20 December 2010
Russian
Original: English

Группа экспертов по киберпреступности
Вена, 17-21 января 2011 года

Проекты тем для рассмотрения в рамках всестороннего исследования проблемы киберпреступности и ответных мер

I. 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. Эта рекомендация была принята Комиссией по предупреждению преступности и уголовному правосудию и затем Экономическим и Социальным Советом в его резолюции 2010/18.

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

V.10-58679 (R)

международное сотрудничество), а также 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 13 тем в соответствии с поставленной в Декларации задачей. Эти 13 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) правонарушения, связанные с киберпреступностью (тема 1);

b) статистические данные (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 пять конкретных областей принятия правовых ответных мер:

a) согласование законодательства (тема 4);

b) материальное уголовное право (тема 5);

c) следственные инструменты (тема 6);

d) международное сотрудничество (тема 7);

e) электронные доказательства (тема 8);

f) ответственность (тема 9).

Неюридические 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.

Ответные меры со стороны международного сообщества (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 согласованного подхода к борьбе с киберпреступностью техническая помощь рассматривается в рамках всестороннего исследования как отдельная тема.

Ответные меры со стороны частного сектора (тема 13)

10. Как уже отмечалось, в Салвадорской декларации рекомендуется также в рамках всестороннего исследования провести анализ ответных мер со стороны частного сектора.

II. Подробный обзор тем

Тема 1. Явление киберпреступности

Общая информация

11. Компьютерная преступность и, более конкретно, киберпреступность – термины, используемые для обозначения конкретной категории преступных деяний. К этой категории относятся правонарушения от размещения запрещенной информации до некоторых форм экономической преступности. 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

12. В 1960–х годах, 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 1970-х годах произошел переход от традиционных имущественных преступлений против компьютерных систем[3] к новым формам преступности[4], в частности противоправному использованию

---

[1] О связанных с этим проблемах см. Slivka/Darrow; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, p. 217 et seq.

[2] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, p. 217 et seq.

[3] Gemignani, Computer Crime: The Law in ‘80, Indiana Law Review, Vol. 13, 1980, p. 681.

[4] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, p. 217 et seq.

компьютерных систем[5] и манипуляциям[6] с электронными данными[7]. Переход от личного заключения сделок к заключению сделок при помощи компьютеров способствовал возникновению еще одной новой формы преступности – компьютерного мошенничества[8]. В 1980-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 и появление 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 1990-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

---

[5] Freed, Materials and cases on computer and law, 1971, p. 65.

[6] Bequai, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, p. 8 et seq.

[7] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, p. 225 et seq; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[8] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, p. 217 et seq; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, p. 22.

[9] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, p. 73.

[10] BloomBecker, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, p. 428; Schmidt, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 et seq. Denning, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 et seq; Weiss, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, p. 1 et seq; Bigelow, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, p. 401; Thackeray, Computer-Related Crimes, Jurimetrics Journal, 1984, p. 300 et seq.

[11] Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, p. 336 et seq; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, p. 89 et seq; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review, Vol. 33, 1984, p. 777 et seq.

[12] Child Pornography, CSEC World Congress Yokohama Conference, 2001, p. 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, United States House of Representatives, 109th Congress, 2007, p. 9.

[13] Под термином "фишинг" ("phishing") понимается действие, имеющее целью побудить жертву к раскрытию личной или секретной информации. Этот термин (созвучный

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

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

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

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

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

d) перечень соответствующих дел;

e) определение и типология киберпреступности;

f) механизмы предупреждения преступности (технические);

g) изучение важности определения киберпреступности;

h) соображения относительно возможности решений, предусматривающих исключение некоторых киберпреступлений из числа уголовно наказуемых деяний.

Тема 2. Статистические данные

Общая информация

14. 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

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. "Понимание киберпреступности – Руководство для развивающихся стран", Международный союз электросвязи, 2009 год, раздел 2.8.4.

[14] "Бот-сеть" – краткий термин, обозначающий группу компьютеров, зараженных программой, которая позволяет посторонним лицам управлять ими удаленно. Более подробно об этом см. Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, p. 4.

[15] Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006.

[16] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, p. 499 et seq.

[17] Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, p. 308, на веб-сайте: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

киберпреступности позволит правоохранительным органам совершенствовать стратегии борьбы с киберпреступностью, предотвращать возможные атаки и обеспечивать принятие и осуществление более целенаправленного и эффективного законодательства.

Нынешнее положение дел в области сбора статистических данных о киберпреступности

15. 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].

16. 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. Osborne/Wernicke, Introduction to Crime Analysis, 2003, p. 1 et seq; размещено по адресу www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

[19] В этом контексте см. Overcoming barriers to trust in crimes statistics, United Kingdom Statistics Authority, 2009, p. 9, на веб-сайте: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[20] Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, p. 168, на веб-сайте: 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, Oct. 2006, p. 3.

[22] О связанных с этим трудностях см. Kabay, Understanding Studies and Surveys of Computer Crime, 2009, на веб-сайте: 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. Heise News, 27.10.2007, на веб-сайте: www.heise-security.co.uk/news/80152. 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

17. 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. Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, на веб-сайте: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, p. 310, на веб-сайте: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620andrep=rep1andtype=pdf.

[25] См. Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, p., 310, на веб-сайте: http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.66.1620andrep=rep1andtype=pdf; Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, p. 2, на веб-сайте: www.aic.gov.au/conferences/other/ smith_russell/2003-09-cybercrime.pdf.

[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", The New York Times, 09.10.2007, на веб-сайте: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1andoref= slogin; а также информацию, размещенную на веб-сайте Интерпола по адресу: www.interpol.int/Public/THB/vico/Default.asp.

[27] См. SOCA, "International crackdown on mass marketing fraud revealed, 2007", на веб-сайте: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[28] Согласно докладу Национального центра борьбы с экономическими преступлениями об Интернет-преступности за 2006 год 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

18. 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

19. 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 органы. Интернет изначально создавался как военная сеть[31] на основе

---

[29] "Websense Security Trends Report 2004", p. 11; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, p. 3; Sieber, Council of Europe Organised Crime Report 2004, p. 143.

[30] Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", p. 9.

[31] Краткую историю Интернета, в том числе описание его военного происхождения см. Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, "A Brief History of the Internet", на веб-сайте: www.isoc.org/internet/history/brief.shtml.

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

20. Изучение данной темы будет предусматривать следующее:

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

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

Тема 4. Согласование законодательства

Общая информация

21. 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

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

---

[32] Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

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

[34] См. Spam Issue in Developing Countries, P. 4, на веб-сайте: www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] Обеспокоенностью в связи с соблюдением принципа свободы слова объясняется то, что в Конвенции о киберпреступности некоторые акты расизма не были признаны противоправными, однако их криминализация была предусмотрена в Первом дополнительном протоколе. См. Пояснительный доклад к Первому дополнительному протоколу, № 4.

[36] О принципе свободы слова см. Tedford/HerbeckHaiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of

23. 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 единого понимания проблемы и согласования законодательства[39].

Сфера охвата исследования

24. Изучение данной темы будет предусматривать следующее:

a) анализ достижений и проблем в области усилий по согласованию законодательства о борьбе с киберпреступностью;

b) 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;

c) анализ масштаба влияния различий в правовых стандартах на международное сотрудничество;

d) определение методов разработки законодательства, обеспечивающих необходимую гибкость для сохранения основополагающих правовых традиций в рамках процесса согласования.

Speech; Emord, Freedom, Technology and the First Amendment, 1991; о важности этого принципа применительно к электронному наблюдению см.: Woo/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, p. 530 et seq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; Volokh, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, p. 57 et seq, на веб-сайте: www.law.ucla.edu/volokh/harass/religion.pdf ; Cohen, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, на веб-сайте www.fas.org/sgp/crs/misc/95-815.pdf.

[37] О масштабах наиболее разрушительных транснациональных кибератак см. Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 7, на веб-сайте: http://media.hoover.org/documents/0817999825_1.pdf.

[38] О важности международного сотрудничества в борьбе с киберпреступностью см. Putnam/Elliott, International Responses to Cyber Crime, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 35 et seq, на веб-сайте: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq, на веб-сайте: http://media.hoover.org/documents/0817999825_1.pdf.

[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, 269, на веб-сайте: www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, p. 5, на веб-сайте: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

Тема 5. Криминализация киберпреступлений

Общая информация

25. Для эффективного расследования киберпреступлений и привлечения виновных к ответственности потребуется признание соответствующих деяний уголовно наказуемыми, если это уже не сделано 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

26. 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 изготовления подделок с помощью компьютерных технологий. Однако существуют также и более широкие подходы, в рамках которых уголовно наказуемыми признаются такие деяния, как производство и распространение инструментов (таких, как программные средства или оборудование), которые могут использоваться для совершения киберпреступлений, действия, связанные с детской порнографией, подготовка детей к вовлечению в изготовление порнографических материалов или занятие проституцией или ненавистническая риторика.

Сфера охвата исследования

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

a) обзор национальных и региональных подходов к криминализации киберпреступности;

b) оценка наилучших видов практики в отношении криминализации;

c) анализ отличий подходов к криминализации киберпреступности, применяемых в странах общего и гражданского права.

Тема 6. Следственные процедуры

Общая информация

28. 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

29. 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.

30. В дополнение к этим стандартным положениям ряд государств приняли меры для решения таких конкретных задач, как перехват речевой связи по Интернету (VoIP)[42]. Хотя в большинстве государств предусмотрены такие следственные процедуры, как прослушивание телефонных разговоров, которые позволяют им перехватывать сообщения, передаваемые как по проводной, так и по мобильной связи[43], таких мер, как правило, не достаточно для того, чтобы перехватывать сообщения, передаваемые по Интернет-протоколу VoIP.

---

[40] О подходах к борьбе с киберпреступностью, основывающихся на учете особенностей пользователей, см. Görling, The Myth Of User Education, 2006, по адресу www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. См. также замечания, с которыми выступил министр внутренних дел Франции Жан-Пьер Шевенман на Конференции Группы восьми 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 последствиями преступлений см. "Понимание киберпреступности – Руководство для развивающихся стран", Международный союз электросвязи, 2009 год, раздел 3.2.7.

[42] Термины "речевая связь по Интернету или "IP-телефония" используются для описания технологии передачи голосовых сообщений при помощи сетей с коммутацией пакетов и соответствующих протоколов. Более подробно см. Swale, Voice Over IP: Systems and Solutions, 2001; Black, "Voice Over IP", 2001.

[43] О важности перехвата и технических решениях см.: Karpagavinayagam/State/Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection", ICIMP 2007. О проблемах, связанных с перехватом передаваемых данных см. SwaleChochliouros/Spiliopoulou/Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response", in Janczewski/Colarik, "Cyber Warfare and Cyber Terrorism", 2007, p. 424.

Перехват обычных телефонных разговоров осуществляется при помощи поставщиков услуг телефонной связи[44]. Применительно к IP-телефонии правоохранительные органы, как правило, действуют по тому же принципу и обращаются к поставщикам Интернет-услуг и поставщикам услуг по IP-телефонии. Если же услуги связи IP-телефонии предоставляются на основе технологии передачи данных в распределенной системе одноуровневых сетей, то поставщики услуг, возможно, будут не в состоянии перехватить сообщения[45].

Сфера охвата исследования

31. Изучение данной темы будет предусматривать следующее:

a) примеры расследований, в рамках которых отмечалась необходимость специальных мер по расследованию киберпреступлений;

b) перечень 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;

d) анализ различий в подходах к положениям о следственных процедурах применительно к киберпреступности в странах общего и гражданского права.

Тема 7. Международное сотрудничество

Общая информация

32. Растет количество преступлений, совершаемых в международных масштабах[46], 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

---

[44] Об отличиях связи, обеспечиваемой при помощи ТСОП и VoIP, см. Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

[45] О перехвате сообщений, передаваемых при помощи IP-телефонии, правоохранительными органами см. Bellovin and others, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

[46] О транснациональных аспектах киберпреступности см. Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law and Policy, Vol. 12, No. 2, p. 289, на веб-сайте: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq, на веб-сайте: http://media.hoover.org/documents/0817999825_1.pdf.

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[47]. 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. Различия в законодательстве и практике разных государств могут осложнить международное сотрудничество, равно как и относительно небольшое количество международных договоров и соглашений о международном сотрудничестве, которыми могут воспользоваться государства[48].

Механизмы международного сотрудничества

33. Существуют четыре основных источника обеспечения правовой основы, необходимой для официального международного сотрудничества в таких формах, как выдача, оказание взаимной правовой помощи по уголовным делам и сотрудничество в целях конфискации.

34. Во-первых, положения о международном сотрудничестве могут быть включены в международные и региональные соглашения, направленные на борьбу с конкретной формой международной преступности, такие как Конвенция Организации Объединенных Наций против транснациональной организованной преступности[49,50] и Конвенция Совета Европы о киберпреступности[51]. Во-вторых, существуют региональные договоры о международном сотрудничестве, в частности, конвенции Совета Европы, межамериканские конвенции и конвенции Сообщества по вопросам развития стран Юга Африки о выдаче или взаимной правовой помощи по уголовным делам. Третьим источником являются двусторонние соглашения о выдаче или взаимной правовой помощи. Такие соглашения, как правило, содержат конкретную информацию, касающуюся видов запросов, которые могут быть представлены, и определяют соответствующие процедуры и формы взаимодействия, а также права и обязанности запрашивающих и

---

[47] В этой связи см. руководства для законодательных органов по осуществлению Конвенции Организации Объединенных Наций против транснациональной организованной преступности и протоколов к ней, 2004 год, стр. 217 текста на английском языке, размещено по адресу: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[48] Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, p. 156, на веб-сайте: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[49] Относительно Конвенции см. Smith, An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, p. 1118, на веб-сайте: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[50] Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. Текст Конвенции на английском языке и список подписавших и ратифицировавших ее государств размещены на веб-сайте: www.oas.org/juridico/english/sigs/a-55.html.

[51] Council of Europe Convention on Cybercrime, ETS 185.

запрашиваемых государств[52]. Четвертым источником для налаживания международного сотрудничества является внутреннее право, которое может предусматривать международное сотрудничество на основе взаимности или по отдельным делам.

Сфера охвата исследования

35. Изучение данной темы будет предусматривать следующее:

a) задачи в области международного сотрудничества по делам о киберпреступности;

b) перечень касающихся международного сотрудничества положений, которые применимы к расследованию киберпреступлений и уголовному преследованию за эти деяния;

c) перечень примеров наилучших видов практики на основе двусторонних соглашений;

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

e) роль таких неофициальных способов сотрудничества, как обмен оперативными данными;

f) обзор текущих потребностей соответствующих органов в области международного сотрудничества.

Тема 8. Электронные доказательства

Общая информация

36. 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[53] и низкая стоимость[54] хранения документов в цифровом виде по сравнению с хранением бумажных документов привели к увеличению количества цифровых

---

[52] См. в этой связи Типовой договор Организации Объединенных Наций о взаимной помощи в области уголовного правосудия, 1990 год, резолюция 45/117 Генеральной Ассамблеи; Руководства для законодательных органов по осуществлению Конвенции Организации Объединенных Наций против транснациональной организованной преступности и протоколов к ней, 2004 год, стр. 217 текста на английском языке; размещено по адресу: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[53] См. Abramovitch, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, p. 28 et seq; Coughlin/Waid/Porter, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, на веб-сайте: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[54] Giordano, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, p. 161; Willinger/Wilson, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, 2004, Vol. X, No. 5.

документов[55]. В настоящее время значительная часть данных хранится только в цифровом виде[56]. Как следствие, электронные документы, в частности текстовые документы, цифровые видеозаписи и цифровые изображения[57], имеют существенное значение при расследовании киберпреступлений и в рамках связанных с этим судебных разбирательств[58].

Правила, касающиеся электронных доказательств

37. С электронными доказательствами связан целый ряд проблем, которые возникают как на этапе сбора, так и при определении их приемлемости[59]. 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[60].

38. Все более широкое применение цифровых технологий отражается и на методах работы правоохранительных органов и судов с доказательствами[61]. Бумажные документы обычно просто предъявляются суду, тогда как для цифровых доказательств могут требоваться особые процедуры, которые не

---

[55] Lange/Minster, Electronic Evidence and Discovery, 2004, 6.

[56] Homer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, p. 1, на веб-сайте: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[57] О приемлемости и достоверности цифровых изображений см. Kwiatkowski, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law and Policy, p. 267 et seq.

[58] Harrington, A Methodology for Digital Forensics, T.M. Cooley J. Pac. and Clinical L., 2004, Vol. 7, p. 71 et seq; Casey, Digital Evidence and Computer Crime, 2004, p. 14. О правовых рамках, действующих в различных странах, см. Rohrmann/Neto, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Wang, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Bazin, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Makulilo, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5. Winick, Search and Seizures of Computers and Computer Data, Harvard Journal of Law and Technology, 1994, Vol. 8, No. 1, p. 76; 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

[59] Casey, Digital Evidence and Computer Crime, 2004, p. 9.

[60] О необходимости утверждения официальных процедур компьютерной судебной экспертизы см. Leigland/Krings, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2.

[61] О проблемах работы с цифровыми доказательствами с применением традиционных процедур и доктрин см. 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, p. 57 et seq.

могут применяться к традиционным доказательствам, в частности, когда речь идет о распечатке файлов[62].

Сфера охвата исследования

39. Изучение данной темы будет предусматривать следующее:

a) перечень положений, касающихся обращения с электронными доказательствами и их приемлемости;

b) анализ различий в подходах и выявление общих принципов в отношении электронных доказательств в странах общего и гражданского права.

Тема 9. Ответственность поставщиков Интернет-услуг

Общая информация

40. 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[63]. Аналогичная ситуация складывается в отношении загрузки из сети фильмов, содержащих детскую порнографию. В процессе загрузки участвуют поставщик содержимого, 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.

Роль поставщика Интернет-услуг

41. 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 Интернет-услуг[64]. Ответ на этот вопрос имеет важнейшее значение с точки зрения

---

[62] См. Vacca, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, p. 3. Первоначальное обсуждение вопроса об использовании распечатанных документов см. Robinson, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, p. 291 et seq.

[63] Об архитектуре сети и последствиях с точки зрения участия поставщиков услуг см. Black, Internet Architecture: An Introduction to IP Protocols, 2000; Zuckerman/McLaughlin, Introduction to Internet Internet Architecture and Institutions, 2003, на веб-сайте: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[64] Первичные замечания по этому вопросу см. Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, p. 15 et seq, на веб-сайте: www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

экономических аспектов развития инфраструктуры информационно-коммуникационных технологий.

42. Эффективность усилий правоохранительных органов во многом зависит от сотрудничества поставщиков Интернет-услуг. В этой связи высказываются некоторые опасения, поскольку ограничение ответственности поставщиков Интернет-услуг за действия, совершаемые их пользователями, может сказаться на сотрудничестве и поддержке со стороны поставщиков Интернет-услуг в деле расследования киберпреступлений, а также на практических мерах по предупреждению киберпреступности.

Сфера охвата исследования

43. Изучение данной темы будет предусматривать следующее:

a) перечень подходов, регулирующих ответственность поставщиков Интернет-услуг в разбивке по различным видам таких поставщиков;

b) концепция ограничения ответственности поставщиков Интернет-услуг;

c) возможности поставщиков Интернет-услуг в деле оказания помощи правоохранительным органам и предупреждения киберпреступности.

Тема 10. Неюридические 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.

Неюридические меры по противодействию киберпреступности

45. К неюридическим мерам по противодействию киберпреступности относятся, в частности, создание необходимой инфраструктуры для расследования преступлений и уголовного преследования за их совершение (например, оборудование и персонал), подготовка экспертов, занимающихся вопросами борьбы с киберпреступностью, просвещение пользователей Интернета и технические решения, направленные на предупреждение или расследование киберпреступлений.

Сфера охвата исследования

46. Изучение данной темы будет предусматривать следующее:

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

b) определение методов оценки эффективности таких подходов;

c) анализ взаимосвязи между различными мерами неюридического характера и возможности применения комплекса таких мер.

Тема 11. Международные организации

Общая информация

47. В 70-х и 80-х годах прошлого века правовые механизмы борьбы с киберпреступностью разрабатывались в основном на национальном уровне. В 1990-х годах проблемой киберпреступности занялись региональные и международные организации, в том числе Генеральная Ассамблея Организации Объединенных Наций, которая за прошедшие годы приняла несколько резолюций, касающихся киберпреступности[65]. Содружество (Типовой закон о киберпреступности), Совет Европы (Конвенция о киберпреступности) и Европейский союз (решение о кибератаках на информационные системы).

Согласование стандартов

48. Применение единых согласованных стандартов в отношении технических протоколов доказало свою эффективность, в связи с чем возникает вопрос о способах предупреждения коллизии различных международных подходов[66]. Наиболее всеобъемлющий подход предусмотрен Конвенцией Совета Европы о киберпреступности и Типовым законом Содружества о киберпреступности, поскольку в них предусмотрены положения материального уголовного права, процессуального права и 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 недоработок.

Сфера охвата исследования

49. Изучение данной темы будет предусматривать следующее:

a) перечень наилучших видов практики региональных и международных организаций;

b) преимущества и недостатки существующих 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-

---

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

[66] Более подробно см. Gercke, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, p. 7 et seq.

пользователей в развивающихся странах впервые превысило число Интернет-пользователей в промышленно развитых странах[67]. Поскольку одна из 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 развития и сотрудничества опубликовала доклад, в котором проводится анализ последствий рассылки спама на развивающиеся страны[68], 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 Интернет-пользователи в развитых странах.

Техническая помощь

51. Вследствие транснационального характера киберпреступности борьба с этим явлением требует согласованных усилий всех стран. Одной из ключевых задач в этом деле является предотвращение создания "безопасных убежищ" для киберпреступников[69]. В этой связи одной из главных задач международного сообщества стало наращивание потенциала развивающихся стран, который позволит им бороться с киберпреступностью. Об этом говорится 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.

Сфера охвата исследования

52. Изучение данной темы будет предусматривать следующее:

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

---

[67] См. "Development Gateway's Special Report, Information Society – Next Steps?", 2005, на веб-сайте: http://topics.developmentgateway.org/special/informationsociety.

[68] "Spam Issue in Developing Countries", на веб-сайте: www.oecd.org/dataoecd/5/47/34935342.pdf.

[69] 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 Плане действий из 10 пунктов Группы восьми отмечено следующее: "Лица, преступно злоупотребляющие информационными технологиями, не должны иметь возможность укрываться где бы то ни было".

b) выявление наилучших видов практики в области оказания технической помощи в связи с киберпреступностью.

Тема 13. Частный сектор

Общая информация

53. Предупреждение и расследование киберпреступлений зависят от ряда различных факторов. 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. Однако участие его представителей в расследовании киберпреступлений сопряжено с рядом проблем.

Роль отраслевых предприятий

54. 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

55. Изучение данной темы будет предусматривать следующее:

a) перечень наилучших видов практики частного сектора в области предупреждения и расследования киберпреступлений;

b) анализ потребностей отраслевого сектора и правоохранительных органов;

c) оценка преимуществ и недостатков существующих подходов.