющими случаями, как установление личности педофила путем раскрытия манипуляций с фотографиями подозреваемого. Более подробно об этом случае и его освещении см. "Interpol in appeal to find paedophile suspect", *New York Times*, 9 October 2007. Размещено по адресу www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin. См. также информацию, размещенную на веб-сайте Международной организации уголовной полиции (Интерпол) по адресу www.interpol.int/Public/THB/ vico/Default.asp.

[27] См. United Kingdom, Serious Organised Crime Agency, "International crackdown on mass marketing fraud revealed", 2007.

[28] Согласно докладу Национального центра борьбы с экономическими преступлениями *2006 NW3C Internet Crime Report* с рассылкой нигерийского мошеннического письма были связаны только 1,7 процента от общего объема зарегистрированных финансовых потерь в долларах США, однако в каждом из случаев речь шла об утрате в среднем 5 100 долларов США. Зарегистрировано очень мало киберпреступлений, однако все они, как правило, связаны с крупными финансовыми потерями.

c) выявление возможных сложностей при сборе точных статистических данных;

d) выявление стран, которые собирают статистическую информацию непосредственно о киберпреступности;

e) анализ необходимости и преимуществ сбора статистической информации о киберпреступности;

f) изучение возможных методов сбора такой информации;

g) обсуждение возможной модели центрального органа, ответственного за хранение статистической информации.

Тема 3. Вызовы, создаваемые киберпреступностью

Общая информация

17. В настоящее время разработке стратегий противодействия конкретным вызовам со стороны киберпреступности уделяется большое внимание. Это обусловлено двумя факторами: во-первых, некоторые из инструментов, необходимых для расследования киберпреступлений, являются новыми и поэтому требуют проведения тщательных исследований, и, во-вторых, расследование преступлений, связанных с сетевыми технологиями, сопряжено с рядом особых трудностей, не возникающих в ходе обычных расследований.

Трудности борьбы с киберпреступностью и связанными с нею угрозами

18. Борьба с киберпреступностью связана с многочисленными, характерными только для этого вида преступности, техническими и правовыми трудностями. Так, к примеру, преступники могут совершать киберпреступления при помощи средств, не требующих глубоких технических знаний, в частности, как один из примеров, программных продуктов[29], разработанных для определения местонахождения открытых портов или взлома систем защитных паролей[30]. Еще одна проблема связана с отслеживанием преступников. Несмотря на то, что пользователи оставляют множество следов при пользовании Интернет-службами, преступники могут скрывать свою личность, что затрудняет проведение расследований. Если, например, преступники в целях совершения преступлений используют точки публичного доступа к сети Интернет или незащищенные беспроводные сети, то установить их личности, возможно, будет нелегко. В целом расследование киберпреступлений осложняется тем, что с технической точки зрения в Интернете практически отсутствуют механизмы контроля, которые могли бы использовать правоохранительные

---

[29] "Websense", *Security Trends Report 2004*, p. 11; United States of America, General Accounting Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837 (Washington, D.C., 2003), p. 3; U. Sieber, "The threat of cybercrime", in *Organised Crime in Europe: The Threat of Cybercrime – Situation Report 2004* (Strasbourg, Council of Europe Publishing, 2005), p. 143.

[30] K. Ealy, "A new evolution in hack attacks: a general overview of types, methods, tools, and prevention", SANS Institute, 2003, p. 9.

органы. Интернет изначально создавался как военная сеть[31] на основе децентрализованной сетевой архитектуры, призванной сохранять свои основные функциональные возможности даже в случае атак на компоненты этой сети. Такой децентрализованный подход изначально не был направлен на содействие проведению уголовных расследований или предотвращение нападений из самой сети, и следственные мероприятия, требующие наличия тех или иных средств контроля, в таких условиях сопряжены с особыми трудностями[32].

Сфера охвата исследования

19. Изучение данной темы будет предусматривать следующее:

a) составление всеобъемлющего перечня трудностей, связанных с борьбой с киберпреступностью;

b) краткий обзор наилучших видов технической и правовой практики по преодолению этих трудностей.

Тема 4. Общие подходы к законодательству

Общая информация

20. За последние 20 лет разные страны и региональные организации в целях борьбы с киберпреступностью разработали соответствующие законодательные и правовые рамочные документы. При этом, несмотря на формирование определенных общих тенденций, положения национального законодательства стран по-прежнему заметно отличаются друг от друга.

Национальные и региональные различия

21. Существование региональных и национальных различий в законодательной сфере обусловлено, в частности, разным воздействием, оказываемым киберпреступностью на страны, о чем свидетельствует борьба со спамом[33]. Из-за нехватки и высокой стоимости ресурсов проблема спама оказалась для развивающихся стран гораздо более серьезной, чем для западных стран[34]. Что касается материалов запрещенного содержания, то в некоторых странах и регионах уголовно наказуемым может признаваться

---

[31] Краткую историю Интернета, в том числе описание его военного происхождения, см. B. Leiner and others, "A brief history of the Internet", размещено по адресу www.isoc.org/internet/history/brief.shtml.

[32] H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002).

[33] "Понимание киберпреступности – Руководство для развивающихся стран", Международный союз электросвязи, 2009 год, раздел 2.6.7.

[34] См. Organization for Economic Cooperation and Development, "Spam issues in developing countries", document DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005, p. 4. Размещено по адресу www.oecd.org/dataoecd/5/47/34935342.pdf.

распространение материалов, которые могут считаться защищенными принципом свободы слова[35] в других странах[36].

22. Киберпреступность имеет поистине транснациональные масштабы[37], и поэтому залогом успешных расследований и привлечения виновных к ответственности является международное сотрудничество[38]. Эффективное международное сотрудничество в целях предотвращения создания убежищ требует в определенной степени общего понимания проблемы и общих подходов к законодательству[39].

Сфера охвата исследования

23. Изучение данной темы будет предусматривать следующее:

---

[35] О принципе свободы слова см. T. L. Tedford and D. A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pennsylvania, Strata, 2005); E. Barendt, *Freedom of Speech* (Oxford, Oxford University Press, 2007); C. E. Baker; *Human Liberty and Freedom of Speech* (New York, Oxford University Press, 1989); J. W. Emord, *Freedom, Technology and the First Amendment* (San Francisco, Pacific Research Institute for Public Policy, 1991); о важности этого принципа применительно к электронному наблюдению см. C. Woo and M. So, "The case for Magic Lantern: September 11 Highlights – the need for increasing surveillance", *Harvard Journal of Law and Technology*, vol. 15, No. 2 (2002), pp. 530 ff.; M. Chesterman, *Freedom of Speech in Australian Law: A Delicate Plant* (Aldershot, Hampshire, Ashgate, 2000); E. Volokh, "Freedom of speech, religious harassment law, and religious accommodation law", *Loyola University Chicago Law Journal*, vol. 33, 2001, pp. 57 ff., размещено по адресу www.law.ucla.edu/volokh/harass/religion.pdf; H. Cohen, "Freedom of speech and press: exceptions to the First Amendment", Congressional Research Service Report 95-815, 2009, размещено по адресу www.fas.org/sgp/crs/misc/95-815.pdf.

[36] Обеспокоенностью в связи с соблюдением принципа свободы слова (см., например, первую поправку к Конституции Соединенных Штатов Америки) объясняется то, что в Конвенции о киберпреступности (Council of Europe, *European Treaty Series*, No. 195) некоторые акты расизма не были признаны противоправными, однако их криминализация была предусмотрена в Первом дополнительном протоколе к Конвенции о киберпреступности, касающемся криминализации актов расистского и ксенофобного характера, совершенных через компьютерные системы (Council of Europe, *European Treaty Series*, No. 189). См. также пояснительный доклад к Дополнительному протоколу по адресу http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[37] О масштабах наиболее разрушительных транснациональных кибератак см. A. D. Sofaer and S. E. Goodman, "Cyber crime and security: the transnational dimension", in *The Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 7. Размещено по адресу http://media.hoover.org/documents/0817999825_1.pdf.

[38] О необходимости международного сотрудничества в борьбе с киберпреступностью см. T. L. Putnam and D. D. Elliott, "International responses to cyber crime", in *Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), pp. 35 ff., размещено по адресу http://media.hoover.org/documents/0817999825_35.pdf; and Sofaer and Goodman, "Cyber crime and security: the transnational dimension".

[39] О принципе обоюдного признания того или иного деяния уголовно наказуемым применительно к международным расследованиям см. "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, Nos. 43 and 44, 1994 (United Nations publication, Sales No. E.94.IV.5), para. 269, размещено по адресу www.uncjin.org/Documents/EighthCongress.html; Judge Stein Schjolberg and Amanda M. Hubbard, "Harmonizing national legal approaches on cybercrime", paper prepared for the International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005, p. 5.

a) анализ усилий по выработке общих подходов к законодательству о борьбе с киберпреступностью;

b) другие элементы, относящиеся к выработке общих подходов к законодательству о борьбе с киберпреступностью, включая предполагаемую степень тяжести соответствующих деяний и последствия с точки зрения норм в области прав человека;

c) составление свода материалов региональных организаций о подходах, применяемых разными странами в целях осуществления правовых стандартов, и анализ с целью определения методов, которые могли бы способствовать обеспечению согласованности этих подходов;

d) анализ масштаба влияния различий в законодательстве о борьбе с киберпреступностью на международное сотрудничество.

Тема 5. Криминализация

Общая информация

24. Для эффективного расследования киберпреступлений и привлечения виновных к ответственности потребуется установление новых составов преступлений, если соответствующие деяния уже не признаны уголовно наказуемыми в действующем законодательстве. Существование надлежащего законодательства не только играет важную роль в деле проведения национальных расследований, но и, как это отмечалось выше, отражается на международном сотрудничестве.

Материальное уголовное право

25. Большинство всеобъемлющих региональных рамочных нормативных документов, разработанных в целях борьбы с киберпреступностью, содержат ряд положений материального уголовного права, призванных заполнить лакуны, существующие в национальном законодательстве. Стандартные положения этих рамочных документов предусматривают, в частности, криминализацию незаконного доступа, незаконного перехвата, незаконного вмешательства в данные, незаконного вмешательства в работу систем, компьютерного мошенничества и изготовления подделок с помощью компьютерных технологий. Однако в рамках национальных базовых систем могут применяться и более широкие подходы, при которых уголовно наказуемыми признаются такие деяния, как производство и распространение инструментов (таких, как программные средства или оборудование), которые могут использоваться для совершения киберпреступлений или в террористических целях, а также действия, связанные с детской порнографией, подготовкой детей к вовлечению в изготовление порнографических материалов или занятие проституцией или ненавистнической риторикой.

Сфера охвата исследования

26. При изучении этой темы будут учтены результаты рассмотрения темы 1, посвященной феномену киберпреступности, и будет предусмотрено следующее:

a) обзор национальных и региональных подходов к криминализации киберпреступности, в том числе в связи с участием и покушением;

b) оценка наилучших видов практики в отношении криминализации;

c) анализ отличий подходов к криминализации киберпреступности, применяемых в различных правовых системах и традициях.

Тема 6. Процессуальные полномочия

Общая информация

27. Для эффективного раскрытия преступлений правоохранительным органам необходимо иметь доступ к таким следственным процедурам, которые позволят им принимать необходимые меры по установлению личности преступников и сбору доказательств для уголовного преследования[40]. Такие меры могут быть аналогичны обычным следственным процедурам, не связанным с киберпреступностью. Однако ввиду того, что преступнику необязательно находиться непосредственно на месте преступления или даже вблизи этого места, то весьма вероятно, что методика расследований киберпреступлений будет отличаться от методики проведения обычных расследований[41].

Следственные мероприятия

28. Наряду с положениями, касающимися собственно составов киберпреступлений, большинство всеобъемлющих региональных рамочных документов, разработанных в целях борьбы с киберпреступностью, также содержат ряд специальных положений, призванных содействовать проведению расследований киберпреступлений. Стандартные положения предусматривают, в частности, специальные процедуры проведения обысков и изъятий, оперативные процедуры обеспечения сохранности компьютерных данных, раскрытие хранимых данных, перехват данных о содержании и сбор данных о трафике.

---

[40] О подходах к борьбе с киберпреступностью, основывающихся на учете особенностей пользователей, см. S. Görling, "The myth of user education", paper prepared for the Virus Bulletin Conference, Montreal, 11-13 October 2006, размещено по адресу www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml. См. также замечания, с которыми выступил министр внутренних дел Франции Жан-Пьер Шевенман на конференции Группы восьми, посвященной вопросам безопасности и доверия в киберпространстве и проведенной в Париже в 2000 году: "Если говорить более широко, то мы должны обучить пользователей. Они все должны понимать, что можно и что нельзя делать в Интернете, и знать о возможных угрозах. По мере расширения масштабов использования Интернета, нам, конечно, придется активизировать наши усилия в этом отношении".

[41] Благодаря используемым в Интернете протоколам связи и возможности доступа к Интернету из любой точки мира в физическом присутствии на месте, где предоставляется та или иная услуга, практически нет никакой необходимости. В силу такой независимости от места действия или места преступления многие преступления, связанные с Интернетом, имеют транснациональный характер. Об отсутствии связи между местом действия и последствиями преступлений см. "Понимание киберпреступности – Руководство для развивающихся стран" (см. сноску 13 выше), раздел 3.2.7.

29. В настоящее время правоохранительные органы сталкиваются с делами, в рамках которых используются вновь появляющиеся технологии, оказывающие негативное воздействие на применение классических следственных методов. Многие из этих трудностей все еще не решены.

Сфера охвата исследования

30. Изучение данной темы будет предусматривать следующее:

a) составление перечня примеров расследований, в рамках которых отмечалась необходимость применения специальных следственных методов в отношении киберпреступлений;

b) составление перечня различных положений о следственных процедурах, содержащихся в региональных и национальных правовых рамочных документах;

c) обзор текущих потребностей правоохранительных органов в отношении специальных положений, касающихся расследований киберпреступлений в целях решения задач, создаваемых новыми технологиями;

d) анализ различий в подходах к положениям о следственных процедурах применительно к киберпреступности в различных правовых системах и традициях

Тема 7. Международное сотрудничество

Общая информация

31. Растет количество преступлений, совершаемых в международных масштабах[42], что, в частности, объясняется тем, что преступникам, действующим через не имеющий межгосударственных границ Интернет, зачастую нет необходимости находиться в том же месте, где и жертва. Тот факт, что местонахождение потерпевших и местонахождение преступников могут не совпадать, а также мобильность преступников диктуют правоохранительным и судебным органам необходимость развития международного сотрудничества и оказания содействия тем государствам, которые относят соответствующие преступления к своей юрисдикции[43]. Налаживание эффективного международного сотрудничества является одной из основных задач в деле борьбы с преступностью, все больше приобретающей глобальный характер, как в ее традиционных формах, так и с киберпреступностью. Осложнить

---

[42] О транснациональных аспектах киберпреступности см. Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, No. 2 (2003), p. 289, размещено по адресу www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer and Goodman, "Cyber crime and security: the transnational dimension" (см. сноску 37 выше), pp. 1 ff.

[43] В этой связи см. *Руководства для законодательных органов по осуществлению Конвенции Организации Объединенных Наций против транснациональной организованной преступности и протоколов к ней* (издание Организации Объединенных Наций, в продаже под № R.05.V.2), стр. 217 текста на английском языке, размещено по адресу www.unodc.org/pdf/crime/legislative_guides/ Legislative%20guides_Full%20version.pdf.

международное сотрудничество могут различия в законодательстве и практике разных государств, равно как и относительно небольшое количество международных договоров и соглашений о международном сотрудничестве, которыми могут воспользоваться государства[44]. Кроме того, следует обсудить и согласовать вопрос о том, какие аспекты связанных с киберпреступностью дел должны считаться международными.

Инструменты международного сотрудничества

32. Существуют различные источники обеспечения правовой основы, необходимой для официального международного сотрудничества по таким вопросам, как выдача, оказание взаимной правовой помощи по уголовным делам и сотрудничество в целях конфискации. Положения о международном сотрудничестве могут быть включены в международные и региональные соглашения, в том числе речь идет о Конвенция Организации Объединенных Наций против транснациональной организованной преступности[45],

Сфера охвата исследования

33. Изучение данной темы будет предусматривать следующее:

a) перечень внутренних правовых подходов к определению международного предмета применительно к уголовной правоприменительной практике в условиях Интернета;

b) изучение возможных путей действий в вопросах создания эффективной правовой базы, включая универсальную международную базу, и других ответных мер по борьбе с киберпреступностью;

c) трудности в обеспечении эффективного международного сотрудничества по делам о киберпреступности, в частности применительно к выдаче и взаимной правовой помощи, в том числе в связи с обоюдным признанием соответствующих деяний уголовно наказуемыми и различиями в следственных методах;

d) перечень касающихся международного сотрудничества внутренних и международных положений, которые имеют отношение к расследованию киберпреступлений и уголовному преследованию за эти деяния;

e) перечень примеров наилучших видов практики на основе двусторонних и многосторонних договоров и соглашений, в том числе уроков, извлеченных из опыта деятельности сети координационных центров, работающих круглосуточно;

---

[44] Carlos A. Gabuardi, "Institutional framework for international judicial cooperation: opportunities and challenges for North America", *Mexican Law Review*, vol. 1, No. 2 (2009), p. 156, размещено по адресу http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[45] United Nations, *Treaty Series*, vol. 2225, No. 39574; относительно Конвенции см. Jennifer M. Smith, "An international hit job: prosecuting organized crime acts as crimes against humanity", *Georgetown Law Journal*, vol. 97, 2009, p. 1,118, размещено по адресу www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

f) перечень касающихся киберпреступности дел, связанных с международным сотрудничеством;

g) роль таких неофициальных способов сотрудничества, как обмен информацией, и трудности в этой связи;

h) обзор текущих потребностей соответствующих органов в области международного сотрудничества;

i) выявление осуществляемых программ по подготовке кадров, в том числе мероприятий по обмену опытом, наращиванию потенциала и технической помощи, в целях укрепления потенциала систем уголовного правосудия и предоставления странам возможностей для участия в международном сотрудничестве, и выдвижение идей на будущее в этой связи.

Тема 8. Электронные доказательства

Общая информация

34. Поскольку информация в настоящее время все чаще хранится в цифровом виде, вопрос об электронных доказательствах имеет отношение к расследованию как киберпреступлений, так и обычных преступлений. В развитых странах компьютерные и сетевые технологии стали частью повседневной жизни, и это же явление все более широко наблюдается в развивающихся странах. Увеличение емкости жестких дисков[46] и относительно низкая стоимость[47] хранения документов в цифровом виде по сравнению с хранением бумажных документов привели к увеличению количества цифровых документов[48]. В настоящее время значительная часть данных хранится только в цифровом виде[49]. Как следствие, электронные документы, в частности текстовые документы, цифровые видеозаписи и цифровые изображения[50], имеют существенное значение при расследовании киберпреступлений и в рамках связанных с этим судебных разбирательств[51].

---

[46] См. D. Abramovitch, "A brief history of hard drive control", *IEEE Control Systems Magazine*, vol. 22, No. 3 (2002), pp. 28 ff.; T. Coughlin, D. Waid and J. Porter, "The disk drive: 50 years of progress and technology innovation – the road to two billion drives", *Computer Technology Review*, April 2005, размещено по адресу www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[47] S. M. Giordano, "Electronic evidence and the law", *Information Systems Frontiers*, vol. 6, No. 2 (2006), p. 161; S. D. Willinger and R. M. Wilson, "Negotiating the minefields of electronic discovery", *Richmond Journal of Law and Technology*, vol. 10, No. 5 (2004).

[48] Lange/Minster, Electronic Evidence and Discovery, p. 6.

[49] Chet Hosmer, "Proving the integrity of digital evidence with time", *International Journal of Digital Evidence*, vol. 1, No. 1 (2002), p. 1, размещено по адресу www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[50] О приемлемости и достоверности цифровых изображений см. Jill Witkowski, "Can juries really believe what they see? New foundational requirements for the authentication of digital images", *Washington University Journal of Law and Policy*, vol. 10, 2002, pp. 267 ff.

[51] Michael Harrington, "A methodology for digital forensics", *Thomas M. Cooley Journal of Practical and Clinical Law*, vol. 7, 2004, pp. 71 ff.; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 14. О правовых основах в различных странах см. C. A. Rohrmann and J.S.A. Neto, "Digital evidence in Brazil", *Digital Evidence and Electronic Signature Law*

Правила, касающиеся электронных доказательств

35. С электронными доказательствами связан целый ряд проблем, которые возникают как на этапе их сбора, так и при определении их приемлемости[52]. В ходе сбора доказательств следователи должны выполнять определенные процедуры и требования, в частности принимать особые меры, необходимые для защиты целостности данных. Правоохранительным органам необходимо осуществлять конкретные мероприятия, чтобы успешно расследовать преступления. Возможность проведения таких мероприятий имеет особое значение в том случае, когда невозможно получить обычные виды доказательств, в частности отпечатки пальцев или показания свидетелей. В таких случаях установить личность преступника и привлечь его к ответственности позволяет надлежащий сбор и анализ цифровых доказательств[53].

36. Все более широкое применение цифровых технологий отражается и на методах работы правоохранительных органов и судов с доказательствами[54]. Бумажные документы обычно просто предъявляются суду, тогда как для цифровых доказательств могут требоваться особые процедуры, которые не могут применяться к традиционным доказательствам, в частности, когда речь идет о распечатке файлов[55].

Сфера охвата исследования

37. Изучение данной темы будет предусматривать следующее:

a) составление перечня положений, гарантий и стандартов, касающихся сбора, сохранения, хранения и анализа электронных доказательств и их приемлемости;

Review, No. 5, 2008; M. Wang, "Electronic evidence in China", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008; P. Bazin, "An outline of the French Law on digital evidence", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008; A. B. Makulilo, "Admissibility of computer evidence in Tanzania", *Digital Evidence and Electronic Signature Law Review*, No. 4, 2007; R. Winick, "Search and seizures of computers and computer data", *Harvard Journal of Law and Technology*, vol. 8, No. 1 (1994), p. 76; F. Insa, "Situation report on the admissibility of electronic evidence in Europe", in *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, p. 213.

[52] Casey, *Digital Evidence and Computer Crime* (см. сноску 51 выше), p. 9.

[53] О необходимости официальных процедур компьютерной судебной экспертизы см. R. Leigland and A. W. Krings, "A formalization of digital forensics", *International Journal of Digital Evidence*, vol. 3, No. 2 (2004).

[54] О трудностях работы с цифровыми доказательствами в условиях применения традиционных процедур и доктрин см. R. Moore, "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice*, vol. 29, No. 1 (2004), pp. 57 ff.

[55] См. John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. (Hingham, Massachusetts, Charles River Media, 2005), p. 3. Первоначальное обсуждение вопроса об использовании компьютерных распечаток см. Robinson, "The admissibility of computer printouts under the business records exception in Texas", *South Texas Law Journal*, vol. 12, 1970, pp. 291 ff.

b) анализ различий в подходах и выявление общих принципов в отношении электронных доказательств в различных правовых системах и традициях;

c) сбор информации о наилучших видах практики применительно к специализированной подготовке кадров, наращиванию потенциала и обмену технологиями;

d) анализ создания механизма трансграничного обмена цифровыми доказательствами.

Тема 9. Роль и ответственность поставщиков услуг и частного сектора

Общая информация

38. Предупреждение киберпреступности и расследование соответствующих дел зависят от ряда различных элементов. Даже в случае, когда преступник действует в одиночку, целый ряд людей и предприятий автоматически становятся причастными к совершению киберпреступления. Интернет имеет такую структуру, что для передачи простого сообщения электронной почты требуются услуги нескольких поставщиков: поставщика услуг электронной почты, поставщиков услуг доступа к сети и маршрутизаторов электронной почты, доставляющих сообщения получателям. Аналогичная ситуация складывается в отношении загрузки из сети фильмов, содержащих детскую порнографию. В процессе загрузки участвуют поставщик содержания, загружающий изображения в сеть (например, на веб-сайт), поставщик сервера, предоставивший место для хранения информации, загруженной на веб-сайт, маршрутизаторы, доставляющие файлы пользователю, и, наконец, поставщик услуг доступа, предоставивший пользователю возможность доступа к Интернету.

39. Хотя зачастую основной акцент делается на обеспечении принятия надлежащего законодательства, однако важная роль в деле предупреждения киберпреступлений и оказания содействия в их расследовании по-прежнему отводится частному сектору. В то же время участие его представителей в расследовании киберпреступлений сопряжено с рядом проблем.

Правовые вопросы

40. С учетом того, что киберпреступление не может быть совершено без участия поставщиков услуг, а также того, что такие поставщики зачастую не в состоянии предотвратить киберпреступления, возникает вопрос о целесообразности ограничения ответственности поставщиков услуг. Ответ на этот вопрос имеет важнейшее значение с точки зрения экономических аспектов развития инфраструктуры информационно-коммуникационных технологий.

41. Эффективность усилий правоохранительных органов во многом зависит от сотрудничества поставщиков Интернет-услуг. В этой связи высказываются некоторые опасения, поскольку ограничение ответственности поставщиков услуг за действия, совершаемые их пользователями, может сказаться на сотрудничестве и поддержке со стороны поставщиков услуг в деле

расследования киберпреступлений, а также на практических мерах по предупреждению киберпреступности.

Роль отраслевых предприятий

42. Отраслевой сектор играет важную роль в деле борьбы с киберпреступностью по ряду направлений: от разработки и осуществления решений в области защиты своих собственных услуг от противоправного использования до защиты пользователей и содействия проводимым расследованиям. Меры, принимаемые отраслевыми предприятиями в целях собственной защиты, зачастую являются логическим компонентом комплексных стратегий ведений дел, и, как правило, для их принятия не требуется какой-либо особой правовой основы, если только они не связаны с противозаконными активными контрмерами. Меры защиты пользователей, при условии, что они принимаются с их согласия, также не вызывают проблем. Вместе с тем во многих странах участие представителей отраслевого сектора в уголовных расследованиях сопряжено с проблемами, и к их решению применяются различные подходы. Некоторые страны привлекают представителей частного сектора к участию в уголовных расследованиях исключительно на добровольной основе и разработали руководящие указания в целях содействия налаживанию сотрудничества между ними и правоохранительными органами. В других странах применяется иной подход, в соответствии с которым на отраслевые предприятия налагаются юридические обязательства по сотрудничеству с правоохранительными органами в деле проведения уголовных расследований.

Сфера охвата исследования

43. Изучение данной темы будет предусматривать следующее:

a) подходы и виды практики, регулирующие ответственность поставщиков услуг, в том числе в разбивке по различным видам таких поставщиков;

b) схема ролей, характерных особенностей и функций частного сектора, включая поставщиков услуг;

c) практика частного сектора в деле предупреждения киберпреступлений и их расследования;

d) практика в деле сотрудничества между частным сектором и правоохранительными органами в области предупреждения киберпреступлений и их расследования;

e) возможности национальных и международных поставщиков услуг в деле оказания помощи правоохранительным органам в предупреждении киберпреступлений и их расследовании;

f) распределение издержек в связи с киберпреступностью;

g) оценка сильных и слабых сторон применяемых в настоящее время подходов.

Тема 10. Потенциал в области предупреждения преступности и уголовного правосудия и другие меры по противодействию киберпреступности

Общая информация

44. При обсуждении мер борьбы с киберпреступностью зачастую в центре внимания оказываются правовые меры противодействия, однако стратегии борьбы с киберпреступностью, как правило, предусматривают более широкий подход.

Другие меры противодействия

45. В дополнение к правовым мерам по противодействию киберпреступности применяются и другие меры, к которым относятся, в частности, принятие мер по предупреждению преступности, создание необходимой инфраструктуры для расследования преступлений и уголовного преследования за их совершение (например, оборудование и персонал), подготовка экспертов, занимающихся вопросами борьбы с киберпреступностью, разработка наилучших видов практики, просвещение пользователей Интернета и технические решения, направленные на предупреждение или расследование киберпреступлений.

Сфера охвата исследования

46. Изучение данной темы будет предусматривать следующее:

a) обзор других подходов, применяемых в борьбе с киберпреступностью;

b) меры по предупреждению киберпреступности;

c) определение методов оценки эффективности таких подходов;

d) анализ взаимосвязи между различными мерами и возможностей применения комплекса таких мер;

e) возможная роль академических кругов, особенно применительно к подготовке учебных планов и научным исследованиям феномена киберпреступности.

Тема 11. Международные организации

Общая информация

47. В 70-х и 80-х годах прошлого века правовые подходы к борьбе с киберпреступностью разрабатывались в основном на национальном уровне. В 90-х годах проблемой киберпреступности занялись региональные и международные организации, в том числе Генеральная Ассамблея, которая за прошедшие годы приняла несколько резолюций, касающихся киберпреступности[56], Содружество (Типовой закон о киберпреступности и возможное расширение Харарского плана с целью охвата электронных

[56] См., например, резолюции Генеральной Ассамблеи 45/121, 55/63, 56/121 и 60/177.

данных), Совет Европы (Конвенция о киберпреступности), Европейский союз (Рамочное решение о кибератаках на информационные системы и принятая Советом в соответствии со статьей 34 Договора о Европейском союзе Конвенция о взаимной помощи в уголовных делах между государствами – членами Европейского союза), Содружество независимых государств (СНГ) (Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 года), Организация американских государств и Шанхайская организация сотрудничества. Международные организации, включая Международный союз электросвязи. который провел ряд мероприятий в рамках Глобальной программы кибербезопасности, и Управление Организации Объединенных Наций по наркотикам и преступности, занимались сбором данных и подготовкой исследований.

Согласование стандартов

48. Применение единых унифицированных стандартов в отношении технических протоколов доказало свою эффективность, в связи с чем возникает вопрос о способах предупреждения коллизии различных международных подходов[57]. Наиболее всеобъемлющий подход предусмотрен Конвенцией Совета Европы о киберпреступности и Типовым законом Содружества о киберпреступности, поскольку в них включены положения материального уголовного права и процессуального права, а также положения о международном сотрудничестве. В рамках этой темы можно было бы изучить существующие рамочные документы в целях определения их сферы охвата, преимуществ, недостатков и любых возможных пробелов.

Сфера охвата исследования

49. Изучение данной темы будет предусматривать следующее:

a) перечень наилучших видов практики региональных и международных организаций, включая Организацию Объединенных Наций;

b) сильные и слабые стороны применяемых в настоящее время подходов;

c) анализ пробелов в существующих международно-правовых подходах.

Тема 12. Техническая помощь

Общая информация

50. Киберпреступность иногда считают проблемой, затрагивающей главным образом развитые страны, однако это не так. В 2005 году число Интернет-пользователей в развивающихся странах впервые превысило число Интернет-пользователей в промышленно развитых странах[58]. Поскольку одна из

---

[57] Более подробно см. M. Gercke, "National, regional and international legislative approaches in the fight against cybercrime", *Computer Law Review International*, 2008, pp. 7 ff.

[58] См. Development Gateway's Special Report, *Information Society – The Next Steps* (2005).

основных целей стратегий противодействия киберпреступности заключается в защите пользователей от таких преступлений, важность борьбы с киберпреступностью в развивающихся странах переоценить невозможно. При этом также обязательно следует учитывать, что киберпреступность может по-разному воздействовать на развивающиеся и развитые страны. В 2005 году Организация экономического сотрудничества и развития опубликовала доклад, в котором проводится анализ последствий рассылки спама на развивающиеся страны[59], и пришла к выводу, что развивающиеся страны часто сообщают о том, что их Интернет-пользователи чаще становятся жертвами рассылки спама и использования Интернета в неправомерных целях, чем пользователи в развитых странах.

Техническая помощь

51. Вследствие транснационального характера киберпреступности борьба с этим явлением требует эффективных и скоординированных усилий всех стран. В предоставлении технической помощи в равной мере заинтересованы как развивающиеся, так и развитые страны. Одной из ключевых задач в деле борьбы с киберпреступностью является предотвращение создания "безопасных убежищ" для киберпреступников[60]. В этой связи одной из главных задач международного сообщества стало наращивание потенциала развивающихся стран, который позволит им бороться с киберпреступностью.

52. Важность технической помощи отражена в Салвадорской декларации, которая была принята двенадцатым Конгрессом Организации Объединенных Наций по предупреждению преступности и уголовному правосудию в 2010 году и в которой Управлению Организации Объединенных Наций по наркотикам и преступности рекомендуется, по получении соответствующей просьбы, оказывать техническую помощь государствам в борьбе с киберпреступностью. В ней также предлагается рассмотреть возможность разработки совместно со всеми заинтересованными партнерами плана действий по наращиванию потенциала на международном уровне. Техническая помощь, учитывающая все современные новшества, должна оказываться на непрерывной основе.

---

[59] "Spam issues in developing countries" (см. сноску 34 выше).

[60] Этим вопросом занимался целый ряд международных организаций. Генеральная Ассамблея в своей резолюции 55/63 заявила следующее: "Государства должны обеспечить, чтобы их законодательство и практика не оставляли возможности тем, кто злоупотребляет информационными технологиями, укрываться где бы то ни было". Полный текст резолюции размещен по адресу: http://daccess-dds-ny.un.org.doc/UNDOC/GEN/NOO/563/19/PDF/N0056319.pdf?OpenElement. В принципах и плане действий по борьбе с высокотехнологичной преступностью, которые были утверждены на Совещании министров юстиции и внутренних дел Группы восьми, проведенном в Вашингтоне, О.К., 10 декабря 1997 года, отмечено следующее: "Лица, преступно злоупотребляющие информационными технологиями, не должны иметь возможность укрываться где бы то ни было".

Сфера охвата исследования

53. Изучение данной темы будет предусматривать следующее:

a) определение основных элементов и принципов оказания технической помощи в борьбе с киберпреступностью;

b) составление перечня существующих курсов подготовки кадров по вопросам киберпреступности на национальном, региональном и международном уровнях;

c) выявление наилучших видов практики в деле предоставления технической помощи в связи с киберпреступностью.

Приложение II

Методология исследования

1. В целях выполнения мандата группы экспертов в отношении исследования была выработана нижеизложенная структура для содействия его проведению под эгидой группы экспертов.

2. Каждая страна будет иметь право представить свои мнения, которые будут отражены в исследовании.

3. На Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) будет возложена задача по подготовке исследования, в том числе по составлению вопросника, сбору и анализу данных и подготовке проекта текста исследования. Для выполнения этой задачи ЮНОДК будет использовать свои внутренние экспертные возможности и потенциал различных тематических подразделений ЮНОДК (Отдел по вопросам международных договоров, Сектор анализа политики и исследований). В этих целях должны быть предоставлены надлежащие внебюджетные ресурсы, с тем чтобы позволить ЮНОДК эффективно выполнять эти функции. Для оказания помощи Секретариату в обеспечении надлежащей представленности крупных технологических экспертных источников информации, а также учета различных систем и потребностей каждая региональная группа сообщит Секретариату имена правительственных экспертов (не более шести), их контактную информацию и области специализации. Секретариат, по мере необходимости, будет проводить специальные консультации с этими экспертами с целью получения их вклада.

4. Секретариат будет регулярно информировать и оповещать бюро группы экспертов о ходе работы и распространять среди государств-членов протоколы проведенных консультаций. Подготовка списка экспертов не преследует цели создать в каком бы то ни было виде закрытую группу экспертов или другие параллельные или вспомогательные органы группы экспертов.

5. В целях сбора информации ЮНОДК подготовит вопросник для последующего распространения среди государств-членов, межправительственных организаций и субъектов частного сектора (ориентировочный график см. ниже), который будет составлен в виде единого опросного инструмента, основывающегося на схеме, изложенной в концептуальном/рабочем документе первого совещания группы экспертов, с внесенными поправками, и на рекомендациях первого совещания группы экспертов, как они отражены в докладе о его работе.

6. Во-вторых, Секретариат, по мере потребности, с учетом необходимости в сбалансированной представленности различных регионов, будет проводить консультации с представителями частного сектора, включая представителей поставщиков Интернет-услуг, пользователей услуг и других заинтересованных участников; представителями академических кругов как из развитых, так и из развивающихся стран; и представителями соответствующих межправительственных организаций.

Ориентировочный график

Январь 2011 года: Программные установки и руководящие положения, сформулированные первым совещанием группы экспертов. Утверждение тем, методологии и графика исследования.

Февраль-апрель 2011 года: Выявление экспертов для оказания помощи ЮНОДК в проведении исследования (см. выше). Представление их имен бюро группы экспертов. Сообщение имен правительственных экспертов через региональные группы.

Апрель 2011 года: Двадцатая сессия Комиссии по предупреждению преступности и уголовному правосудию. Распространение проекта вопросника ЮНОДК для сбора информации. Обращение к государствам-членам с просьбой представить замечания/комментарии. Проведение консультаций в режиме онлайн для получения комментариев членов группы экспертов. Признание Комиссией результатов первого совещания группы экспертов и содержания будущей работы, как оно было предложено на первом совещании.

Середина июня 2011 года: Получение комментариев по вопроснику.

Середина июля 2011 года: Окончательная доработка вопросника и его распространение среди государств-членов. Вопросник будет также направлен посредством отдельных почтовых отправлений межправительственным организациям и представителям частного сектора и академических учреждений, которым будет предложено представить информацию и ответить на вопросы, имеющие отношение к их деятельности. Будут предоставлены гарантии, особенно частному сектору, что будет сохранен конфиденциальный характер любых полученных данных и что, в случае опубликования, эти данные будут публиковаться на анонимной основе.

Середина июля – конец декабря 2011 года: Сбор данных и их классификация (5,5 месяцев; в середине этого срока в начале октября 2011 года Секретариат направит напоминание).

Начало декабря 2011 года: Второе совещание группы экспертов в рамках возобновленной двадцатой сессии Комиссии по преступности. Представление информации о ходе работы. Промежуточный доклад о ходе работы в целях информирования Комиссии по преступности на ее двадцать первой сессии (апрель 2012 года).

Апрель 2012 года: Представление промежуточного доклада о ходе работы Комиссии по преступности на ее двадцать первой сессии.

Середина января 2012 года – июль 2012 года: Анализ данных и составление текста исследования. Окончательная доработка проекта текста исследования.

Август 2012 года: Распространение проекта текста исследования среди членов группы экспертов для обеспечения своевременной подготовки к проведению третьего совещания группы экспертов.

Октябрь 2012 года: Проведение третьего совещания группы экспертов для рассмотрения, доработки и принятия проекта исследования.

Апрель 2013 года: Представление исследования на рассмотрение Комиссии по преступности на ее двадцать второй сессии.