Организация Объединенных Наций E/CN.15/2001/4

Экономический и Социальный Совет

Distr.: General
30 March 2001

Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Десятая сессия
Вена, 8–17 мая 2001 года
Пункт 4 предварительной повестки дня*
Международное сотрудничество в борьбе с транснациональной преступностью

Выводы исследования по вопросу об эффективных мерах предотвращения высокотехнологичных и компьютерных преступлений и борьбы с ними

Доклад Генерального секретаря

Резюме

Настоящий доклад подготовлен во исполнение резолюции 1999/23 от 28 июля 1999 года, в которой Экономический и Социальный Совет просил Генерального секретаря провести исследование по вопросу об эффективных мерах, которые можно принять на национальном и международном уровнях в целях предотвращения компьютерных преступлений и борьбы с ними. В докладе приводятся предварительные результаты рассмотрения этого вопроса и содержится рекомендация о проведении более подробного исследования для представления в качестве первоочередного вопроса на рассмотрение Комиссии по предупреждению преступности и уголовному правосудию на ее одиннадцатой сессии. Кроме того, в нем содержится рекомендация о том, чтобы Комиссия на своей одиннадцатой сессии рассмотрела серию альтернативных вариантов в отношении будущей деятельности, включая возможную разработку международного документа против компьютерных преступлений, а также альтернативных вариантов краткосрочной стратегии, включая создание глобальной программы Организации Объединенных Наций против высокотехнологичной и компьютерной преступности. В докладе приводится также информация о деятельности других соответствующих международных и межправительственных организаций, а также предпринимается попытка ответить на вопросы, которые вызывают беспокойство у отдельных государств–членов.

* E/CN.15/2001/4.

V.01-82401 (R) 230401 070501

0182401

Содержание

I. Введение

1. Проблема преступной деятельности с использованием современных компьютеров, компьютерных сетей и телекоммуникационных технологий по-прежнему является одной из наиболее серьезных проблем, с которой сталкиваются система уголовного правосудия и правоохранительные органы государств–членов. Эту проблему можно рассматривать с точки зрения следующих характерных элементов:

a) Проблема носит глобальный характер. В прошлом большинство пользователей современных технологий и, следовательно, большинство правонарушителей и жертв находились в развитых странах. Расширение доступа к таким технологиям в развивающихся странах определялось в качестве одной из основных первоочередных задач, с тем чтобы обеспечить превращение глобального информационного общества в один из факторов, не препятствующих, а скорее способствующих развитию[1]. Развивающиеся страны окажутся в уязвимом положении по отношению к компьютерной и телекоммуникационной преступности и могут быть лишены доступа к компьютерным и коммуникационным сетям в результате применения правоохранительных технологий или технологий безопасности, если они не смогут принять участия в разработке и осуществлении программы борьбы с этим видом преступной деятельности.

b) Проблема носит динамичный характер. В результате быстрого развития новых технологий не менее быстрыми темпами появляются различные нововведения в сфере преступной деятельности, и глобальный характер таких технологий приводит к быстрому распространению новых методов преступной деятельности. Поэтому принципиально важное значение приобретает мониторинг разработки законных технологий и преступных нововведений в целях обеспечения актуальности внутренних и международных мер борьбы, в частности, в странах, обладающих лишь ограниченными техническими ресурсами. Этот процесс главным образом определяется развитием технологии и поэтому носит непрерывный характер.

c) Проблема имеет многодисциплинарный характер. В результате развития компьютерных технологий и телекоммуникационных сетей происходят существенные сдвиги в социально–экономической деятельности, которые все больше связаны не с физическими усилиями и товарами, а с чистой информацией и знаниями. Это будет иметь существенные последствия в таких областях, как права человека и устойчивое социально–экономическое развитие. Поэтому важно, чтобы мероприятия по борьбе с преступностью стали составным элементом программ в этих областях и наоборот. Информационные технологии и архитектура компьютерных и телекоммуникационных сетей в значительной степени являются также продуктом разработок в частном секторе, и поэтому при разработке мер по борьбе с высокотехнологичными и компьютерными преступлениями необходимо принимать во внимание такие факторы, как коммерческая рентабельность и экономическая конкурентоспособность соответствующих технологий.

II. История вопроса

A. Рассмотрение в других межправительственных или международных организациях

2. Подтверждением растущей озабоченности государств в связи с характером и масштабами данной проблемы и необходимостью принятия эффективных мер на глобальном уровне является ее обсуждение в рамках различных форумов.

1. Совет Европы

3. Совет Европы завершает разработку текста конвенции о кибернетической преступности[2], в котором рассматриваются уголовные преступления, связанные с проникновением в системы, получением несанкционированного доступа, электронным мошенничеством и подлогом, оскорбительным содержанием и нарушением прав интеллектуальной собственности. В этом проекте текста рассматривается вопрос о следственных полномочиях, включая отслеживание сообщений, а также поиск электронных доказательств, их выемка и сохранение. В нем будет дано также определение основных терминов и установлены стандарты в отношении взаимной правовой помощи и других форм международного

сотрудничества. В случае успешного завершения этот текст будет представлять собой первую попытку разработать всеобъемлющий международный документ о борьбе с компьютерными преступлениями. В отношении представленного проекта текста были высказаны противоречивые мнения. В целом правительства, эксперты и правоохранительные органы рассматривают его как позитивный шаг, хотя многие считают, что некоторые более сложные вопросы не были рассмотрены. Многие заинтересованные группы придерживаются позиции, согласно которой международные сети не подлежат регулированию, и выступили против этого документа, рассматривая его как попытку расширить полномочия национальных правоохранительных органов в ущерб праву на частную жизнь и другим интересам.

4. Переговоры по тексту этого документа проводились в рамках Комитета экспертов по преступности в кибернетическом пространстве, который был учрежден в феврале 1997 года после проведения серии исследований, посвященных этой проблеме[3]. Помимо членов Комитета для участия в его работе были приглашены эксперты из Канады, Соединенных Штатов Америки и Японии, и в ходе переговоров к этому процессу присоединились другие государства. Комитет подготовил 25 последовательных проектов текста в течение срока своих полномочий, которые истекли в декабре 2000 года. Окончательный текст был представлен на рассмотрение Парламентской ассамблеи Совета Европы. После этого он будет представлен Европейскому комитету по проблемам преступности для рассмотрения в июне 2001 года, и в случае одобрения этот документ будет передан на утверждение Комитету министров Совета Европы.

2. Группа восьми

5. После обсуждения проблем, возникающих в связи с транснациональной преступностью, на совещании на высшем уровне, проходившем в июне 1995 года в Галифаксе, Канада, семь ведущих промышленно развитых стран и Российская Федерация (Группа восьми) учредили Лионскую группу старших экспертов по транснациональной организованной преступности, в состав которой входила подгруппа экспертов по компьютерным преступлениям. Эта подгруппа проводила свои совещания на регулярной основе начиная с 1997 года и подготовила ряд инициатив. К числу основных проблем, которые были рассмотрены этой группой, относились проблемы, связанные с трансграничным электронным поиском, отслеживанием сообщений и необходимостью налаживания сотрудничества между правительствами и соответствующими заинтересованными группами в частном секторе.

6. В декабре 1997 года Группа восьми приняла план действий из 10 пунктов по кибернетической преступности, который предусматривал проведение обзора законодательства, принятие мер в целях обеспечения квалифицированного и надлежащим образом оснащенного персонала правоохранительных органов, рассмотрение вопросов, связанных с кибернетической преступностью, при подготовке соглашений о правовой помощи, рассмотрение методов сохранения электронных доказательств и их представления в рамках иностранного уголовного судопроизводства, развитие сотрудничества с промышленностью, а также установление судебных и других технических стандартов в отношении обеспечения компьютерной безопасности и использования электронных доказательств в ходе судебного разбирательства[4].

7. В 1999 году Группа восьми приняла ряд предварительных основных принципов в отношении действий правоохранительных органов, желающих получить доступ к электронным данным, хранящимся в иностранных государствах[5]. В целом было решено, что доступ к таким данным должен быть свободным, если они предназначены для публичного пользования, например, если речь идет об открытом web–сайте, или если получено согласие лица, обладающего законными полномочиями на получение доступа к данным и их разглашение. В связи с данными, которые не предназначены для публичного пользования, лица, осуществляющие поиск, сталкиваются с определенной дилеммой. Если им не удается быстро скопировать данные, то правонарушители, как правило, сразу же их уничтожат. Если же они копируют такие данные без предварительного получения разрешения того государства, в котором эти данные находятся, то возникают серьезные вопросы, связанные с суверенитетом этого государства и защитой прав лиц, имеющих интерес в данных, которые оказались объектом выемки. Принципы, согласованные Группой восьми, предусматривают направление запроса в отношении оказания на оперативной основе взаимной правовой помощи. Государству, в котором находятся данные, должна быть направлена

просьба принять незамедлительные меры для их сохранения до тех пор, пока не будет предоставлена более официальная помощь в целях обеспечения их выемки и передачи запрашивающему государству. После этого передача данных запрашивающему государству производится с применением более общепринятых процедур и гарантий в отношении оказания взаимной правовой помощи.

8. Кроме того, рассматриваются основные принципы отслеживания сообщений по компьютерным сетям. Большинство поставщиков услуг хранят электронные записи в отношении источника и получателя сообщений, например сообщений по электронной почте, однако делают это в течение ограниченного периода времени. В большинстве стран доступ к записям, которые могут быть использованы для отслеживания сообщений и установления личности соответствующих пользователей системы, можно получить только используя операции по поиску и выемке под судебным надзором. Это не является сколько–нибудь серьезным препятствием при отслеживании большинства внутренних сообщений, однако в транснациональном контексте задержки могут оказаться более продолжительными, в результате необходимости направлять запросы по каналам взаимной правовой помощи. Опытным правонарушителям известно о наличии такой проблемы, и они пытаются этим воспользоваться, направляя свои сообщения через многие различные страны, с тем чтобы усложнить путь от источника до получателя, или же направлять такие сообщения через страны, в которых отсутствуют законы или инфраструктура для проведения эффективного отслеживания, с тем чтобы скрыть истинное происхождение или место назначения своих сообщений.

9. Для содействия оперативному сотрудничеству между правоохранительными органами в транснациональном контексте Лионская группа рекомендовала создать в каждом государстве сеть органов по контактам, к которым можно обращаться в любое время суток на протяжении семи дней в неделю с просьбой об оказании помощи в проведении компетентного расследования. Первоначально в эту сеть входили государства – члены Группы восьми, однако в настоящее время она охватывает 19 стран и функции по обеспечению ее эксплуатации переданы Международной организации уголовной полиции (Интерпол).

10. В целях развития сотрудничества между правительствами и частным сектором Группа восьми провела ряд конференций по проблемам сотрудничества с промышленностью[6]. В целом представителями промышленности выступают представители компаний, которые разрабатывают компьютерное и телекоммуникационное оборудование, программное обеспечение и другие инфраструктурные элементы, а также компаний, которые предоставляют услуги индивидуальным пользователям. В ходе обсуждений рассматриваются вопросы, касающиеся готовности и способности компаний осуществлять сотрудничество с правоохранительными органами, а также необходимости мероприятий по предупреждению преступности на основе проведения надлежащей работы с клиентами и включения в новые разрабатываемые технологии соответствующих элементов для обеспечения безопасности.

3. Другие международные и межправительственные организации

11. Вопрос о высокотехнологичных и компьютерных преступлениях рассматривается также другими межправительственными и международными организациями либо в виде отдельного вопроса, либо в контексте других связанных с преступностью проблем, например отмывания денег и транснациональной организованной преступности. Содружество наций приступило к рассмотрению таких вопросов в 1998 году, включив соответствующую тему в повестку дня совещания министров юстиции стран Содружества в мае 1999 года. В результате этого совещания была учреждена рабочая группа экспертов по компьютерным преступлениям и преступлениям, совершаемым с использованием компьютеров, в целях разработки типового законодательства для стран Содружества, однако проведение работы по этому проекту было отложено до заключения Конвенции Совета Европы о кибернетических преступлениях. Работа возобновилась в июле 2000 года, и в настоящее время ведется подготовка проекта типового законодательства. Кроме того, Содружество наций обязалось обеспечить распространение среди государств–членов материалов по международным усилиям в этой области и провести обзор соответствующих систем Содружества для розыска правонарушителей и оказания взаимной правовой помощи, с тем чтобы обеспечить использование таких систем

для налаживания надлежащего сотрудничества в новой области высокотехнологичных преступлений.

12. Деятельность в этой области начинает проводить Интерпол, учредившая ряд региональных рабочих групп по проблемам преступности, связанной с информационной технологией. Проведенные Интерпол исследования и подготовленные ею материалы, как правило, отражают потребности и проблемы правоохранительных органов. Материалы, предназначенные для подготовки следователей, включают руководства по новым методам проведения расследований, а также более подробное учебное пособие по компьютерным преступлениям, в котором приводятся примеры наилучшей практики и соответствующие методы для более опытных следователей. Интерпол осознает также необходимость использования высокотехнологичных средств для распространения соответствующих данных среди правоохранительных органов и создает для этих целей web-сайт. Организация взяла на себя ответственность за регулярное обновление справочника по сети контактов, которая была первоначально создана Лионской группой. Интерпол планирует новые мероприятия, в частности в области подготовки сотрудников правоохранительных органов, а также будет следить за мероприятиями и участвовать в мероприятиях других международных организаций в целях обмена информацией и исключения дублирования усилий.

B. Мероприятия Организации Объединенных Наций

13. Проблема преступлений, совершаемых с использованием компьютеров и телекоммуникационных технологий, рассматривается в ходе различных мероприятий Организации Объединенных Наций и по-прежнему остается в центре внимания. В дополнение к настоящему исследованию, которое проведено во исполнение резолюции 1999/23 Экономического и Социального Совета от 28 июля 1999 года[7] для решения этой проблемы были приняты следующие меры:

a) в резолюции 45/109 Генеральной Ассамблеи от 14 декабря 1990 года и резолюции 1996/11 Экономического и Социального Совета от 23 июля 1996 года содержится настоятельный призыв к государствам–членам применять современные компьютерные технологии для более эффективного и действенного управления операциями в области уголовного правосудия и информационными системами. Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, проходивший в Гаване 27 августа – 7 сентября 1990 года, рекомендовал разработать международный документ по вопросам компьютеризации систем уголовного правосудия[8]. Этот вопрос рассматривался в ходе двухдневного семинара–практикума, который был организован в ходе девятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, проходившего в Каире 29 апреля – 8 мая 1995 года, и на котором было указано на необходимость компьютеризации в целях обеспечения готовности к борьбе с новыми формами преступности и в то же время было выражено беспокойство в связи с возможными проблемами в области права на частную жизнь, прав человека и совместимости систем внутри стран и между отдельными странами. В ходе семинара–практикума было указано также на необходимость оказания технической помощи в форме выделения финансовых ресурсов и обеспечения услуг технических экспертов[9]. В целом основное внимание уделялось применению компьютеров в процессе управления уголовным правосудием и сбора статистической информации, а не использованию компьютерных сетей в качестве инструмента в проведении расследований и оперативных мероприятий. Недавно положения, предусматривающие расширение использования современных технологий в рамках деятельности по борьбе с преступностью, были включены в Конвенцию Организации Объединенных Наций против транснациональной организованной преступности[10], а электронная система распространения документации сыграла важную роль в процессе ведения переговоров;

b) восьмой Конгресс рассмотрел также собственно проблему преступлений, совершаемых с применением компьютеров[11], и рекомендовал принять серию следующих мер:

i) модернизация положений внутреннего законодательства о составах преступлений, процедурах расследования, правилах доказывания, конфискации или реституции, взаимной правовой помощи и выдачи в целях

распространения их действия на преступления, совершаемые с использованием компьютеров;

ii) повышение компьютерной безопасности и совершенствование других технических мер в целях предупреждения преступности;

iii) повышение информированности населения и подготовка должностных лиц по вопросам расследования, уголовного преследования и рассмотрения в судах дел о преступлениях, связанных с применением компьютеров;

iv) разработка и распространение этических норм в отношении использования компьютерных систем;

v) разработка политики в отношении жертв преступлений, связанных с применением компьютеров, включая меры, направленные на поощрение к сообщению о таких преступлениях;

c) в соответствии с рекомендацией восьмого Конгресса, содержащейся в его резолюции 9, в 1994 году в качестве пособия для следователей и работников директивных органов было обеспечено издание и широкое распространение через Интернет *Руководства Организации Объединенных Наций по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними*[12];

d) вопрос о преступлениях, связанных с компьютерами, был включен также в повестку дня десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, который проходил в Вене 10–17 апреля 2000 года. В ходе десятого Конгресса Азиатским и дальневосточным институтом Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями был организован семинар–практикум по этому вопросу продолжительностью в один день[13]. В ходе семинара–практикума были проведены обсуждения в четырех группах по следующим темам: криминологические аспекты компьютерных преступлений; проблемы, связанные с поиском и изъятием данных из компьютерных сетей; проблемы, связанные с прослеживанием сообщений в рамках компьютерных сетей; а также взаимосвязи правоохранительной деятельности с компьютерной индустрией и Интернет. Ведущие эксперты в этой области представили участникам информацию по текущим вопросам и результатам обсуждений в рамках Совета Европы, Группы восьми и других форумов. Помимо представителей участвующих государств в работе семинара–практикума принимали также участие ряд представителей промышленности. Участники семинара–практикума сформулировали ряд рекомендаций, в том числе обратились с призывом расширить сотрудничество между правительствами и деловыми кругами, улучшить международное сотрудничество в целях отслеживания преступников и предпринять в рамках Организации Объединенных Наций дальнейшие действия по техническому сотрудничеству и оказанию технической помощи[14];

e) в Венской декларации о преступности и правосудии: ответы на вызовы XXI века, которая была принята десятым Конгрессом[15] и одобрена Генеральной Ассамблеей в ее резолюции 55/59 от 4 декабря 2000 года, также рассматривается вопрос о преступлениях, связанных с использованием высоких технологий и компьютеров. В пункте 18 Венской декларации государства–члены постановили разработать ориентированные на конкретные действия программные рекомендации в отношении предупреждения преступлений, связанных с использованием компьютеров и борьбы с ними, и обязались работать в направлении укрепления своих возможностей по предупреждению, расследованию и преследованию таких преступлений. Комиссии по предупреждению преступности и уголовному правосудию было предложено приступить к разработке таких программных рекомендаций, принимая во внимание работу, которая ведется в других форумах. Генеральная Ассамблея в своей резолюции 55/60 от 4 декабря 2000 года просила Комиссию продолжить рассмотрение заключений и рекомендаций, изложенных в Венской декларации, и доклада десятого Конгресса, а также просила Генерального секретаря подготовить в консультации с государствами–членами проекты планов действий для рассмотрения Комиссией на ее десятой сессии;

f) помимо участия в подготовке семинара–практикума, который был проведен в ходе десятого Конгресса и который был посвящен преступлениям, связанным с компьютерными сетями, Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями провел серию совещаний и семинаров–практикумов для выявления вопросов и определения повестки дня для

последующей деятельности. Был проведен, в частности, обзор положения в государствах–членах по вопросам, касающимся компьютерных преступлений, результаты которого будут вскоре опубликованы. Кроме того, в настоящее время Институт занимается обобщением и изданием материалов, которые были использованы Организацией Объединенных Наций и отдельными участниками в ходе семинара–практикума, организованного в рамках десятого Конгресса. В планах на будущее основное внимание уделяется разработке и распространению практической информации по вопросам расследования и уголовного преследования в связи с компьютерными преступлениями;

g) на своей десятой сессии Комиссия рассмотрит доклад Генерального секретаря о проектах планов действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века (E/CN.15/2001/5). В докладе Генерального секретаря рассматриваются также высокотехнологичные и компьютерные преступления и содержится серия программных рекомендаций и конкретных мер, которые могут быть приняты в целях укрепления потенциала на национальном и международном уровнях в области предупреждения, расследования и уголовного преследования таких преступлений. Эти рекомендации и меры основаны на материалах, которые рассматриваются в настоящем докладе;

h) Генеральная Ассамблея в своей резолюции 55/63 от 4 декабря 2000 года отметила значение усилий по борьбе с преступным использованием информационных технологий. Такие усилия должны предусматривать следующие меры: ликвидация убежищ для правонарушителей; сотрудничество правоохранительных органов в расследовании трансграничных преступлений; обмен информацией; обучение и оснащение персонала; защита конфиденциальности; обеспечение сохранности данных, имеющих отношение к расследованию преступлений, и быстрого доступа к ним; обеспечение надлежащих режимов взаимной правовой помощи; повышение осведомленности общественности; разработка информационных систем для предупреждения преступлений и содействия их расследованию; а также учет необходимости защиты личных свобод и частной жизни при сохранении у правительств возможности бороться с преступным использованием информационных технологий. Генеральная Ассамблея постановила также включить вопрос о преступном использовании информационных технологий в повестку дня своей пятьдесят шестой сессии;

i) в своей резолюции 55/25 от 15 ноября 2000 года Генеральная Ассамблея приняла Конвенцию Организации Объединенных Наций против транснациональной организованной преступности и два Протокола к ней (резолюция 55/25, приложения I–III). Конвенция не применяется в тех случаях, когда преступления не носят серьезного характера, когда в их совершении не участвует организованная преступная группа и когда соответствующие преступления не носят транснационального характера[16], что исключает некоторые категории электронных преступлений. Тем не менее Конвенция применяется в тех случаях, когда компьютер или телекоммуникационные сети используются преступниками в рамках более традиционных форм транснациональной организованной преступности. В пункте 1(h) статьи 29 содержится конкретный призыв в отношении разработки внутренних мер и программ технической помощи для борьбы с транснациональными организованными преступлениями, совершаемыми с использованием компьютеров, телекоммуникационных сетей и других видов современной технологии;

j) после принятия Конвенции был проведен еще один семинар–практикум по теме "Угроза трансграничной кибернетической преступности" в рамках Симпозиума по вопросу о правопорядке в мировой деревне – вопросы суверенитета и универсальности, который был организован в рамках Политической конференции высокого уровня для подписания Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Протоколов к ней, проходившей в Палермо, Италия, 12–15 декабря 2000 года. В ходе семинара–практикума были рассмотрены темы, касающиеся компьютерных преступлений и других форм транснациональной преступности, в отношении которых меры борьбы, предусмотренные исключительно во внутреннем законодательстве, все чаще рассматриваются как недостаточные. Было указано, что такая преступность расширяется по мере распространения технологий, которые используются при совершении соответствующих преступлений, и поскольку становится легче совершать трансграничные преступления. Было высказано мнение о том, что важными элементами решения данной проблемы является принятие

законодательства на национальном уровне, а также всеобъемлющего международного документа. Однако в то же время было выражено беспокойство в отношении опасности преждевременной разработки соответствующих нормативных документов. Эта проблема может быть также частично решена за счет принятия профилактических мер, например, на основе обеспечения технической безопасности, просветительской деятельности и разработки этических норм в отношении использования новых технологий. В ходе семинара–практикума было также высказано мнение о том, что различного рода кибернетические преступления можно разделить на следующие основные категории: несанкционированный доступ к компьютерам или компьютерным системам; разрушение или изменение данных; вмешательство в процессы законного использования компьютеров и компьютерных систем; хищение нематериальной собственности и получение материальной выгоды обманным путем.

C. Характер компьютерных и высокотехнологичных преступлений: предварительная типология

14. Высокотехнологичные и компьютерные преступления требуют определения новых и модификации существующих составов преступлений, с тем чтобы они охватывали неправомерное использование новых технологий. Необходимо проанализировать новые формы деликтного поведения, с тем чтобы определить целесообразность применения в качестве ответной меры норм уголовного права, а также целесообразность квалификации такого поведения в качестве преступлений. В отношении существенных элементов наиболее серьезных и причиняющих наибольший вред видов поведения в настоящее время формируется определенный международный консенсус, однако по-прежнему существует ряд областей, которые рассматриваются в качестве преступлений не всеми, а лишь некоторыми государствами. Два наиболее показательных примера касаются таких проблем, связанных с правами интеллектуальной собственности, как несанкционированное копирование программного обеспечения или данных, а также проблемы так называемого непристойного содержания.

15. Использование новых технологий в преступных целях привело к возникновению абсолютно новых форм преступности. С другой стороны, более традиционные преступления в настоящее время совершаются новыми методами, которые позволяют увеличить выгоды или снизить риски для преступников. Третья основная категория преступной деятельности связана с более общим использованием технологий преступниками в организационных целях, для поддержания связей и для того, чтобы скрыть свою деятельность от наблюдения. Другие основные области предлагаемой классификации касаются классификации по признаку того, совершены ли преступления с целью получения преступниками экономической или материальной выгоды или же по другим мотивам, и представляют ли они собой преступление, совершенное против компьютерных или коммуникационных систем, или же использование этих технологий для причинения ущерба другим лицам.

16. Ниже рассматриваются основные виды высокотехнологичных и компьютерных преступлений.

1. Преступления, совершаемые против технологий и их пользователей.

a) Получение несанкционированного доступа к компьютерам или компьютерным системам

17. В большинстве случаев получение несанкционированного доступа к компьютерам или компьютерным системам рассматривается в качестве преступления, поскольку это может означать вмешательство в частную жизнь законных пользователей, к данным которых можно получить доступ, и поскольку несанкционированный доступ часто сопровождается другими правонарушениями или же препятствует законному использованию данной системы.

b) Несанкционированное использование компьютерных систем

18. Несанкционированное использование компьютерных систем частично совпадает с несанкционированным доступом, поскольку для получения такого доступа необходимо использовать системы. Тем не менее после получения доступа система используется также для совершения других правонарушений или для сокрытия истинной личности правонарушителя. Несанкционированное использование, как правило, квалифицируется в качестве

преступления на том основании, что использование компьютерного времени или оборудования является ценным ресурсом, за который правонарушители не платят, и доступа к которому в некоторых случаях не могут получить законные пользователи, оплачивающие такие ресурсы.

c) Считка, копирование и использование данных без разрешения

19. Как и в случае обычной кражи, вред от считывания, копирования или использования данных без получения разрешения состоит в утрате жертвой определенной ценности и в неправомерном приобретении определенной ценности правонарушителем. Тем не менее в случае данных эти аспекты проявляются раздельно, поскольку данные могут быть скопированы без изъятия. Такое деяние также может быть признано уголовно наказуемым как форма вмешательства в частную жизнь

d) Создание и распространение "враждебных" программ

20. Компьютерные вирусы, черви и другие программы нарушают работу компьютерных систем в результате снижения производительности компьютера и сокращения его памяти. В большинстве случаев они также распространяются самостоятельно в результате использования электронной почты или при передаче зараженных дискет, и, таким образом, правонарушители быстро утрачивают контроль за масштабами причиняемого ущерба сразу же после того, как только начинается распространение данной программы. Многие "враждебные" программы причиняют также фактический ущерб данным в результате стирания или искажения файлов. Ущерб, который может оказаться весьма существенным, как правило, состоит в прекращении функционирования системы, утрате ценных данных и дополнительных расходах на устранение программ и восстановление функций системы.

e) Компьютерный вандализм или саботаж

21. Ущерб может быть причинен непосредственно правонарушителями, которые получают несанкционированный доступ либо умышленно, либо неумышленно, когда они пытаются использовать систему или скрыть факт получения доступа. Такие правонарушения в некоторых случаях совершаются также лицами, которые обладают санкционированным доступом к соответствующей системе. К этой категории правонарушений относятся вторжения с целью вынудить систему отказывать в обслуживании, когда правонарушители получают несанкционированный доступ к большому количеству компьютеров, объединенных в единую сеть, и используют их для массированного направления в целевую систему произвольных данных, что приводит к перегрузке целевой системы и ее отключению. Такие действия могут представлять собой простой акт вандализма или же использоваться в качестве отвлекающего маневра для сокрытия других правонарушений в результате выведения из строя технических средств обеспечения безопасности. "Враждебные" программы, например вирусы, также могут использоваться для конкретных актов вандализма или саботажа, однако они отличаются от целенаправленных действий правонарушителей, поскольку по мере распространения они, как правило, оказывают беспорядочное воздействие.

2. Традиционные преступления, совершаемые с использованием компьютерных или коммуникационных технологий

a) Правонарушения, связанные с материалами оскорбительного содержания

22. Правонарушения, связанные с материалами оскорбительного содержания, состоят в использовании компьютерных систем для создания или распространения изображений, текстов или другой информации, за которые предусмотрено уголовное наказание. Между различными государствами существуют расхождения в отношении категории содержания материалов, распространение которых является уголовно наказуемым. Большинство государств в настоящее время признают уголовно наказуемым создание или распространение детской порнографии, однако в отношении материалов, которые рассматриваются в качестве непристойных, порнографических или богохульных, или же пропагандирующих ненависть, единого подхода не существует. Защита конституционных принципов прав человека, включая свободу выражения или свободу слова, ограничивает во многих государствах возможности криминализации некоторых категорий содержания.

b) Похищение с использованием Интернет

23. В настоящее время педофилы начинают использовать Интернет для получения доступа к детям, не раскрывая при этом своего истинного имени. Диалоги начинаются в электронных "кулуарах", и как только достигается атмосфера доверия, правонарушитель договаривается о личной встрече и похищает жертву. Сотрудникам правоохранительных органов, которые выступали в роли детей в Интернет, удалось арестовать ряд правонарушителей. В некоторых случаях правонарушители побуждали жертв стирать файлы с записью их переговоров, с тем чтобы уничтожить доказательства, связанные с похищением.

c) Мошенничество

24. К категории мошенничества относится большая часть преступлений, которые связаны с перенаправлением средств электронным способом или предоставлением пользователям технологий ложной информации, с тем чтобы лишить их средств или каких-либо активов. Такие преступления могут совершаться "инсайдерами", например собственными служащими, или же посторонними лицами, которые используют несанкционированный доступ к частным сетям или размещают ложную информацию в публичных системах. Ожидается, что по мере расширения электронной торговли будет возрастать число случаев мошенничества или других экономических преступлений. Все более серьезной проблемой в этой области является использование различных технических средств для осуществления манипуляций на финансовых рынках.

d) Коммерческий или промышленный шпионаж

25. Расширение использования компаниями компьютерных систем для создания и передачи информации приводит также к тому, что они все чаще становятся объектом промышленного шпионажа. Такой шпионаж может осуществляться в результате получения несанкционированного доступа извне или же собственными сотрудниками, которые используют соответствующие технологии для обобщения ценной информации и ее незаметного направления конкурентам.

e) Преступления, связанные с правами интеллектуальной собственности

26. Способность новых технологий обеспечивать хранение, передачу и копирование информации порождает серьезные проблемы, связанные с несанкционированным копированием. Тем не менее не все государства рассматривают такие действия как уголовно наказуемые деяния. В некоторых государствах эти проблемы относятся к сфере гражданско–правовых вопросов, подлежащих урегулированию непосредственно заинтересованными сторонами.

f) Игорный бизнес

27. Развитие инфраструктуры для поддержки мелкой электронной торговли создает также возможности для организации игорного бизнеса через Интернет. Если web–сайт в какой-либо стране, где азартные игры не запрещены, используются игроками в странах, где такие действия составляют преступления, возникает уголовно–правовая проблема. Игорный бизнес, как правило, регулируется не только из соображений морального характера, но и для мобилизации налоговых поступлений, а также обеспечения контроля в целях предупреждения организованной преступности и защиты игроков от нечестной игры. В последнее время игорный бизнес через Интернет рассматривается также как один из возможных методов осуществления операции по отмыванию денег.

g) Отмывание денег

28. Постоянное расширение электронной торговли и других видов коммерческой деятельности с использованием компьютерных сетей будет создавать, как ожидается, различные возможности для отмывания денег. Компьютерные технологии, как правило, позволяют преступникам скрывать свою истинную личность и местонахождение, манипулировать различиями в правовых системах, используя иностранные счета или параллельную юрисдикцию, а также скрывать истинный характер своих сделок, применяя такие технические средства, как шифрование. В некоторых случаях такие действия могут сопровождаться также другими преступлениями, например участием в азартных играх или мошенничеством[17].

3. Использование компьютерных технологий для поддержки другой преступной деятельности

29. В целом современные компьютерные и телекоммуникационные сети, а также другие подобные технологии обеспечивают преступным организациям такие же преимущества, как и законным коммерческим пользователям. К числу преимуществ относятся быстрые, надежные и недорогостоящие глобальные системы связи, которые в большинстве случаев являются более безопасными с точки зрения внешнего перехвата или наблюдения, чем традиционные методы. Характер таких систем, а также более высокие скорости и большие объемы передаваемых данных неизбежно затрудняет деятельность правоохранительных органов по перехвату отдельных сообщений. Специальные системы защиты, например системы защиты доступа и программы шифрования, позволяют преступникам защитить свои сообщения от перехвата или раскрытия содержания так же эффективно, как они защищают законные системы связи. В некоторых случаях сетевые технологии могут также использоваться абсолютно новыми видами преступных организаций. В качестве примера в связи с этим наиболее часто упоми-наются педофилы, которые устанавливают связи друг с другом и обмениваются детской порно-графией, сохраняя при этом анонимность, и которые могут взаимодействовать различными методами, ко-торые не охватываются существующими концеп-циями или определениями организованной преступ-ности. Традиционные преступные организации так-же могут изыскивать новые возможности для выявления преступников в других регионах или странах и организации с ними сотрудничества.

D. Оценка масштабов компьютерной и высокотехнологичной преступности и причиняемого ею ущерба

30. В результате расширения масштабов и усложнения компьютерных и телекоммуникационных сетей быстро возрастает число людей, которые их используют, а также степень зависимости от таких систем. В своем докладе Ассамблее тысячелетия Генеральный секретарь отметил, что с момента появления Интернет в начале 90-х годов число пользователей этой сети достигло к 1998 году 143 млн. человек и что к 2001 году, как ожидается, количество пользователей достигнет 700 миллионов. Объем электронной торговли, которая появилась несколько позже, достиг в 1996 году 2,6 млрд. долл. США, и предполагается, что к 2002 году он возрастет до 300 млрд. долларов США[18]. Статистические данные, касающиеся высокотехнологичной и компьютерной преступности, являются весьма ограниченными, однако периодически появляющиеся сообщения и имеющиеся статистические данные свидетельствуют о том, что масштабы такой преступности возрастают по мере роста числа потенциальных правонарушителей и жертв, использующих компьютерные сети[19]. По-видимому, происходит также расширение круга преступной деятельности, поскольку новые технологии создают новые возможности для преступной деятельности и преступники находят новые пути их использования. Особое беспокойство в настоящее время вызывает быстрое расширение электронной торговли и соответствующей вспомогательной инфраструктуры, что, по-видимому, будет сопровождаться впоследствии ростом компьютерной экономической преступности, включая мошенничество, манипулирование финансовыми рынками и отмывание денег.

31. По мере повышения степени зависимости от компьютерных сетей возрастает также потенциальный ущерб от уголовных преступлений. Большинство промышленно развитых стран, где отмечается наиболее высокая степень такой зависимости, в настоящее время рассматривает компьютерные и телекоммуникационные сети и соответствующую вспомогательную инфраструктуру в качестве потенциального объекта для террористических актов. Нападения на компьютерные системы в стратегических или политических целях по-прежнему отмечаются редко, однако преступные деяния, основанные на других мотивах, регулярно наносят значительный ущерб, который в некоторых случаях во много раз превышает тот ущерб, который фактически предполагали нанести преступники. Одним из недавних примеров является создание и распространение в марте 1999 года вируса "Melissa", прямой ущерб от которого только в Соединенных Штатах Америки превысил 10 млн. долл. США, а также появление в мае 2000 года вируса "I love you", ущерб от которого, по имеющимся оценкам, составил от 7 до 10 млрд. долл. США и которым было заражено около 45 млн. компьютеров во всем мире. Еще одним примером

является серия нападений, вынуждающих системы отказывать в обслуживании, в ходе которых web–сайты бомбардируются крупными объемами бессмысленных данных и в результате которых менее чем за два часа закрываются 1 200 сайтов, включая сайты новых организаций и сайты электронной торговли. Ущерб в результате некоторых таких действий, в частности, связанных с распространением вирусов, в большинстве случаев усугубляется тем, что другие преступники копируют вирусы, вносят изменения, с тем чтобы скрыть их характер от пользователей или фильтрующих программ, а затем осуществляют его повторное распространение[20].

32. Довольно трудно дать количественную оценку фактического ущерба, однако такой ущерб включает прямые затраты на ремонт системы программного обеспечения, утрату доступа или услуг пользователями и причиняемый вследствие этого ущерб, утрату ценных данных и потерю доходов от эксплуатации сайтов. Рост такой преступности требует также разработки и внедрения систем безопасности и принятия других превентивных мер, что приводит к увеличению общих затрат. Совокупное увеличение масштабов такой преступности и особый характер некоторых преступлений способствуют также возникновению существенного, однако непредсказуемого политического давления в целях укрепления уголовно–правовых мер для сдерживания такой преступности, назначения более строгих наказаний и принятия технических мер предосторожности производителями программного обеспечения и компьютерного оборудования, а также компаниями, которые предоставляют доступ к сетям для клиентов. Еще одним скрытым стоимостным фактором таких происшествий является страх перед кибернетической преступностью, который может препятствовать расширению использования компьютерных технологий или заставлять правительства и население в развивающихся странах воздерживаться от максимально эффективного применения таких технологий.

33. Проведение обоснованного анализа характера и масштабов самих преступлений также сопряжено с определенными трудностями. По-прежнему нерешенными остаются вопросы, касающиеся целесообразности криминализации тех или иных видов поведения, а также методов их определения и классификации, если такая криминализация будет сочтена целесообразной. Любая система классификации зависит также в определенной степени от соответствующих технологий, и в связи с этим также возникает проблема определений. Такие технологии, как компьютерные сети, кабельные системы вещания и системы мобильной и обычной телефонной связи, становится все труднее разграничить по мере расширения использования компьютерных сетей и внедрения цифровых технологий в рамках более традиционных систем. Одним из последних примеров является так называемое устройство palm–pilot, в котором объединены различные аспекты мобильной телефонной связи, сетевого вещания и доступа к компьютерным сетям. Эта проблема в ближайшем будущем будет вызывать повышенное беспокойство исследователей, политических аналитиков и законодателей, а также послужила основанием для призывов использовать нейтральные с технической точки зрения концепции и формулировки, с тем чтобы избежать пробелов и несоответствий.

34. Серьезные проблемы возникают также в процессе сбора точных статистических данных даже в тех случаях, когда удается четко выявить соответствующие преступления. Большинство экспертов считает, что данные об обычных компьютерных преступлениях являются существенно заниженными, поскольку жертвы могут не подозревать, что они стали жертвами, могут не осознавать, что соответствующее деяние является преступлением или же могут воздерживаться от подачи жалоб, испытывая смущение или опасаясь подорвать доверие к своей компании. Дополнительные проблемы возникают в связи с массовой виктимизацией в результате таких преступлений, как распространение вирусов, поскольку число жертв оказывается попросту чрезмерно большим для выявления и подсчета и поскольку в результате использования таких программ могут появляться новые жертвы спустя много времени после того, как преступники были пойманы и понесли наказание. Еще один фактор, усложняющий сбор и сопоставление национальных статистических данных о преступности, связан с тем, что транснациональные компьютерные преступления, по определению, совершаются или имеют последствия по меньшей мере в двух государствах, в некоторых случаях во многих государствах, в результате чего возникает опасность получения повторных сообщений или неполучение вообще никаких сообщений.

III. Выводы и рекомендации: разработка глобальной политики по предупреждению компьютерной и высокотехнологичной преступности и борьбе с ней

A. Необходимость рассмотрения высокотехнологичной и компьютерной преступности в качестве отдельного вопроса

35. Преступные деяния, которые рассматриваются в настоящем докладе, непосредственно связаны с используемыми технологиями и имеют много общих характерных черт. Некоторые из них являются новыми видами деятельности, порожденными и определяемыми самими технологиями, в то время как другие являются более традиционными видами преступности, на которые такие технологии оказали существенное влияние. Многие основополагающие политические вопросы, например, обеспечение соответствующего баланса между правами человека и полномочиями следственных органов, а также между внутренними и международными интересами, характерны для всех форм высокотехнологичной и компьютерной преступности. Проблемы, возникающие на более практическом уровне в процессе расследования и судебного преследования, например, определение местонахождения и идентификация преступников, а также выемка, сохранение, аутентификация и использование компьютерных или электронных доказательств в суде, по существу аналогичны независимо от характера конкретных преступлений. Поэтому рекомендуется рассматривать эту область в качестве отдельной темы для исследовательских целей и любых будущих многосторонних обсуждений. Тем не менее следует также отметить, что многие вновь возникающие проблемы, например распространение детской порнографии, мошенничество и другие финансовые преступления, потребуют также привлечения квалифицированных экспертов, которые хорошо знают соответствующую категорию преступников и конкретные методы их деятельности.

B. Необходимость оказания помощи развивающимся странам

36. До последнего времени обсуждения на политическом уровне, касающиеся компьютерных систем и компьютерной преступности, в значительной степени проводились в странах и с участием стран с хорошо развитым сектором высоких технологий. В этих странах существуют заинтересованные стороны, которым может быть нанесен ущерб в результате компьютерных преступлений. В таких странах осуществляются значительные инвестиции в компьютерные технологии как в государственном, так и в частном секторе, и все более значительная часть населения прибегает к использованию компьютерных сетей. Тем не менее не следует забывать также об интересах развивающихся стран. Новые технологии открывают существенные возможности для удовлетворения социальных, экономических и других потребностей в развивающихся странах[21], однако они могут также стать причиной углубления существующего неравенства, если эти страны не смогут в полной мере воспользоваться такими возможностями. В связи с этим компьютерная преступность, а также усилия развитых стран и индустрии высоких технологий по борьбе с такой преступностью могут стать препятствием на пути развития, если развивающиеся страны не смогут принять активного участия в обсуждениях. Их участие необходимо для выявления и определения в полном объеме их интересов, для оценки потребностей в технической и другой помощи на различных этапах этого процесса, для разработки мер по предупреждению преступности и борьбе с ней, которые будут эффективны во всех обществах, а также для обеспечения осуществления таких мер в полном объеме и на эффективной основе.

37. Необходимо будет обеспечить практически универсальное осуществление эффективных мер по борьбе с преступностью, поскольку новые технологии могут использоваться преступниками, минуя практически все ограничения, с которыми сталкиваются традиционные преступники вследствие наличия национальных границ. Если деятельность традиционных преступников ограничивается такими факторами, как географические расстояния, таможенный контроль и необходимость получения физического доступа к жертвам, электронные преступники могут действовать на расстоянии, причем

действовать безнаказанно, в рамках любой правовой системы, в которой отсутствует соответствующее законодательство или же желание или способность обеспечивать соблюдение такого законодательства. Широкое представительство и эффективное участие будут иметь принципиально важное значение для обеспечения жизнеспособности разработанных программ и мер во всех странах, а также для обеспечения во всех странах воли и потенциала для их эффективного осуществления.

38. Для обеспечения эффективного участия потребуется помощь развитых стран на различных этапах процесса. На первоначальном этапе потребуется также информация от развивающихся стран для оценки их заинтересованности в новых технологиях и определения того, каким образом компьютерные преступления и усилия по борьбе с ними могут повлиять на такие интересы. Поэтому помощь на первоначальных этапах приобретает особое значение. Ряд стран уже некоторое время активно занимаются соответствующими вопросами, однако многие по-прежнему еще не осведомлены о новых технологиях, и технические, правовые и политические вопросы, которые будут возникать, не подвергались серьезному обсуждению. Даже если соответствующая помощь будет обеспечена, накопление соответствующих знаний и опыта потребует определенного времени. Поэтому важно как можно быстрее приступить к оказанию такой помощи и предоставлять ее в течение достаточно длительного периода времени, с тем чтобы обеспечить активное участие на протяжении всего процесса обсуждений. В более долгосрочной перспективе потребуется также непрерывная техническая помощь для обеспечения оперативной эффективности. Тот факт, что технологии и преступления, при совершении которых они используются, постоянно изменяются, потребует глобальных усилий для мониторинга нововведений, разработки эффективных ответных мер и достаточно оперативного их распространения, с тем чтобы правоохранительные и судебные органы не отставали и даже опережали преступников.

39. Поэтому рекомендуется незамедлительно предпринять усилия для оценки потребностей в технической помощи тех развивающихся стран, которые запрашивают такую помощь, и как можно быстрее удовлетворить такие потребности. Такую оценку следует проводить с учетом стратегий развития электроники в таких странах и расширения использования во всем мире технологий компьютерных и телекоммуникационных систем, а также мероприятий по предупреждению преступности. Оценку следует также проводить в консультации с компаниями частного сектора, занимающимися такими технологиями, и, по возможности, при содействии таких компаний. Важными элементами оценки в глобальном контексте должны стать выявление критических технологий и установление приоритетов.

C. Необходимость рассмотрения мер на международном и национальном уровнях, а также в рамках частного сектора

40. Эксперты во всем мире признают, что международный характер современных компьютерных и телекоммуникационных технологий приводит к появлению новых форм транснациональной и многонациональной преступности. Концепция кибернетического пространства и то, насколько легко преступные деяния в одном географическом регионе могут иметь последствия в других регионах, настоятельно требует согласования национальных и международных мер. Без такого согласования ответные меры могут оказаться неэффективными в борьбе с преступностью и могут вопреки ожиданиям иметь отрицательные последствия, например вынуждать население воздерживаться от использования новых технологий, наносить ущерб правам человека и создавать разрыв в промышленной конкурентоспособности и развитии.

41. Особая роль промышленности в разработке и эксплуатации технологий требует также согласования мер, принимаемых на государственном уровне и в рамках частного сектора. Компании частного сектора, как правило, поддерживают эффективные меры по борьбе с преступностью, однако их мотивы, которые, как правило, носят коммерческий, а не политический характер, и методы их деятельности, которые имеют скорее технический, а не правовой характер, должны быть учтены и по возможности согласованы с усилиями правительств на внутригосударственном и международном уровнях.

D. Роль Организации Объединенных Наций

42. В рамках подготовки к Ассамблее тысячелетия Организации Объединенных Наций Экономическому и Социальному Совету было предложено рассмотреть роль информационной технологии в области развития и международного сотрудничества. Совет пришел к выводу о том, что разработка и распространение новых видов информационной технологии в значительной степени является изолированным процессом, однако Организация Объединенных Наций может принять весьма действенные меры для поддержки этого процесса[22]. Такие меры включают оказание содействия развивающимся странам в освоении новых технологий, в частности в тех регионах или в тех областях, в которых изменения, происходящие под воздействием рыночных факторов, вероятно, не будут содействовать удовлетворению их потребностей, а также оказание содействия в разработке конкретных технологий, которые могут принести социальные выгоды, однако отнюдь не обязательно являются коммерчески рентабельными. В более общем плане был сделан вывод о том, что ключевая роль Организации Объединенных Наций состоит в содействии достижению консенсуса и налаживании партнерских отношений между заинтересованными сторонами данного процесса, включая правительства, научные учреждения и компании частного сектора. Цель усилий по достижению консенсуса заключается в мобилизации необходимого экспертного потенциала и ресурсов, с тем чтобы обеспечить для всех доступ к новым информационным технологиям и возможность получать выгоды от их применения.

43. Высокотехнологичная и компьютерная преступность представляет собой существенное препятствие в процессе обеспечения доступа к тому, что, по выражению Совета, является основанной на знаниях глобальной экономикой, и для получения соответствующих выгод, и поэтому столь же важное значение будет иметь достижение консенсуса в области борьбы с преступностью. Необходимость принятия эффективных мер по борьбе с преступностью в настоящее время повсеместно признается в государствах, которые осуществляют крупные инвестиции в такие технологии и в значительной степени зависят от этих технологий, однако это лишь начало длительного процесса. Для разработки конкретных мер потребуется провести оценку и согласование многих экономических, социальных, культурных и правовых вопросов. Разработка и осуществление многочисленных мер в области борьбы с преступностью должны подкрепляться практически универсальным консенсусом и обеспечением соответствующего уровня технических возможностей практически в каждой стране, с тем чтобы добиться эффективности таких мер. Консенсус должен существовать не только среди стран и их правительств, но также и на более широкой основе, охватывая также многонациональные корпорации в частном секторе.

44. В ближайшем будущем важно обеспечить сбор и распространение точной информации о характере и масштабах проблемы, а также мнений государств–членов о том, что следует предпринять для ее решения, с тем чтобы государства смогли рассмотреть соответствующие мнения и дать Организации Объединенных Наций руководящие указания в отношении методов ее деятельности. Межправительственные организации, деятельность которых рассматривалась в настоящем докладе, а также некоторые отдельные правительства уже приступили к процессу обмена опытом в области разработки законодательства, судебного преследования, технических вопросов и правоохранительной деятельности с другими государствами как в целом, так и в контексте отдельных дел, касающихся крупных транснациональных преступлений. Этот процесс следует расширить как с точки зрения его масштабов, так и числа участвующих стран, однако для достижения этого необходимо провести точную оценку существующих потребностей и имеющихся ресурсов для удовлетворения таких потребностей.

45. Поэтому рекомендуется поручить Центру по международному предупреждению преступности Управления по борьбе с наркотиками и предупреждению преступности Секретариата провести более подробные исследования в связи с этой проблемой для представления Комиссии по предупреждению преступности и уголовному правосудию на ее одиннадцатой сессии. Возможная тема такого исследования будет более подробно рассмотрена ниже, однако оно должно охватывать по меньшей мере обзор основных потребностей государств–членов, оценку их готовности оказать содействие путем выделения финансовых ресурсов и предоставления услуг технических экспертов, а также их мнений в отношении методов разработки глобальных

мер по решению данной проблемы и надлежащей формы таких ответных мер.

46. Кроме того, рекомендуется учредить межправительственную группу экспертов открытого состава для рассмотрения этого исследования и разработки вариантов и рекомендаций в отношении дальнейшего рассмотрения и принятия соответствующих решений Комиссией на ее одиннадцатой сессии. Как отмечалось выше, на всех стадиях этого процесса важно обеспечить участие широкого круга стран. Необходимо обеспечить максимально широкий членский состав этой группы, в работе которой должны принимать участие, в частности, представители развивающихся стран. Поэтому рекомендуется в максимально возможной степени обеспечить поддержку такого участия за счет добровольных взносов других государств.

47. Кроме того, после завершения этого исследования и получения мнений группы экспертов рекомендуется создать глобальную программу против высокотехнологичной и компьютерной преступности, и предложить заинтересованным государствам предоставить добровольные взносы для создания и поддержки такой программы. Эта рекомендация более подробно рассматривается ниже в разделе F.

48. В более долгосрочной перспективе для определения политики, полномочий, процедур и механизмов в отношении международного сотрудничества, необходимого для эффективной борьбы с транснациональной компьютерной преступностью, потребуется, по мнению многих экспертов, разработать всеобъемлющий глобальный правовой документ против высокотехнологичной и компьютерной преступности. Тем не менее существуют различные мнения по вопросу о том, насколько быстро удастся разработать такой документ. Как отмечалось в разделе B выше, на ранних этапах этого процесса необходимо обеспечить вовлечение широкого круга стран. В процессе разработки такого документа необходимо также решить ряд важных вопросов, например, вопросов, касающихся национального суверенитета, применения судебных и других гарантий прав человека и роли предприятий частного сектора в принятии мер по обеспечению компьютерной безопасности и борьбе с преступностью. Эти вопросы необходимо учитывать при оценке различных вариантов процесса разработки данного документа, а также его возможной формы и содержания. В целом документ, содержащий более исчерпывающие и императивные положения, будет более эффективным, однако его подготовка потребует больше времени, а его осуществление окажется более сложным и длительным процессом для многих государств. На текущем этапе невозможно сделать каких-либо выводов, однако рекомендуется поручить группе экспертов рассмотреть процедурные и существенные варианты подготовки международного документа и представить соответствующие рекомендации в рамках своего доклада одиннадцатой сессии Комиссии.

49. Еще один фактор, который необходимо учитывать, связан с тем, что в настоящее время отмечается быстрый рост числа случаев, географического охвата и технической сложности высокотехнологичных и компьютерных преступлений, и этот процесс, по-видимому, будет продолжаться параллельно с быстрым развитием и распространением новых компьютерных, сетевых и телекоммуникационных систем. С учетом таких перспектив можно предположить, что, хотя глобальный правовой документ может иметь важное значение в долгосрочной перспективе, необходимо также обеспечить принятие эффективных мер в ближайшем будущем. Поэтому рекомендуется поручить группе экспертов разработать дополнительные варианты в отношении глобальной краткосрочной стратегии борьбы с высокотехнологичной и компьютерной преступностью, уделив особое внимание таким областям, как правовая и техническая помощь в целом и по конкретным делам; установление технических стандартов в отношении сбора, сохранения, аутентификации и предъявления электронных доказательств; а также создание координационных центров или органов по контактам для обработки запросов в отношении предоставления помощи. В связи с этим необходимо принимать во внимание ту работу, которая уже проводится организациями и которая рассматривалась в подразделе A раздела II настоящего доклада.

E. Элементы подробного исследования

50. На текущем этапе с учетом имеющегося объема знаний в области компьютерной преступности по-прежнему возникает гораздо больше вопросов, чем существует ответов, и поэтому необходимо провести дополнительное изучение для установления

предмета исследования, определения того, какие интересы затрагиваются и каким образом они затрагиваются, а также для выявления программных вариантов будущей деятельности. Исследование должно охватывать по меньшей мере следующие элементы:

a) следует провести обзор мнений государств относительно характера и масштабов проблемы и возможных внутригосударственных и международных мер для ее решения;

b) следует обеспечить консультации с государствами, представляющими все категории промышленных, правовых, социальных и экономических систем;

c) следует учитывать как внутреннюю, так и транснациональную преступную деятельность. Хотя многие государства будут рассматривать некоторые вопросы в качестве чисто внутренних проблем, характер компьютерных технологий делает бессмысленным традиционное разграничение между внутренней и транснациональной преступностью. Исследователям, работникам директивных органов и участникам переговоров зачастую будет трудно провести разграничение между внутренней и транснациональной преступной деятельностью, что свидетельствует о необходимости применения комплексного подхода, в частности, на предварительных этапах данного процесса;

d) следует обеспечить учет мнений и содействие со стороны частного сектора, уделив особое внимание следующим вопросам:

i) в рамках исследования необходимо рассмотреть и принять во внимание мнения и материалы компаний, отвечающих за разработку и эксплуатацию соответствующих технологий, включая компьютерное оборудование и программное обеспечение, а также компьютерные и телекоммуникационные сети;

ii) в рамках исследования необходимо рассмотреть также мнения соответствующих неправительственных организаций. Организации, деятельность которых направлена на защиту свободы слова и права на личную жизнь, подвергали критике предыдущие попытки создать эффективные механизмы расследования и способствовали мобилизации политической оппозиции усилиям Группы восьми и Совета Европы в этой области;

e) в рамках исследования необходимо рассмотреть такие вопросы, выходящие за рамки борьбы с преступностью, как устойчивое развитие, защита личной жизни, свобода выражения и других основных прав, а также коммерческие и другие интересы. Эти основополагающие и другие интересы тесно связаны с развитием технологий и, вероятно, будут испытывать определенное воздействие в результате расширения компьютерной преступности и принятия правительствами и международным сообществом мер по предупреждению такой преступности и борьбе с ней;

f) в ходе исследования необходимо оценить масштабы преступной деятельности как в целом, так и в контексте статистически значимых факторов, например конкретные формы преступности, географическое распределение и другие социальные или экономические условия. Вопрос о проблемах, возникающих в процессе сбора и анализа точных статистических данных, уже рассматривался выше. Тем не менее по мере формирования единого мнения относительно технических параметров соответствующей области деятельности и типологии совершаемых в этой области преступлений будут появляться более надежные данные. Кроме того, по мере повышения осведомленности населения о соответствующих видах поведения и о том, что они квалифицируются или должны квалифицироваться в качестве преступлений, должно сократиться число случаев, когда о таких преступлениях не сообщается. Для мобилизации политической поддержки в отношении эффективных внутренних и международных мер по борьбе с такими преступлениями важно также обеспечить сбор предварительных данных;

g) в ходе исследования необходимо рассмотреть определение и классификацию высокотехнологичной и компьютерной преступности. Использованная в настоящем докладе классификация соответствует подходу в этой области других организаций и может послужить основой для дальнейшего рассмотрения, однако для определения рамок, которые будут пользоваться поддержкой правительств, заинтересованных групп и экспертов в этой области, необходимо провести более тщательное и подробное исследование. Это является одной из важнейших первоочередных задач, поскольку определение и

классификация необходимы для обеспечения последовательности при сборе статистических данных и проведении исследований, на которых будет основана последующая деятельность по разработке политики. Для подготовки обоснованной типологии необходимо будет рассмотреть конкретные факторы в ряде важнейших областей, включая следующие:

i) *Соответствующие технологии.* Развитие высокотехнологичной и компьютерной преступности в значительной степени определяется характером и масштабами соответствующих технологий, которые быстро развиваются и переплетаются друг с другом. По этой причине в настоящем докладе и в других работах по этой теме используется общая формулировка "высокотехнологичная и компьютерная преступность". Необходимо провести исследование для обзора всех видов применяемых технологий и разработки вариантов общей классификации, которая будет охватывать все виды такой технологии. Необходимо также более тщательно рассмотреть конкретные технические достижения и виды преступной деятельности, в рамках которой они используются. С учетом быстрого развития технологий следует рассмотреть не только существующие виды технологий, но также и перспективные разработки;

ii) *Характер и мотивы преступников.* Преступники, совершающие преступления в результате применения новых технологий, представляют собой относительно новую область исследований. Мотивы более традиционных преступников, например педофилов, мошенников или международных торговцев наркотиками, хорошо известны. Необходимо рассмотреть с точки зрения компьютерной преступности приспособление таких преступников к новым технологиям;

iii) *Географические аспекты преступлений.* Соответствующие географические аспекты отличаются от географических аспектов более традиционных преступлений по меньшей мере в двух отношениях. Во-первых, происходит взаимное наложение двух основных "географий". Важное значение имеют фактическое физическое местонахождение преступников и связанные с ним конкретные ситуационные факторы, например социальные, экономические или культурные условия. В то же время важное значение будет иметь также электронная география, которая связана с часто упоминаемыми соображениями кибернетического пространства и которая оказывает определенное воздействие на методы преступной деятельности.

F. Варианты и конкретные рекомендации в отношении будущей работы в области высокотехнологичной и компьютерной преступности

1. Возможный международный документ против высокотехнологичной и компьютерной преступности

51. После завершения исследования рекомендуется, чтобы группа экспертов представила Комиссии свои замечания по различным вопросам и вариантам, касающимся возможности и целесообразности разработки международного документа против высокотехнологичной и компьютерной преступности. К числу таких вопросов относятся следующие:

a) вопрос о том, должен ли такой документ, если он будет разработан, носить нормативный или же юридически обязательный характер. В таком документе можно попытаться установить обязательные требования в отношении уголовных преступлений, следственных полномочий и механизмов международного сотрудничества или же просто предусмотреть руководящие указания, которые помогут государствам разрабатывать эффективные меры и содействовать международной унификации законодательства и процедур. Компромиссным решением между этими двумя вариантами, как показывает Конвенция Организации Объединенных Наций против транснациональной организованной преступности, мог бы стать документ, некоторые положения которого предусматривают жесткие обязательства, в то время как другие содержат более общие руководящие принципы или же оставляют регулирование соответствующих вопросов на усмотрение государств–участников;

b) какова взаимосвязь, если она вообще будет существовать, между таким дополнительным

документом и Конвенцией Организации Объединенных Наций против транснациональной организованной преступности. В целом Конвенция может послужить прецедентом для некоторых положений, в то время как другие положения, возможно, окажутся неуместными применительно к предмету высокотехнологичной и компьютерной преступности. Ограничение сферы применения Конвенции только деятельностью "организованных преступных групп", например, исключит из сферы применения значительную часть высокотехнологичных и компьютерных преступлений, поскольку такие преступления совершаются отдельными лицами или группами, которые не охватываются определением, предусмотренным в Конвенции[23]. Таким образом, по-видимому, не представляется возможным разработать еще один протокол к Конвенции, касающийся преступлений такого рода[24];

c) каким образом такой документ, после его принятия, можно будет регулярно обновлять. Как отмечалось в введении к настоящему докладу, для рассматриваемой области характерны быстрые темпы изменения технологий и связанной с нею преступной деятельности, и поэтому необходимо будет обеспечить, чтобы любые нормативные рамки для интеграции внутренних и международных мер соответствующим образом пересматривались по мере таких изменений. Для этих целей можно было бы делегировать отдельные законодательные полномочия определенному органу экспертов, представляющему договаривающиеся государства и созданному для этих целей, разрабатывать протоколы для охвата новых конкретных вопросов по мере их возникновения, применять относительно общие и нейтральные с точки зрения технологии формулировки или же использовать другие меры;

d) каким образом можно обеспечить учет соответствующих интересов, например права на личную жизнь, свободу выражения и другие права человека, а также коммерческие интересы, в рамках международного документа. Хотя с учетом характера данной проблемы основное внимание в документе должно уделяться предупреждению преступности и борьбе с ней, такие другие интересы должны также учитываться как в процессе разработки документа, так и в его существенных положениях.

2. Краткосрочная стратегия борьбы с высокотехнологичной и компьютерной преступностью

52. Как отмечалось выше, высокотехнологичная и компьютерная преступность является одной из наиболее острых проблем, которая может потребовать принятия на международном уровне согласованных ответных мер как в краткосрочной, так и в долгосрочной перспективе. Рекомендуется рассмотреть в исследовании возможные меры, которые могут быть приняты в ближайшем будущем, а группе экспертов необходимо разработать рекомендации, касающиеся краткосрочной стратегии для рассмотрения Комиссией на ее одиннадцатой сессии. Соответствующая стратегия могла бы содержать следующие элементы:

a) обобщение и распространение среди всех государств–членов информации относительно высокотехнологичной и компьютерной преступности и возможных ответных мер, с тем чтобы как можно раньше информировать те государства, которые еще не принимают участия в обсуждениях. Предлагаемое исследование будет являться ключевым элементом таких информационных пакетов, однако в настоящее время имеются также другие материалы, включая следующие:

i) *Руководство Организации Объединенных Наций по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними*, изданное в 1994 году, может быть обновлено и переиздано;

ii) доклады о работе и материалы семинара–практикума по преступлениям, связанным с использованием компьютерной сети, который был организован в ходе десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, могут быть изданы для последующего распространения[25];

iii) материалы других межправительственных организаций, в частности Совета Европы, Интерпол и Лионской группы, учрежденной Группой восьми, могут быть распространены на более широкой основе;

iv) для официальных представителей заинтересованных государств могут быть организованы практикумы, семинары или брифинги, в

которых могут принять участие представители частного сектора;

b) можно было бы обеспечить более широкое распространение материалов, касающихся подготовки работников следственных органов и прокуратуры. Организация Объединенных Наций не занималась подготовкой таких материалов, однако некоторые государства–члены разработали соответствующие материалы для использования в процессе подготовки своих собственных должностных лиц, а в некоторых случаях для использования в рамках проектов технического сотрудничества с другими государствами;

c) некоторые государства будут нуждаться в прямой технической помощи. Такая помощь может охватывать подготовку судей, прокуроров, следователей, а также технических или судебных экспертов, многие из которых смогут впоследствии организовать подготовку других сотрудников. В некоторых случаях такие проекты могут быть объединены с более общими проектами в целях развития, направленными на оказание помощи государствам в приобретении и использовании новых технологий в целях развития. Как отмечалось выше, важно обеспечить, чтобы мероприятия по предупреждению преступности и борьбе с ней стали неотъемлемым элементом таких проектов, что позволит избежать отрицательных последствий компьютерной преступности для развития;

d) следует содействовать созданию во всех государствах–членах координационных центров или органов по контактам. К их числу будут относиться органы по контактам для оказания срочной помощи в связи с расследованием компьютерных преступлений[26], а также для более общих контактов в целях сбора информации о происходящих изменениях в каждом государстве, а также для получения информации от международного сообщества и ее распространения;

e) необходимо обеспечить выделение существенных финансовых и технических ресурсов. Такая помощь может быть предоставлена в форме добровольных взносов в Фонд Организации Объединенных Наций по предупреждению преступности и уголовному правосудию или же на основе предоставления экспертов или материалов для поддержки глобальной программы против высокотехнологичной и компьютерной преступности или конкретных проектов Организации Объединенных Наций. Универсальный характер технологий и их уязвимость от попыток преступников использовать такие технологии в своих целях в любом месте стимулируют государства, обладающие финансовыми или техническими ресурсами, оказывать помощь другим государствам. Компании, занимающиеся разработкой и эксплуатацией компьютерных и телекоммуникационных сетей, также обладают финансовыми и техническими ресурсами, которые могут быть использованы, и заинтересованы в оказании содействия, поскольку многие формы компьютерной преступности угрожают коммерческой жизнеспособности их продукции.

3. Создание глобальной программы против высокотехнологичной и компьютерной преступности

53. Имеющиеся данные свидетельствуют о том, что в настоящее время проводится обширная исследовательская деятельность и деятельность по разработке политических, правовых и технических мер, однако общей координации такой деятельности практически не осуществляется. Масштабы такой деятельности различаются в зависимости от конкретной страны. В ней участвует ряд межправительственных и неправительственных организаций, а также некоторые учреждения и департаменты Организации Объединенных Наций, и за этой деятельностью активно следят коммерческие компании и неправительственные группы заинтересованных сторон. Основное внимание, а также основные ресурсы, как правило, сконцентрированы на рассмотрении конкретных вопросов, вызывающих беспокойство правительств или непосредственно участвующих организаций, что порождает возможность появления пробелов и несоответствий в результатах исследований. Глобальный характер Организации Объединенных Наций обеспечивает ей уникальные возможности в плане изучения и координации деятельности в рассматриваемой области. Поэтому после завершения анализа потребностей и мнений государств–членов рекомендуется создать глобальную программу против высокотехнологичной и компьютерной преступности. Заинтересованным государствам рекомендуется также предоставить добровольные взносы для создания и поддержки такой глобальной программы.

54. Возможный мандат глобальной программы следует рассмотреть на одиннадцатой сессии

Комиссии после получения результатов исследований и мнений группы экспертов. Мандат глобальной программы может охватывать мероприятия, указанные в пункте 52 выше, а также следующую деятельность:

a) выявление государств–членов, нуждающихся в помощи, и анализ их конкретных потребностей;

b) разработка материалов для оказания помощи работникам директивных, законодательных, правоохранительных и судебных органов, а также другим соответствующим должностным лицам в рассмотрении внутренних и транснациональных дел;

c) сбор, обобщение и распространение материалов, подготовленных другими организациями;

d) предоставление правовой, технической и другой помощи государствам по их запросам при наличии достаточных ресурсов;

e) разработка перечня технических экспертных услуг, которые могут быть предоставлены отдельными специалистами и учреждениями, желающими оказывать помощь запрашивающим государствам;

f) координация деятельности с другими учреждениями и департаментами Организации Объединенных Наций, в частности в области прав человека и развития, в целях включения вопросов компьютерной преступности, когда это целесообразно, в другие программы и обеспечение учета материалов других программ при разработке стратегии в области предупреждения преступности и борьбы с ней;

g) координация деятельности с другими межправительственными организациями и отдельными правительствами и учреждениями, занимающимися вопросами высокотехнологичной и компьютерной преступности;

h) координация деятельности с неправительственными группами заинтересованных сторон и компаниями частного сектора, а также мобилизация денежных ресурсов и технической помощи со стороны компаний в рамках глобальной стратегии против высокотехнологичной и компьютерной преступности.

4. Предварительный перечень существенных вопросов для рассмотрения

55. Необходимо будет рассмотреть большое количество аналогичных существенных вопросов в качестве элементов как краткосрочной, так и долгосрочной стратегии. На основе результатов предшествующей работы в рамках Организации Объединенных Наций и других форумов, упомянутых в настоящем докладе, потребуется рассмотреть следующие существенные вопросы:

a) определение причиняющих вред деяний, связанных с использованием новых технологий, и определение новых составов преступлений или расширение существующих составов преступлений для признания таких деяний уголовно наказуемыми;

b) разработка принципов деятельности при транснациональном отслеживании сообщений, включая полномочия на получение, сохранение и раскрытия данных о передаче сообщений[27];

c) разработка принципов, регулирующих преднамеренные и неумышленные трансграничные электронные поиски;

d) разработка общих принципов в отношении перехвата сообщений, передаваемых по компьютерным сетям или в рамках аналогичных систем;

e) оценка необходимости в обеспечении конфиденциальности и неприкосновенности личной жизни в связи с различными формами хранения и передачи данных в целях разработки соответствующих процедур в отношении изъятия и перехвата данных с учетом таких соображений. Большинство государств практически не устанавливают каких-либо ограничений для правоохранительных органов в отношении получения доступа к открытым web–сайтам или сообщениям, передаваемым по web–каналам, однако, вероятно, будут устанавливать определенные ограничения на изъятия данных из более частных источников;

f) разработка общих стандартов или практики для выявления отдельных пользователей компьютерной сети или телекоммуникационных услуг с учетом необходимости обеспечения неприкосновенности личной жизни и сохранения анонимности;

g) разработка общих принципов корректировки судебной практики и норм доказательственного права, с тем чтобы обеспечить возможности для

сохранения, аутентификации и использования компьютерных доказательств в рамках уголовного судопроизводства;

h) разработка общих принципов защиты основных прав как при определении международной политики и мер против высокотехнологичной и компьютерной преступности, так и в процессе применения таких мер в конкретных случаях;

i) разработка общих принципов по вопросам конфиденциальности и целостности данных и согласование таких принципов с потребностями в области обеспечения эффективности мер по борьбе с преступностью;

j) разработка программ и материалов для оказания технической помощи государствам, запрашивающим такую помощь, и мобилизация необходимых финансовых ресурсов. Такие программы и материалы необходимы для оказания помощи государствам в целях обеспечения их эффективного участия в процессе разработки глобальной политики и для обеспечения надлежащей подготовки кадров и оснащения национальных органов, с тем чтобы они могли эффективно и оперативно удовлетворять просьбы об оказании помощи при расследовании транснациональных компьютерных преступлений;

k) сбор, анализ и распространение информации о новых технологиях, преступниках и методах их деятельности, а также об эффективных методах предупреждения и расследования преступлений и организации судебного преследования;

l) подготовка, оснащение и наделение соответствующими ресурсами экспертов правоохранительных органов в целях обеспечения возможностей для эффективного расследования и судебного преследования по внутренним делам, а также возможностей для эффективного сотрудничества с другими государствами по транснациональным делам;

m) необходимость оценки и уточнения роли частного сектора и его взаимоотношений с правительствами как на национальном, так и на международном уровнях. Потребуется рассмотреть следующие конкретные элементы или аспекты таких взаимоотношений:

i) необходимость обеспечения соответствующего баланса между эффективными мерами по борьбе с преступностью, а также техническими и коммерческими ограничениями на их разработку и применение. Требования в области борьбы с преступностью должны учитываться компаниями на стадии разработки новых технологий, а правоохранительным органам следует признавать, что некоторые меры могут оказаться технически неосуществимыми или же могут привести к таким изменениям, которые сделают данную технологию непродуктивной или неконкурентоспособной. Требования в области борьбы с преступностью не должны подрывать рентабельность или конкурентоспособность новых технологий, однако ущерб от преступности и расходы на ее предупреждение должны стать элементом общей оценки затрат–выгод как для правительств, так и для промышленности, а соответствующие расходы при необходимости должны распределяться с учетом прибылей, получаемых в результате применения технологий, которые используются при совершении преступлений;

ii) необходимость налаживания эффективного сотрудничества между правительствами и промышленностью для максимизации выгод и минимизации соответствующих расходов. Меры в этой области предусматривают определение и разработку эффективных методов обеспечения безопасности и других методов предупреждения преступности и их интеграцию в новые технологии на самых ранних этапах разработки, а также организацию учебных и подготовительных мероприятий для правоохранительных органов и органов уголовного преследования в отношении новых технологий, прежде чем потенциальные преступники получат к ним доступ. Развитие технологии в соответствующих отраслях обусловливает важность или даже обязательный характер участия представителей таких отраслей для обеспечения успешного осуществления программ технической помощи, а коммерческие интересы соответствующих предприятий во многих случаях будут оправдывать их участие в таких программах;

iii) необходимость разработки систем и осуществления операций таким образом, чтобы это способствовало эффективному расследованию и уголовному преследованию с учетом необходимости защиты права на личную жизнь и

других прав пользователей соответствующих технологий. В качестве примера можно отметить эксплуатацию систем, позволяющих сохранять доказательства в отношении передачи сообщений в течение разумного срока на случай, если они потребуются в ходе расследования, а также необходимость обеспечения возможности для идентификации клиентов;

iv) необходимость подготовки глобальной оценки в отношении потенциальной роли частного сектора в борьбе с преступностью. С этой весьма сложной проблемой уже сталкиваются многие поставщики услуг, которые разделяют публичную заинтересованность в обеспечении эффективной борьбы с преступностью, однако признают те риски и проблемы, которые могут возникнуть в том случае, если они возьмут на себя определенные функции государственных правоохранительных органов. Компании сталкиваются с весьма противоречивыми требованиями в отношении обеспечения мер безопасности при разработке новых технологий, которые могут оказаться коммерчески нерентабельными или которые могут затрагивать основополагающие интересы их клиентов[28]. Они испытывают также давление со стороны правительств в отношении ограничения или исключения содержания, которое считается незаконным или неприемлемым, или же в отношении оказания помощи государственным правоохранительным органам в проведении уголовных расследований. В связи с этим возникают сложные этические, правовые и политические вопросы, которые должны быть изучены на национальном и глобальном уровнях в целях достижения максимально возможной глобальной унификации.

Примечания

[1] См. "Наведение цифровых мостов" в докладе Генерального секретаря Ассамблее тысячелетия Организации Объединенных Наций (A/54/2000, пункты 150–167). См. также доклад Генерального секретаря о развитии и международном сотрудничестве в XXI веке: роль информационной технологии в контексте основанной на знаниях глобальной экономики (E/2000/52, разделы III–V).

[2] См. European Committee on Crime Problems, Committee of Experts on Crime in Cyberspace, "Draft Convention on Cyber-crime" (PC-CY (2000), draft No. 25, rev.5), с этим текстом можно ознакомиться в интерактивном режиме по адресу http://conventions.coe.int/treaty/en/projets/cybercrime25.htm.

[3] Выводы этих исследований излагаются в рекомендациях Совета Европы R (89) 9 и R (95) 13. Комитет экспертов был учрежден Комитетом министров Совета Европы на 583-м заседании заместителей министров 4 февраля 1997 года.

[4] См. приложение к коммюнике Совещания министров юстиции и внутренних дел Группы восьми, проходившего в Вашингтоне, округ Колумбия, 10 декабря 1997 года.

[5] См. коммюнике Конференции министров стран Группы восьми по проблемам борьбы с транснациональной организованной преступностью, проходившей в Москве 19–20 октября 1999 года, пункт 17 и приложение 1.

[6] Такие совещания были проведены в Париже 15–17 мая 2000 года и в Берлине 24–26 октября 2000 года. Очередное совещание планируется провести в Токио в мае 2001 года.

[7] В пункте 14 резолюции 1999/23 Совет просил Генерального секретаря провести исследование по вопросу об эффективных мерах, которые можно принять на национальном и международном уровнях в целях предотвращения компьютерных преступлений и борьбы с ними, включая рассмотрение вопроса о целесообразности подготовки руководств, руководящих принципов и рекомендаций, и представить Комиссии по предупреждению преступности и уголовному правосудию на ее десятой сессии доклад о выводах этого исследования.

[8] См. резолюции Генеральной Ассамблеи 45/109 и 45/121 от 14 декабря 1990 года и *Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Гавана, 27 августа –7 сентября 1990 года: доклад, подготовленный Секретариатом* (издание Организации Объединенных Наций, в продаже под № R.91.IV.2), глава I, раздел C, стр. 147.

[9] См. A/CONF.169/16/Rev.1, пункты 370–385.

[10] См. резолюцию 55/25 Генеральной Ассамблеи от 15 ноября 2000 года, приложение I, статья 18, пункты 8 и 18.

[11] См. *Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, ...* глава I, раздел C.

[12] *Международный обзор уголовной политики*, №№ 43 и 44 (издание Организации Объединенных Наций, в продаже под № R.94.IV.5).

[13] См. резолюции Генеральной Ассамблеи 52/91 от 12 декабря 1997 года и 53/110 от 9 декабря 1998 года. См. также A/CONF.187/10 и *Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Вена, 10–17 апреля 2000 года: доклад, подготовленный Секретариатом* (издание Организации Объединенных Наций, в продаже под № R.00.IV.8), пункты 161–174.

[14] См. A/CONF.187/L.10, пункт 14.

[15] См. *Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями…*, глава I.

[16] См. статью 2 (термины) и 3 (сфера применения) Конвенции (резолюция 55/25, приложение I).

[17] Такие преступления были недавно рассмотрены Целевой группой по финансовым мероприятиям для борьбы с отмыванием денег Организации экономического сотрудничества и развития (ОЭСР). См. the FATF "Report on money laundering typologies for 2000–2001" (Paris, OECD, February 2001), paras. 5–18.

[18] A/54/2000, пункт 152.

[19] Так, например, Директор Федерального бюро расследований (ФБР) Соединенных Штатов в своем заявлении о кибернетической преступности в Юридическом комитете Сената Соединенных Штатов 28 марта 2000 года сообщил, что в период 1998–1999 годов количество дел, которыми занималось ФБР, возросло двое с 547 до 1 154, и трудно сказать, было ли это обусловлено ростом преступности или увеличением количества сообщений о совершаемых преступлениях или же сочетанием этих двух факторов. См. также P. Graboski, "Computer crime: a criminological overview", *Forum on Crime and Society,* vol. 1 (2001), p.40.

[20] В создании вируса "Мелисса" признался 31-летний программист из Соединенных Штатов, а 15-летний канадец признал себя виновным по 56 уголовным обвинениям в связи с нападениями, вынуждающими системы отказывать в обслуживании. В связи с вирусом "I love you" никаких обвинений выдвинуто не было, однако считается, что местом его происхождения являются Филиппины. Впоследствии было опубликовано множество оценок ущерба от каждого из таких происшествий, однако истинные потери, вероятно, никогда не будут установлены. Соответствующие показатели приведены для того, чтобы дать представление об общих масштабах ущерба и о степени политического беспокойства в связи с угрозой, возникающей в результате совершения таких крупномасштабных преступлений.

[21] См. E/2000/52, разделы III–V.

[22] См. E/2000/52, пункты 79–99.

[23] См. статьи 2 и 3 Конвенции (резолюция 55/25, приложение I).

[24] Все три существующие протокола включают mutatis mutandis положения, касающиеся сферы и порядка применения Конвенции. Многие положения Конвенции, которые были разработаны исходя из того, что они будут применяться только в случаях, связанных с организованными преступными группами, довольно трудно будет применять в тех случаях, когда компьютерные преступления совершаются отдельными лицами.

[25] Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, который организовал этот семинар–практикум, в настоящее время занимается подготовкой его материалов для издания.

[26] Группа восьми уже приступила к осуществлению такого процесса, и он будет продолжен Интерпол.

[27] Термин "данные о передаче сообщений", как правило, охватывает данные, которые хранятся у поставщиков услуг и в которых регистрируется источник и место назначения электронного сообщения. Такие данные могут включать информацию как о первоначальном источнике и конечном получателе, так и о промежуточных источниках или получателях в рамках компьютерной сети. Смежной концепцией является понятие данных об "абоненте" или "пользователе", которое используется поставщиками услуг для идентификации индивидуальных клиентов.

[28] Одним из последних примеров является приказ французского суда, в соответствии с которым работающая в Интернет компания Yahoo! Inc. обязана разработать технические методы, позволяющие блокировать доступ ее абонентов, находящихся на территории Франции, на web–сайты аукционов, на которых продаются памятные вещи, относящиеся к нацистскому периоду. Продажа таких вещей запрещена во Франции, однако является вполне законной в тех странах, в которых расположены соответствующие web–сайты. Поставщики услуг, как правило, готовы принять подобные меры, если это технически возможно, однако только после того, как компетентный суд или другой публичный орган вынесет постановление о том, что само содержание является незаконным.