Организация Объединенных Наций **E**/CN.15/2002/8

Экономический и Социальный Совет

Distr.: General
29 January 2002

Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Одиннадцатая сессия
Вена, 16–25 апреля 2002 года
Пункт 5 предварительной повестки дня*
Международное сотрудничество в борьбе с транснациональной преступностью

Эффективные меры предотвращения высокотехнологичных и компьютерных преступлений и борьбы с ними

Доклад Генерального секретаря

Содержание

* E/CN.15/2002/1.

V.02-50948

I. Введение

1. На своей возобновленной десятой сессии, состоявшейся 6 и 7 сентября 2001 года, Комиссия по предупреждению преступности и уголовному правосудию приняла в качестве одной из последующих мер и во исполнение пункта 18 Венской декларации о преступности и правосудии: ответы на вызовы XXI века, принятой на десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями[1], план действий[2] по предупреждению высокотехнологичных и компьютерных преступлений и борьбе с ними.

2. В своей резолюции 56/121 от 19 декабря 2001 года Генеральная Ассамблея, выразив обеспокоенность в связи с тем, что технический прогресс создал новые возможности для преступной деятельности, и в частности для преступного использования информационных технологий; признав необходимость содействия передаче информационных технологий, в частности развивающимся странам; подчеркнув необходимость укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и отметив в этом контексте ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации; приветствовав работу десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями и с удовлетворением приняв к сведению работу Комиссии по предупреждению преступности и уголовному правосудию на ее девятой и десятой сессиях, постановила отложить рассмотрение этого вопроса до выполнения работы, предусмотренной в вышеупомянутом плане действий.

3. В своей резолюции 56/261 от 31 января 2002 года Генеральная Ассамблея с удовлетворением приняла к сведению планы действий; просила Генерального секретаря обеспечить максимально широкое распространение планов действий; предложила правительствам тщательно рассмотреть эти планы в качестве руководства в их усилиях по формулированию политики в отношении законодательства и программ; и предложила Генеральному секретарю тщательно рассмотреть и надлежащим образом применять планы действий в соответствии со среднесрочными планами и бюджетами по программам и при условии наличия ресурсов.

II. Деятельность по предотвращению высокотехнологичных и компьютерных преступлений и борьбе с ними: современное состояние

A. Общие тенденции и изменения

4. Сфера высокотехнологичных и компьютерных преступлений по-прежнему характеризуется быстротой происходящих в ней изменений, причем это справедливо как в отношении правонарушителей, усилий по предотвращению этих преступлений, деятельности законодательных и правоохранительных органов, так и в отношении самих технологий, обусловливавших изменения. В 2001 году ряд государств либо создали, либо укрепили свой потенциал по борьбе с высокотехнологичной и компьютерной преступностью, выделив это направление в качестве отдельной области законодательной и правоохранительной деятельности. Среди мер по реформированию законодательства можно назвать определение новых составов преступлений, расширение составов уже вменяемых преступлений и укрепление, с учетом современных требований, полномочий по ведению следствия, в частности в том, что касается права производить обыски и выемки и перехватывать телефонные разговоры с целью эффективной борьбы с такого рода преступностью в новой электронной среде. Ожидается, что эта тенденция будет продолжаться, особенно в Европе, где государства приступили в настоящее время к осуществлению Конвенции о киберпреступности, принятой Советом Европы в Будапеште 23 ноября 2001 года[3].

5. Во многих странах и на политико-законодательном уровне, и на уровне следственной работы и правоохранительной деятельности одним из важнейших по-прежнему оставался вопрос об отношениях между предпринимаемыми государством усилиями по борьбе с преступностью и ролью компаний частного сектора, занимающихся производством технического и программного обеспечения для компьютеров и оказанием услуг. Основными проблемами, вызывавшими споры, были вопросы о том, в каком объеме новые технологии должны включать вспомогательные средства по борьбе с преступностью и проведению расследований, кто должен нести расходы по хранению, перехвату и поиску данных, требующихся правоохранительным органам, а также вопросы политической, уголовной и гражданско-правовой ответственности, которые возникают во взаимоотношениях между

государством, поставщиками услуг и индивидуальными потребителями. После ряда происшедших в 1999 и 2000 годах серьезных компьютерных атак, которые приводили к заражению вирусами или блокированию доступа, группа крупных компаний, занимающихся бизнесом в области высоких технологий, создала и профинансировала совместный некоммерческий центр – Центр по обмену и анализу информации в области информационных технологий, – забыв на время о конкурентном соперничестве и объединив усилия в борьбе с компьютерной преступностью. Одной из первоочередных задач крупных технологических компаний стала задача включения в новое программное обеспечение соответствующих компонентов компьютерной безопасности, ибо эти компании стремились снизить свою собственную уязвимость перед компьютерными атаками и прекрасно осознавали то обстоятельство, что страх перед преступностью и наличие эффективных компонентов безопасности стали важными факторами в глазах потребителей, принимающих решения о приобретении новых продуктов.

6. В 2001 году по-прежнему широко и в нарастающих масштабах использовались технические методы обеспечения безопасности и предупреждения преступности, что было связано с самой природой этих технологий, их непрерывным распространением и теми трудностями, которые возникали при применении традиционных методов законодательного и правоохранительного реагирования, особенно когда речь заходила о делах транснационального характера. Среди таких технических методов можно назвать разработку и использование соответствующих программных продуктов, например продуктов, позволяющих распознавать и отфильтровывать из хранимых и передаваемых данных такие "враждебные" программы, как программы-"черви" и программы-вирусы, а также использование таких защитных продуктов, как, например, программные брандмауэры. В целях предотвращения доступа пользователей из стран, где законом запрещены игорный бизнес, порнография или какие-либо иные виды занятий, все более расширялось применение программ "геолокации", позволяющих распознавать географические источники онлайновой связи. Правоохранительные органы такое развитие событий приветствовали, но эти действия критиковали сторонники абсолютной открытости Интернета и эксперты, которые указывали, что эффективное использование подобных программ зависит от желания операторов web-сайтов, а также от их осведомленности о правовых ограничениях, установленных в других странах. Мнения большинства экспертов совпадали также в том, что использование подобных программ действительно предотвращает случайные нарушения и является эффективным средством противодействия неопытным правонарушителям, но оно не эффективно против более грамотных правонарушителей, которые умеют легко укрывать свое настоящее географическое местонахождение от соответствующих программ и использующих их операторов web-сайтов. Наряду с этим расширялись масштабы использования фильтрующих программ, дающих возможность распознавать и блокировать содержание, не предназначенное для детей или каких-либо иных неправомочных групп пользователей, и многие операторы web-сайтов "для взрослых" установили у себя продукты, предназначенные к запуску таких программ. В целях защиты секретных сообщений и предотвращения несанкционированного доступа пользователей к ведомственным или секретным данным использовались также криптографические программы.

7. В правоохранительном сообществе все более широко признается, что следователи, обладающие необходимыми навыками по перехвату сообщений, проходящих по высокоскоростным цифровым сетям, и умеющие успешно вести поиск хранимых данных, дешифровку зашифрованной информации и выполнять другие задачи подобного рода, являются редким и ценным ресурсом, имеющим особую специфику. Во многих ведомствах уже созданы специальные подразделения, призванные оказывать другим следователям помощь в целом ряде областей, от борьбы с терроризмом до противодействия незаконному обороту наркотиков и экономической преступности. Здесь основные проблемы касаются высокой стоимости и длительности подготовки таких следователей, требующей долговременных капиталовложений, трудностей по сохранению в штате приобретших соответствующие навыки следователей, которые на более щедро финансируемых предприятиях частного сектора могут получать более высокую заработную плату, а также обеспечения того, чтобы следователи постоянно находились в курсе изменений в новых технологиях и новейших способов применения таких технологий преступниками, что, впрочем, можно сделать сравнительно просто.

8. Государства-члены испытывают обеспокоенность по поводу возможного использования новых технологий террористическими организациями в целях нападения или защиты, и эта обеспокоенность существенно возросла после нападений, имевших место 11 сентября 2001 года. Опыт показывает, что изощренные преступники-террористы уже используют для связи между собой Интернет. При этом они применяют сложные системы шифрования и другие программы обеспечения компьютерной безопасности, которые используют

в защитных целях для сокрытия передаваемой информации и хранимых данных. Кроме того, возможность наступательного использования новых технологий в террористических целях заставила ряд стран создать специальные органы, которые должны осуществлять защиту обрабатываемых данных, средств связи и других важнейших высокотехнологичных инфраструктур от кибератак.

9. В ходе расследований, проводившихся сразу же после сентябрьских нападений, выяснилось также, что для получения информации, которая могла использоваться при планировании нападений, либо для получения материалов, требующихся для изготовления или усовершенствования химического, биологического или радиологического оружия, уже прибегали к услугам Интернета. Несколько государств, приславших свои ответы в ходе обзора, проводившегося Организацией Объединенных Наций в том числе и по вопросу об использовании взрывчатых веществ в преступных целях, выразили озабоченность в связи с наличием в Интернете информации о том, как изготавливать взрывчатые вещества и сооружать взрывные устройства[4], а человек, которого арестовали в связи с попыткой привести в действие взрывное устройство, находившееся у него в обуви, во время коммерческого рейса из Парижа в Майами 22 декабря 2001 года, сообщил, как передали средства массовой информации, следователям, что он сделал это взрывное устройство, пользуясь информацией, полученной из Интернета. Ведомства по борьбе с наркоманией выражали аналогичную озабоченность в связи с тем, что в онлайновом режиме доступна информация о том, как изготовить синтетические наркотики и где можно приобрести требующиеся для этого ингредиенты.

10. В 2001 году продолжали вызывать обеспокоенность и другие виды компьютерных и высокотехнологичных преступлений. В числе наиболее заметных среди них было использование цифровых технологий и Интернета для изготовления и распространения детской порнографии. Некоторые участники второго Всемирного конгресса против сексуальной эксплуатации детей в коммерческих целях, который состоялся в Иокогаме, Япония, 17–20 декабря 2001 года, увязывали возможный рост эксплуатации детей и увеличение общей массы детской порнографии с наличием этого расширившегося рынка[5], но отмечали, что в результате совместных операций, проведенных правоохранительными органами, удалось пресечь осуществление ряда крупномасштабных Интернет-акций по детской порнографии, многие из которых были транснациональными по своему охвату. В представленных на Конгрессе материалах Интернет увязывался и с другими видами педофилии, включая детский секс-туризм и похищение детей.

11. Обеспокоенность выражалась и по поводу увеличения случаев "кражи персональных данных", когда персональные данные используются преступниками для того, чтобы выдать себя за лицо, чьи данные были украдены. В сочетании с анонимностью онлайновых транзакций и других видов операций "кражи персональных данных" использовались при совершении целого ряда преступлений – от мошенничества до терроризма. К числу других видов преступной деятельности относятся, согласно получаемым сообщениям, самые разные преступные деяния, включающие мошенничество, онлайновое вымогательство, отмывание денег и компьютерную контрабанду, а также преступления, совершаемые против компьютерных систем и их пользователей, с применением вирусов и других "враждебных" программ, а также блокировки доступа. Новым явлением в сфере компьютерного мошенничества стало использование в Интернете ложных благотворительных фондов, которые учреждались для привлечения пожертвований сразу же после террористических нападений, имевших место 11 сентября, при этом мошенники воспользовались возможностью быстрого создания и ликвидации новых web-сайтов.

12. В таких областях, как налогообложение, регулирование хозяйственной деятельности и наблюдение за выполнение природоохранных норм, онлайновые операции также создали ряд ранее не существовавших проблем для национальных систем регулирования и обеспечения соблюдения законов, поскольку хранение данных за рубежом, все более широкое применение шифрования и способность компаний, находящихся в одной стране, непосредственно взаимодействовать с клиентами, находящимися в другом государстве, делают более трудной работу по контролю за выполнением требований в отношении регулирования деятельности, проверок и ревизий. Одним из примеров подобного рода могут служить онлайновые аптеки, деятельность которых – как было определено в докладе Международного комитета по контролю над наркотиками[6] и установлено экспертами Совета таможенного сотрудничества (именуемого также Всемирной таможенной организацией), а также Комиссией по наркотическим средствам – порождает определенные проблемы. Обеспокоенность Международного комитета по контролю над наркотиками связана в первую очередь с незаконными поставками наркотических средств и психотропных веществ, тогда как, по данным других источников, проблема стоит шире и касается также многих медицинских и других препаратов, на которые в ряде стран распространяются ос-

новные режимы таможенного контроля и выписки лекарств по рецептам. Это создает проблему не только для правоохранительных органов, но и для служб здравоохранения, таможенных ведомств и прочих регулирующих организаций.

B. Деятельность в рамках системы Организации Объединенных Наций

13. В своей резолюции 1999/23 от 28 июля 1999 года, озаглавленной "Работа программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия", Экономический и Социальный Совет просил Генерального секретаря, принимая во внимание работу семинара-практикума по теме преступлений, связанных с применением компьютерных сетей, организованного в рамках десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, провести исследование по вопросу об эффективных мерах, которые можно было бы принять на национальном и международном уровнях в целях предотвращения компьютерных преступлений и борьбы с ними. Доклад Генерального секретаря о выводах данного исследования был представлен Комиссии на ее десятой сессии (E/CN.15/2001/4). Ряд ораторов отмечали серьезность высокотехнологичных и компьютерных преступлений и подчеркивали важность принятия мер против таких преступлений на международном уровне, в том числе и в рамках Организации Объединенных Наций. Подчеркивалось также, что борьба с высокотехнологичными и компьютерными преступлениями требует осуществления большого числа сложных мер расследования и что жизненно важное значение имеет выработка общего подхода к борьбе с такими преступлениями.

14. В приложенные к резолюции 56/261 Генеральной Ассамблеи планы действий по осуществлению Венской декларации и последующим мерам в связи с ней включен план действий по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров, в котором содержится призыв к Центру по международному предупреждению преступности:

a) оказывать поддержку национальной и международной исследовательской деятельности, направленной на выявление новых форм преступности, связанной с использованием компьютеров, и оценку последствий этой противоправной деятельности для таких ключевых областей, как устойчивое развитие, охрана права на частную жизнь и электронная торговля, а также ответных мер, принимаемых в связи с этим;

b) распространять согласованные на международном уровне материалы, такие как руководящие принципы, юридические и технические руководства, минимальные стандартные правила, доказавшие свою эффективность практические меры и типовые законы, для оказания законодателям, а также правоохранительным и другим органам помощи в разработке, принятии и применении эффективных мер борьбы с преступлениями, связанными с использованием высоких технологий и компьютеров, и правонарушителями как в целом, так и по конкретным делам;

c) поощрять, поддерживать и осуществлять, в соответствующих случаях, проекты технического сотрудничества и технической помощи. В рамках таких проектов государствам, нуждающимся в информации или помощи в областях предупреждения преступности, систем компьютерной защиты, уголовного законодательства и процедур, уголовного преследования, методов расследования и других соответствующих областях, будут предоставляться услуги соответствующих специалистов.

15. Согласно пункту 5 резолюции 56/261, в котором Генеральная Ассамблея предложила Генеральному секретарю тщательно рассмотреть и надлежащим образом осуществлять планы действий, включая план действий по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров, в соответствии со среднесрочными планами и бюджетами по программам и при условии наличия ресурсов, а также учитывая замечания, высказанные Комиссией на ее десятой сессии[7], с появлением необходимых ресурсов будет предпринято более глубокое исследование этой проблемы и мер, предусмотренных в плане действий.

16. Постоянную обеспокоенность продолжает вызывать все более широкое использование новых компьютерных и телекоммуникационных технологий организованными преступными группировками. Особенно это относится к организациям, занимающимся изготовлением и незаконным оборотом наркотических средств, которые входят в число наиболее организованных и имеющих наибольший объем финансовых средств преступных группировок, в результате чего они имеют доступ к самому совершенному оборудованию и услугам наиболее квалифицированных специалистов. Изготовителями наркотиков и наркоторговцами указанные технологии используются во многом так же, как и законными коммерческими потребителями. Информация о поставке партий наркотиков передается отправителем получателю с использованием носителей, которые сотрудники правоохранительных органов не могут легко

перехватить или считать. Деловая информация хранится в иностранных государствах, укрывается в большой массе других данных и защищена от просмотра ее сотрудниками следственных органов с помощью таких технологий, как брандмауэры и шифрование. Применяя электронные средства, наркоторговцы отслеживают движение груза и контролируют состояние товара, в котором укрыты наркотики или другая контрабанда, а в случае какой-либо неожиданной задержки – получают предупреждение о возможном обнаружении или перехвате поставки. Относительную анонимность электронных переводов финансовых средств все шире используют для оплаты поставок, не привлекая внимания сотрудников правоохранительных органов, а получатели таких платежей используют ее для их последующего отмывания. Интернет, кроме того, используется для передачи такой базовой информации, как, например, инструкции по изготовлению синтетических наркотиков, а также для отправки сообщений, поощряющих злоупотребление наркотиками.

17. В докладе Секретариата от 21 декабря 2000 года о положении в мире в области незаконного оборота наркотиков рассматривалась проблема электронной преступности и была сделана рекомендация правительствам разработать национальную политику в поддержку усилий правоохранительных органов (E/CN.7/2001/5, para. 150). Правоохранительным ведомствам было предложено установить с поставщиками услуг контакт с целью обеспечения хранения последними соответствующих данных достаточно долго для того, чтобы эти данные можно было извлекать для целей следствия, а также наладить взаимодействие в борьбе с отмыванием денег через Интернет. В январе 2002 года вспомогательный орган Комиссии по наркотическим средствам – Руководители национальных учреждений по обеспечению соблюдения законов о наркотиках (Европа) – провел региональное совещание экспертов, на котором были рассмотрены проблемы, стоящие перед правоохранительными ведомствами в связи с выявлением новых технологий в процессе расследования дел о наркотиках. В числе выявленных этой группой проблем – огромный объем хранимых и передаваемых данных, в массе которых приходится выявлять и отыскивать необходимую информацию; возрастающая зависимость правоохранительных органов от поставщиков услуг в отношении поиска или перехвата данных и связанные с этим финансовые последствия и последствия в плане защиты информации, а также появление ряда новых технологий, таких как цифровая сотовая телефония, спутниковая телефония и организация в Интернете защищенных чат-форумов, в отношении которых перехват осуществлять труднее, чем в отношении прежних способов связи. Особая озабоченность выражалась по поводу появления программных продуктов усиленного шифрования, которые затрудняют или делают невозможным считывание перехваченных или изъятых данных и которые получают все более широкое распространение и как прикладные программы, которые могут приобретать и использовать преступники, и как уже готовые встроенные элементы электронной почты (e-mail), сотовой телефонии и других технологий.

18. В своих докладах за 1997[8], 1998[9] и 2000[10] годы Международный комитет по контролю над наркотиками выражал озабоченность по поводу разнообразных способов, с помощью которых новые коммуникационные технологии становятся одним из факторов незаконной деятельности, связанной с наркотиками. В своем докладе за 2001 год Комитет подробно рассмотрел эту проблему и вынес ряд соответствующих рекомендаций. В целом Комитет констатировал, что организованная преступность приобрела глобальный характер и что свою роль в этом сыграло появление новых коммуникационных технологий. Что касается международных проблем, связанных с наркотиками, появление новых коммуникационных технологий привело к тому, что деятельность изготовителей наркотиков, наркоторговцев и других преступников стала более эффективной, а осуществление расследования и уголовного преследования такой деятельности осложнилось. Конвергенция технологий означала, что преступники стали использовать не только компьютеры и Интернет, но также факсимильные аппараты, электронные пейджеры, карманные компьютеры с функциями записной книжки и сотовые телефоны. Для защиты таких приборов применяют шифрование, брандмауэры и другие программные средства защиты, а для того, чтобы при оплате не указывать поставщику электронных услуг свои подлинные имена и географические адреса для высылки счетов, преступники используют предварительно оплаченные счета. Комитет отметил также появление случаев, когда объекты расследования предпринимают контрнаступательные действия против правоохранительных ведомств. Одни для помощи в защите своих сообщений и хранении данных нанимают профессиональных специалистов по компьютерной безопасности, а другие используют методы "ответного хакерства" и атакуют компьютеры следователей, пытаясь испортить доказательства или подорвать усилия по расследованию. В одном случае, чтобы получить информацию, необходимую для перехвата электронных сообщений, отправляемых и получаемых следователями, у них похитили аппаратуру, в результате чего личности следователей были установлены и они стали получать угрозы[11].

19. Несмотря на то что обеспокоенность в первую очередь, безусловно, вызывает использование новых технологий в качестве средств прямой поддержки незаконного оборота наркотиков, одной из проблем для национальных регулирующих органов Комитет назвал использование Интернет-аптек как поставщиков отпускаемых по рецепту наркотических средств и психотропных веществ, а в более общем плане указал на озабоченность экспертов наличием информации, поощряющей незаконное потребление наркотиков или приуменьшающей связанную с этим опасность. Среди других проблем были обозначены распространение информации о том, как изготавливать незаконные наркотики, и доступность химических веществ-прекурсоров и связанной с ними информации[12].

20. Касаясь более позитивных аспектов, Комитет рассмотрел также возможность расширения использования защищенных Интернет-коммуникаций как основы международного сотрудничества и отметил, что международные и национальные организации могут использовать Интернет как средство профилактики, если с его помощью будет распространяться информация, способствующая делу просвещения и разубеждения потенциальных наркоманов[13].

21. Комитет вынес ряд рекомендаций, направленных на обеспечение того, чтобы сотрудники органов по обеспечению применения законов о наркотиках получали надлежащую подготовку, ресурсы и юридические полномочия, которые давали бы им возможность успешно решать вышеперечисленные проблемы. Эти рекомендации касались ресурсов, требуемых для привлечения квалифицированных сотрудников, закупки аппаратного и программного оборудования, необходимого для проведения расследований, а также обеспечения достаточной защиты основных объектов инфраструктуры, позволяющей предохранять материалы расследований от самых изощренных "кибератак". Несколько рекомендаций имели своей направленностью позитивное использование технологий, в частности в просветительских и профилактических целях, а также укрепление – с целью выявления злоупотреблений и эффективной борьбы с ними – сотрудничества между правоохранительными органами, поставщиками услуг и пользователями этих технологий. Наряду с этим Комитет остановился на необходимости укрепления международного сотрудничества и разработки международных норм и рекомендовал обеспечить скорейшую ратификацию Конвенции Совета Европы о киберпреступности и рассмотреть вопрос о подготовке конвенции Организации Объединенных Наций о борьбе с киберпреступностью[14].

22. После проведения в августе 1996 года Всемирного конгресса в Стокгольме правительство Японии пригласило в свою страну второй Всемирный конгресс против сексуальной эксплуатации детей в коммерческих целях, который состоялся в Иокогаме 17–20 декабря 2001 года и организаторами которого совместно выступили Детский фонд Организации Объединенных Наций (ЮНИСЕФ), организация "За прекращение детской проституции в азиатском туризме" (ECPAT International) и Группа НПО "За Конвенцию о правах ребенка". Присутствовавшие на Конгрессе представители ЮНИСЕФ и ряда неправительственных организаций, а также отдельные эксперты высказывали обеспокоенность по поводу влияния новых технологий на сексуальную эксплуатацию детей. Их обеспокоенность была связана главным образом с тем, как новые технологии обеспечивают, поощряют или облегчают изготовление и распространение детской порнографии. Например, появление технологии цифровой фотографии значительно упростило изготовление порнографии, а для сокрытия порнографии от следственных органов стали применяться методы шифрования и стеганографии[15]. В целях распространения детской порнографии использовали и Интернет как таковой, ибо с его помощью можно организовать относительно безопасный и легкий доступ, повысить спрос и затруднить обнаружение, пресечение, расследование и конфискацию. Наличие легкого доступа и снижение риска для преступников были сочтены факторами, способствующими увеличению спроса на детскую порнографию, в связи с чем возрастает опасность для детей. По поводу новых технологий высказывались и другие опасения. Одно из таких опасений связано с тем, что Интернет используют педофилы, стремящиеся устанавливать анонимные контакты с детьми, а это иногда заканчивается похищением детей. В своей заключительной декларации, озаглавленной "Иокогамское глобальное обязательство, 2001 год", второй Всемирный конгресс призвал к принятию адекватных мер по нейтрализации негативных аспектов новых технологий, в частности той роли, какую играет в детской порнографии Интернет. Он также признал за новыми технологиями потенциальные возможности в деле защиты детей путем распространения соответствующей информации и взаимодействия тех, кого тревожит проблема сексуальной эксплуатации детей.

C. Деятельность других организаций

23. Работа других организаций была подробно описана в докладе Генерального секретаря от 30 марта 2001 года (E/CN.15/2001/4). Эта работа еще продолжается, и многое предстоит сделать, но один орган успешно завершил свою работу в 2001 году. Сессии Ко-

митета экспертов Совета Европы по преступности в киберпространстве завершились тем, что 23 ноября 2001 года Совет принял Конвенцию о киберпреступности. Конвенцию подписали 26 государств – членов Совета, а также 4 неевропейских государства, которые участвовали в ее разработке. Конвенция вступит в силу после того, как ее ратифицируют пять стран, причем как минимум три из них должны входить в состав членов Совета. Другие государства, не являющиеся членами Совета, также могут присоединиться к Конвенции по предложению Комитета министров Совета, но на это требуется согласие государств, ужу ставших ее участниками. После того как был опубликован проект этой конвенции, он получил положительные отклики со стороны правоохранительного сообщества, но раздавались и критические голоса как из среды групп правозащитников, озабоченных предусматривавшимися в конвенции полномочиями по проведению расследований, так и из среды провайдеров услуг Интернета, чьи опасения были связаны с финансовыми последствиями хранения информации и других видов помощи правоохранительным ведомствам.

24. Международная организация уголовной полиции (Интерпол) продолжала в 2001 году выполнение ряда мероприятий, направленных на борьбу с высокотехнологичной и компьютерной преступностью. Интерпол часто выступал базовой организацией по сотрудничеству сил полиции различных государств в проведении многосторонних расследований онлайновых преступлений, в частности связанных с распространением детской порнографии. Он продолжил усилия по оказанию помощи правоохранительным ведомствам развивающихся стран путем рассылки нескольких руководств для следователей и учреждения ряда региональных рабочих групп по преступлениям, связанным с информационными технологиями. В конце 2000 года он расширил свой web-сайт, включив в него сегмент, касающийся преступлений, связанных с информационными технологиями, а впоследствии расширил этот сайт, добавив в него раздел с предупреждениями о вирусах.

25. В 2001 году продолжила свою работу Группа экспертов Всемирной таможенной организации по электронной преступности, которая изучила ряд вопросов, касающихся различных видов противоправной деятельности и представляющих интерес для государств – членов ВТО. Особое внимание уделялось преступлениям, связанным с "кражей персональных данных" или мошенничеством, к которым контрабандисты иногда прибегают, чтобы скрыть свои личные данные или избежать наблюдения; с электронным отслеживанием поставок, которое используется для предупреждения контрабандистов о возможном обнаружении укрытой контрабанды; с онлайновым отмыванием денег и с ростом числа Интернет-аптек, которые уклоняются от соблюдения внутригосударственных законов и средств контроля за ввозом и вывозом наркотиков, применяемых в медицинских целях и отпускаемых по рецептам. Группа экспертов рассмотрела также многие общие проблемы, которые поднимаются и другими правоохранительными ведомствами, в том числе проблемы мошенничества с применением электронных средств, заражения вирусами и другими "враждебными" программами, а также проблему кибервымогательства.

III. Заключительные замечания

26. В настоящем докладе был представлен краткий обзор текущих усилий по предотвращению высокотехнологичных и компьютерных преступлений и борьбе с ними и были освещены общие тенденции и события как в Организации Объединенных Наций, так и вне ее. При условии наличия ресурсов Центр по международному предупреждению преступности Управления по борьбе с наркотиками и предупреждению преступности Секретариата будет руководствоваться в своей будущей деятельности указаниями Комиссии по предупреждению преступности и уголовному правосудию и других директивных органов в отношении выполнения как плана действий по осуществлению Венской декларации, так и всех других конкретных рекомендаций, которые будут исходить от таких органов. В соответствии с резолюцией 56/121 Генеральной Ассамблеи Генеральному секретарю может быть предложено доложить Ассамблее на ее пятьдесят восьмой сессии о ходе работы по данному направлению. Исходя из этого, Комиссия, возможно, пожелает рассмотреть и дать свои руководящие указания относительно будущей работы Центра, а также определит, в рамках существующих приоритетов, возможные варианты действий.

Примечания

[1] *Официальные отчеты Экономического и Социального Совета, 2001 год, Дополнение № 10* (E/2001/30/Rev.1), часть вторая, глава II, раздел A, проект резолюции II, раздел XI.

[2] См. *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).

[3] Council of Europe, *European Treaty Series*, No. 185.

[4] См. доклад Генерального секретаря о результатах исследования о незаконном изготовлении и обороте взрывчатых веществ преступниками и их использовании в преступных

целях (E/CN.15/2002/9/Add.1). Группа экспертов по вопросам незаконного изготовления и оборота взрывчатых веществ также рекомендовала государствам принять меры к тому, чтобы воспрепятствовать распространению подобной информации, в частности через Интернет [E/CN.15/2002/9, пункт 37 g)].

[5] См. “Profiting from abuse: an investigation into the sexual exploitation of our children”, UNICEF, 2001 (Sales No. E.01.XX.14) и ECPAT International, “Child pornography”, pp. 19-21.

[6] *Доклад Международного комитета по контролю над наркотиками за 2000 год* (издание Организации Объединенных Наций, в продаже под № R.01.XI.1), пункты 30, 100 и 133–137.

[7] *Официальные отчеты Экономического и Социального Совета, 2001 год, Дополнение № 10* (E/2001/30/Rev.1), часть первая, глава III, пункты 36–38.

[8] *Доклад Международного комитета по контролю над наркотиками за 1997 год* (издание Организации Объединенных Наций, в продаже под № R.98.XI.1), пункт 23.

[9] *Доклад Международного комитета по контролю над наркотиками за 1998 год* (издание Организации Объединенных Наций, в продаже под № R.99.XI.1), пункт 241.

[10] *Доклад Международного комитета по контролю над наркотиками за 2000 год* (издание Организации Объединенных Наций, в продаже под № R.01.XI.1), пункты 30, 100 и 133–137.

[11] *Доклад Международного комитета по контролю над наркотиками за 2001 год* (издание Организации Объединенных Наций, в продаже под № R.02.XI.1), пункты 5–83.

[12] Там же, пункты 19–21.

[13] Там же, пункты 44–66.

[14] Там же, пункты 72–83.

[15] При шифровании цифровое содержание засекречивается в соответствии с определенным математическим алгоритмом, в результате чего становятся невозможными дешифровка и считывание документа в отсутствие ключа или пароля, которые, как правило, знают лишь владелец или предполагаемый получатель данных. При стеганографии используются программы, позволяющие скрыть данные, образующие один компьютерный файл, среди данных, образующих другой, обычно гораздо бóльших размеров, файл. Стеганографию обычно используют, чтобы скрыть текст или изображения порнографического характера среди безобидных цифровых фотографий, причем без заметного изменения внешнего вида последних. Как правило, скрытые изображения можно найти и извлечь (при условии, что они не зашифрованы), но это делается лишь тогда, когда у следователей уже возникли какие-то подозрения насчет их существования. Цифровая фотография может использоваться для изготовления детской порнографии как путем прямой съемки детей, так и косвенно посредством изменения, или "морфинга", изображений взрослых людей, чтобы они выглядели как дети.