Организация Объединенных Наций A/CONF.187/10

ПРЕСТУПНОСТЬ

Десятый Конгресс
Организации Объединенных Наций
по предупреждению преступности
и обращению с правонарушителями

Вена, 10-17 апреля 2000 года

Distr.: General
14 December 1999

Russian
Original: English

Пункт 5 предварительной повестки дня*
Эффективное предупреждение преступности:
в ногу с новейшими достижениями

Преступления, связанные с использованием компьютерной сети

Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети

Резюме

Для эффективного предупреждения киберпреступности и борьбы с ней необходим согласованный международный подход на различных уровнях. На внутреннем уровне для расследования киберпреступлений требуются надлежащий персонал, специальный опыт и знания и процедуры. Государствам настоятельно рекомендуется изучить механизмы, позволяющие обеспечить своевременную и четкую защиту данных, содержащихся в компьютерных системах и сетях, на тот случай, если данные потребуются в качестве доказательства в процессуальных действиях. На международном уровне для расследования киберпреступлений необходимы оперативные действия, опирающиеся на координацию усилий национальных правоохранительных органов и принятие соответствующего юридического основания.

Кроме того, в настоящем документе, в частности для поддержки уже предпринятых международных инициатив, рассматриваются пути обмена техническими и судебными знаниями и опытом между национальными правоохранительными органами, а также необходимость обсуждения на международном уровне текущих и будущих правовых мер по развитию международного сотрудничества в расследовании киберпреступлений.

* A/CONF.187/1.

V.99-90956

СОДЕРЖАНИЕ

I. Юридическая справка

1. Генеральная Ассамблея в своей резолюции 52/91 от 12 декабря 1997 года постановила провести в рамках десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями четыре семинара-практикума, посвятив один из них вопросу о преступлениях, связанных с использованием компьютерной сети. В своей резолюции 53/110 от 9 декабря 1998 года Ассамблея одобрила программу работы десятого Конгресса, в том числе проведение четырех технических семинаров-практикумов, один из которых будет касаться преступлений, связанных с использованием компьютерной сети. В этой резолюции Ассамблея подчеркнула важное значение семинаров-практикумов и предложила государствам-членам, неправительственным организациям и другим соответствующим органам оказать финансовую, организационную и техническую поддержку мероприятиям по подготовке семинаров-практикумов, включая подготовку и распространение соответствующих информационно-справочных материалов.

2. Экономический и Социальный Совет в своей резолюции 1999/19 от 28 июля 1999 года по рекомендации восьмой сессии Комиссии по предупреждению преступности и уголовному правосудию призвал государства-члены, другие заинтересованные организации и Генерального секретаря действовать совместно для обеспечения того, чтобы четыре семинара-практикума прямо сосредоточили свое внимание на соответствующих вопросах, а также на достижении практических результатов, и предложил заинтересованным правительствам принять последующие меры в форме конкретных проектов или мероприятий в области технического сотрудничества. Во исполнение этой резолюции Азиатский и дальневосточный институт по предупреждению преступности и обращению с правонарушителями организовал два совещания экспертов по преступлениям, связанным с использованием компьютерной сети, на которых был проделан основной объем работ по подготовке к семинару-практикуму по компьютерным преступлениям. Центр по международному предупреждению преступности с удовлетворением отмечает усилия, предпринятые Азиатским и дальневосточным институтом по предупреждению

преступности и обращению с правонарушителями и группой экспертов, которые сделали возможным проведение такого семинара-практикума.

II. Цель и рамки настоящего документа

3. Возникновение таких международных компьютерных сетей, как Интернет, дает возможность пользователям вступать в связь, предпринимать действия и совершать коммерческие операции с другими пользователями во всех странах мира. Поскольку использование компьютеров и сетей может быть как законным, так и незаконным, из этого следует, что изучением возможностей этого нового средства общения занимаются также и лица, и группы, имеющие преступные мотивировки. Борьба с преступностью в современных условиях международных компьютерных сетей усложняется по трем нижеизложенным причинам:

a) преступные деяния могут иметь место в электронной среде. Для расследования киберпреступлений, т.е. любых преступлений, совершенных с использованием какой-либо электронной сети, требуются конкретный специальный опыт и знания, процедуры расследования и юридические полномочия, которыми правоохранительные органы соответствующего государства могут и не располагать;

b) международные компьютерные сети, такие как Интернет, представляют собой открытую среду, дающую пользователям возможности совершать определенные действия за пределами границ государства, в котором они находятся. В то же время следственные действия правоохранительных органов в целом должны ограничиваться территорией собственного государства. Это означает, что для борьбы с преступностью в открытых компьютерных сетях требуется активизировать международное сотрудничество;

c) открытые структуры международных компьютерных сетей позволяют пользователям выбирать такую правовую среду, которая оптимальным образом соответствует их целям. Пользователи могут выбирать такие страны, в которых определенные деяния, совершаемые в электронной среде, не влекут за собой уголовную ответственность. Такие страны могут создавать привлекательные возможности для противоправных действий лиц из тех государств, где такие действия влекут за собой уголовную ответственность в соответствии с их внутренним правом. Наличие "информационных убежищ" - государств, в которых не отдается приоритет сокращению или предотвращению неправомерного использования компьютерных сетей или не разработаны эффективные процессуальные нормы, - может сдерживать усилия других стран по борьбе с преступностью с использованием компьютерных сетей.

4. Ниже в настоящем документе обсуждаются главным образом пути принятия согласованных международных мер в целях содействия, активизации и совершенствования используемых в настоящее время методов борьбы с киберпреступностью. Особый интерес представляет та роль, которую могут играть Организация Объединенных Наций и другие международные организации. Приводится справочная информация, касающаяся семинара-практикума по преступлениям, связанным с использованием компьютерной сети.

5. Ниже обсуждаются некоторые виды преступлений, которые могут совершаться в международных электронных сетях, и рассматриваются причины, по которым такие преступления требуют внимания со стороны международного сообщества и принятия коллективных мер. Для выработки определения таких преступлений необходимо обеспечить их общее понимание международным сообществом и сформулировать руководство для национальной уголовно-правовой политики в данной области.

III. Категории киберпреступлений

6. Такие используемые в настоящем документе термины, как компьютерные системы или компьютерные сети, относятся в целом к электронной среде. Несмотря на то, что еще существуют автономные сети, нормой скорее является наличие одной или нескольких компьютерных систем, включающих персональные компьютеры, связанные между собой и образующие сеть. В документе не проводится различие между частными и публичными сетями и сетями, основанными на наличии действующих каналов связи. В настоящем документе, если не указано иное, телекоммуникационные системы отнесены к той же категории, что и компьютерные системы и сети.

7. В настоящее время хорошо известным примером публичной компьютерной сети может служить Интернет. В последнее десятилетие произошел стремительный рост этой сети, успех которой определяется во многом использованием общих коммуникационных протоколов. Применяющий такие протоколы оператор любой сети или системы без труда может становиться одним из звеньев сети в качестве "поставщика", именуемого в настоящем документе поставщиком услуг Интернет. По коммерческим и техническим соображениям в некоторых странах поставщики услуг образуют ассоциации или общества, вырабатывают общие позиции по определенным вопросам[1]. Согласно оценкам, в настоящее время пользователями Интернет являются во всем мире 200 млн. человек, 112 миллионов из которых приходится на Северную Америку, 47 миллионов - Европу и 33 миллиона - Азию и район Тихого океана[2]. Согласно статистическим данным, на конец 1995 года существовало 26 миллионов пользователей, большинство из которых проживало в Соединенных Штатах Америки. В 1999 году ежемесячные темпы роста числа пользователей составляли, согласно оценкам, свыше трех процентов.

8. Главная функция любой компьютерной системы заключается в обработке данных. Термин "данные" определяется как факты, инструкции или концепции, излагаемые обычным образом, в форме, поддающейся пониманию человеком или автоматизированной обработке[3]. Электронные данные представляют собой серию магнитных точек в постоянной или временной запоминающей среде или форме электронных зарядов в процессе их передачи. Если данные поддаются идентификации и контролю по конкретному носителю данных, например данные, хранящиеся на одной или нескольких дискетах, то с юридической точки зрения они могут рассматриваться как единый и ощутимый материальный предмет. В целом данные, обрабатываемые в рамках компьютерной системы, уже нельзя квалифицировать и контролировать по их носителю. Операционные системы автономно перемещают файлы данных из одного физического места в запоминающей среде в другое. В компьютерных сетях распределенная обработка данных делает невозможным для лиц, контролирующих данные, устанавливать физическое местонахождение всего или части файла без принятия специфических мер. Такие данные контролируются только в рамках логических операций, а не физических действий, что затрудняет подход к чистым данным в юридическом смысле как к материальным предметам.

9. Термин "киберпреступность" охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. В принципе он охватывает любое преступление, которое может быть совершено в электронной среде. В настоящем документе термин "преступность" охватывает такие виды деяний, которые обычно определяются как противоправные, либо в ближайшее время могут быть криминализованы. Определенные деяния могут быть криминализованы лишь в отдельных государствах, однако, как поясняется в пункте 13, на ряде международных форумов была выработана общая позиция по вопросу о том, какие деяния в связи с компьютерными системами и сетями должны быть криминализованы. Это соображение является отправной точкой для дальнейшего обсуждения.

10. Главное внимание в настоящем документе уделяется уголовному расследованию и преследованию киберпреступности. Термин "правоохранительные органы" означает такие органы, на которые согласно закону возложены функции расследования преступлений и преследования за них. В некоторых государствах-членах созданы специализированные подразделения, занимающиеся расследованием или содействием расследованию преступлений, связанных с использованием компьютеров. На международном уровне организацией, выполняющей координационные функции в отношении регистрации и распределения полицейских сведений по таким вопросам, как лица, состоящие в розыске, и похищенное имущество, является Международная организация уголовной полиции (ИНТЕРПОЛ).

11. В ходе расследования киберпреступлений правоохранительные органы одного государства могут сотрудничать с органами других государств в форме как оказания помощи по конкретным делам, так и обмена общей информацией о преступных организациях и уголовных делах. В ходе конкретного расследования они могут обращаться с просьбами, касающимися использования материалов, имеющихся в другом государстве. Рамки сотрудничества между национальными правоохранительными органами определяются внутренним правом каждого государства, а также международными соглашениями, в том числе соглашениями о взаимной правовой помощи.

12. В числе общих примеров злоупотребления международными компьютерными сетями можно отметить использование в сообщениях выражений, запрещенных законом, предложение незаконных продуктов или выдвижение сфальсифицированных предложений с целью получения незаконной финансовой выгоды. В этой связи Интернет используется аналогично любому инструменту или средству, которые могут применяться для совершения того или иного преступления. В сущности сеть представляет собой среду для совершения преступлений, а не неотъемлемый атрибут для их совершения. Правонарушителей могут привлекать специфические свойства сети Интернет, которую можно использовать вместо традиционных средств: Интернет обеспечивает прекрасные каналы связи и возможность скрыть свою личность, причем риск быть подвергнутым уголовному преследованию в рамках какой-либо правовой системы относительно невысок. Помимо вышеуказанных видов преступности, некоторые пользователи сети Интернет получают незаконный доступ к смежным системам, и при этом они нарушают их функционирование или изменяют их содержание. Такие деяния подпадают под определение "компьютерных преступлений". Лица, совершающие преступления с использованием компьютеров, используют конкретные технические знания, опыт или инструменты для осуществления противоправной деятельности. Компьютерные системы могут быть легкими мишенями, поскольку не предусмотрены достаточные меры защиты или поскольку пользователям не известно, с каким риском сопряжены такие системы. Кроме того, факторы, обеспечивающие удобство пользования той или иной системой, как правило, не обеспечивают защиту данных. Необходимо широко разъяснять изъяны с точки зрения защиты, которыми страдают успешные в коммерческом отношении системные виды программного обеспечения.

13. Хотя заинтересованные страны учитывают проблемы, вытекающие из транснациональной киберпреступности, на глобальном уровне такой форме преступности не уделяется достаточное внимание. В рамках Организации Объединенных Наций, например, еще не разработана политика, конкретно касающаяся криминализации киберпреступлений; национальное законодательство, в тех случаях, когда оно вообще применимо к киберпреступлениям, может применяться в их отношении самым различным образом. Причины отсутствия внимания к киберпреступности могут включать в себя относительно низкий уровень участия в международных электронных коммуникациях, недостаточный уровень опыта в правоохранительной области и заниженные оценки социальных издержек, которые, как ожидается, могут влечь за собой преступления, совершаемые в электронной среде. В рамках глобальной компьютерной сети уголовно-правовая политика отдельного государства оказывает

прямое воздействие на международное сообщество. Киберпреступники могут направлять свои действия в электронной среде через определенное государство, где такие деяния не криминализованы, и таким образом они могут находиться под защитой закона такой страны. Даже если в круг конкретных национальных интересов того или иного государства не входит криминализация определенных деяний, оно может рассмотреть вопрос о принятии таких мер, с тем чтобы не превратиться в "информационное убежище" и не поставить себя в условия международной изоляции. Обеспечение международного сотрудничества правоохранительных и судебных органов различных государств невозможно без согласования материальных норм уголовного права в отношении киберпреступлений.

14. Существуют две категории киберпреступлений:

a) киберпреступление в узком смысле ("компьютерное преступление"): любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

b) киберпреступление в широком смысле ("преступление, связанное с использованием компьютеров"): и любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети.

15. По определениям, изложенным в предыдущем пункте, компьютерная преступность охватывает все противоправные деяния, направленные против защиты системы данных посредством электронных операций. Защиту компьютерных систем и данных можно охарактеризовать на основе трех принципов: обеспечение конфиденциальности, целостности или наличия данных и функций обработки. Согласно описанию, подготовленному Организацией экономического сотрудничества и развития в 1985 году[4], а также более подробной рекомендации Совета Европы 1989 года[5], правонарушения, связанные с конфиденциальностью, целостностью или наличием, включают в себя следующее:

a) несанкционированный доступ, т.е. неправомерный доступ к компьютерной системе или сети путем преодоления мер защиты;

b) повреждение компьютерных данных или компьютерных программ, т.е. неправомерное стирание, повреждение, ухудшение состояния или подавление компьютерных данных или компьютерных программ;

c) компьютерный саботаж, т.е. ввод, изменение, стирание или подавление компьютерных данных или компьютерных программ, либо вход в компьютерные системы с целью помешать функционированию компьютера или телекоммуникационной системы;

d) несанкционированный перехват, т.е. перехват без разрешения и с использованием технических средств, сообщений, поступающих в компьютерную систему или сеть, исходящих из компьютерной системы или сети или циркулирующих в рамках такой системы или сети;

e) компьютерный шпионаж, т.е. приобретение, разглашение, передача или использование данных, составляющих коммерческую тайну, без разрешения или юридического основания с целью либо нанесения экономического ущерба лицу, имеющему право на сохранение тайных сведений, либо приобретения незаконных преимуществ для себя или в интересах третьего лица.

16. Первое из упомянутых преступлений - несанкционированный доступ, иногда именуемый хакерством, совершается довольно часто, причем нередко в сочетании со вторым

преступлением, повреждением данных, или с компьютерным шпионажем. Часто используемый в настоящее время хакерами вариант заключается в несанкционированном доступе в Web-узел и размещение информации оскорбительного или вредного характера. Для эффективного расследования правонарушений, совершаемых хакерами, требуются, как правило, сотрудничество с пострадавшей стороной и определенные приемы для захвата хакера на месте преступления. Преступниками нередко являются молодые люди, имеющие прекрасное техническое образование, которые могут не отдавать себе отчета в низком моральном уровне своих действий или размере потенциального ущерба. Помимо преступлений, совершаемых хакерами, некоторые страны ввели уголовную ответственность за такие деяния, как торговля паролями или хакерскими устройствами.

17. Повреждение компьютерных данных и программ включает в себя запуск "червей" или компьютерных вирусов. Червь может в конечном счете полностью выводить из строя компьютер, а вирус может приводить к потере всех данных, хранящихся на жестком диске. Одним из современных способов распространения вирусов являются электронные сообщения, поступающие от неизвестных адресатов. Пользователи сети Интернет могут и не знать о риске, сопряженном с открытыми электронными сетями и получением сообщений от неизвестных адресатов. По финансовым соображениям имеющиеся на рынке антивирусные программы могут и не применяться. Следователи по уголовным делам могут сталкиваться с трудностями в процессе доказательства вины лиц, ответственных за запуск вируса, нанесшего ущерб. Кроме того, хакеры могут (в течение какого-то времени) использовать в своих целях изъяны в защите часто используемых программ, а также получать доступ к компьютерным системам других лиц или, в исключительных случаях, устанавливать контроль над такими системами, заложив в них специфические программные функции. Пользователи сети Интернет не всегда располагают адекватной или последней информацией о возможных опасностях и дополнительных мерах защиты, предлагаемых изготовителями системного программного обеспечения.

18. Совет Европы[5] (см. пункт 15 выше) определяет мошенничество, связанное с использованием компьютеров, следующим образом:

> "Ввод, изменение, стирание или подавление компьютерных данных или компьютерных программ либо иное вмешательство в процесс обработки данных, что наносит другому лицу экономический ущерб или ведет к утрате его имущества, с целью получения незаконной экономической выгоды для себя или в интересах другого лица".

Приведенное выше положение относится к ситуации, когда правонарушитель - несанкционировано или с разрешения - вмешивается в процесс надлежащего функционирования обработки данных компьютером таким образом, что это приводит к последствиям, подпадающим под определение мошенничества. Оно не охватывает хорошо известные схемы обмана людей посредством электронных обращений или сообщений через Интернет, такие как предложения о продаже акций по привлекательной цене; инвестиции в недвижимость в иностранном государстве; предоставление ссуд на условиях, обеспечивающих исключительно высокую норму прибыли; предоплата недостаточно тщательно охарактеризованных товаров; или приглашение присоединиться к финансовой пирамиде. Вероятно, что к таким схемам будут применяться традиционные положения о мошенничестве.

19. Подлог с использованием компьютеров определяется Советом Европы (см. пункт 15 выше) следующим образом:

> "Ввод, изменение, стирание или подавление компьютерных данных или компьютерных программ, либо иное вмешательство в процесс обработки данных таким образом или на таких условиях, которые, согласно национальному законодательству, образуют состав

такого преступления, как подлог, совершенный в отношении традиционного объекта такого правонарушения."

Цель этого положения заключается в криминализации подлога в отношении компьютерных данных таким образом, который функционально эквивалентен криминализации подделки обычных документов.

20. В этой связи следует отметить еще два вида смежных преступлений. Первый из них касается нескольких форм мошенничества в связи телекоммуникационными услугами. В таких случаях преступник пытается получить услуги без оплаты посредством технических манипуляций с устройствами или электронными элементами устройств. Такое поведение обычно криминализуется с помощью конкретных уголовно-правовых положений, однако в ряде случаев его можно отнести к категории, соответствующей классическим положениям, характеризующим мошенничество или подлог. Вторая группа связана со злоупотреблением платежными документами. Преступник, совершая махинации с электронной банковской карточкой или используя поддельные карточки либо ложные коды, пытается получить незаконную финансовую выгоду. Такие деяния могут охватываться конкретными уголовно-правовыми положениями или классическими положениями, характеризующими мошенничество и подлог, в которые могут вноситься поправки в смысле, указанном в пункте 19.

21. Правонарушения, связанные с использованием компьютеров, включают в себя предоставление, информирование и распространение определенных материалов, а в некоторых случаях лишь их хранение. Для совершения подобных правонарушений не требуются электронные сети; в таких случаях сети могут использоваться правонарушителем в целях повышения эффективности преступления или осуществления попыток избежать правосудия. В связи с составом правонарушений следует проводить различие между таким составом, который является противоправным по своему характеру или значению, и составом, который не обязательно сам по себе является незаконным, но приобретает уголовный характер в условиях его распространения. Последняя категория включает нарушение авторских прав и продажу запрещенных товаров или услуг, таких как оружие, наркотики, краденые товары, непрописанные лекарства и доступ к базам азартных игр. Другая категория состава преступлений связана с сообщениями, носящими клеветнический характер, влекущими за собой подрывные или иные противоправные действия либо являющимися оскорбительными в силу их религиозного, дискриминационного с расовой точки зрения или порнографического характера. Степень криминализации таких деяний национальными законодательствами существенно варьируется. В большинстве случаев такие правонарушения предусмотрены существующим законодательством, и в данном случае возникает вопрос о применимости такого законодательства к новой электронной среде.

22. Существует всеобщее согласие в отношении позиций и норм, осуждающих распространение детской порнографии. Такие международные органы, как Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) и Европейский союз, рекомендовали странам, в которых распространение таких материалов еще не объявлено незаконным, принять соответствующие уголовно-правовые положения. Многие государства разрабатывают или уже приняли законы о детской порнографии. Национальные и международные органы полиции уделяют также повышенное внимание расследованиям в связи с детской порнографией.

23. Что касается правонарушений, связанных с материалами, содержащими подстрекательство к ненависти или дискриминации, то по самым различным причинам в мировых масштабах достигнут меньший консенсус в отношении необходимости применения уголовного законодательства к их распространению. Такая ситуация может измениться, если

международное сообщество повысит уровень осведомленности о негативных последствиях такого поведения.

24. Распространение незаконных материалов породило дискуссию о роли и обязанностях поставщиков услуг Интернет. Помимо ряда законодательных инициатив, имеющих своей целью определение и разграничение обязанностей поставщиков услуг, на национальном и международном уровнях наблюдается тенденция предоставлять поставщикам услуг юридический статус, аналогичный статусу традиционных операторов телекоммуникационных служб. Это означает, что поставщики услуг Интернет, как правило, не несут никаких юридических обязательств, связанных с мониторингом и, возможно, блокированием оборота данных, перемещаемых с помощью их компьютерных систем. Тем не менее поставщики услуг Интернет в целом обязаны принимать все разумные меры для предотвращения дальнейшего распространения незаконных материалов, если им становится известно об их характере[6]. В связи с применением к поставщикам услуг Интернет внутреннего законодательства могут возникать неопределенности и в связи с другими аспектами, в том числе такими, как степень возможной гражданской ответственности за передачу незаконного содержания и степень, в которой поставщики услуг Интернет обязаны сотрудничать с правоохранительными органами путем предоставления информации для целей проведения конкретного уголовного расследования или оказания иной помощи.

IV. Уголовное расследование киберпреступлений

25. Как указано выше, к категории киберпреступлений может быть отнесено любое преступление, совершенное с использованием электронных средств или совершенное частично или полностью в электронной среде. Расследование уголовных дел в электронной среде направлено против таких преступлений. В то же время в электронной среде могут также сохраняться следы или доказательства других преступлений. Поэтому расследование уголовных дел в электронной среде не будет ограничиваться киберпреступностью в смысле, используемом в предыдущей главе, а будет охватывать расследование любого преступления, в связи с которым необходимо получить в электронной среде (потенциальные) доказательства.

26. Для проведения уголовных расследований в электронной среде необходимы специальные технические знания и опыт, надлежащие процедуры и достаточные юридические полномочия. В рекомендациях Совета Европы 1989 и 1995 годов (R (1989) 9 en R (95) 13) подчеркивается необходимость создания в рамках национальных правоохранительных органов специализированных подразделений по проблемам компьютерной преступности. Такие подразделения должны быть должным образом укомплектованы кадрами и оснащены соответствующим оборудованием и средствами программного обеспечения. Программы подготовки кадров должны обеспечивать наличие подготовленного персонала, обладающего новейшими техническими знаниями. Во многих государствах такие подразделения по проблеме компьютерной преступности уже созданы. В ряде государств подготовлены руководства, содержащие технические, судебные и процессуальные инструкции, касающиеся путей проведения расследования, позволяющих сократить объем утраченных доказательств и обеспечивающих их приемлемость в суде.

27. Некоторые национальные подразделения полиции "патрулируют" Интернет. Разработаны также специальные средства программного обеспечения для выявления таких преступлений, как хакерство и распространение детской порнографии (см. программное обеспечение, разработанное совместно с Европейским союзом, органами полиции Швеции в целях выявления детской порнографии <http://www.techweb.com>). Учитывая огромный объем информации, имеющейся в международных компьютерных сетях, разработка таких средств программного

обеспечения, которые основаны на структуре распознавания, представляется абсолютно необходимой.

28. Существуют два метода получения данных из компьютерной системы, основанные на технических и правовых критериях. В первом случае данные получают в результате обыска помещений или места, где размещена система. Второй из них предполагает перехват или мониторинг данных, передаваемых в систему, из системы или в рамках системы. В настоящем документе не рассматриваются юридические полномочия на обыск помещений. Предполагается, что такие юридические полномочия будут охватывать право на обыск компьютерной системы, расположенной в определенном месте. Перехват может осуществляться извне техническими средствами системы или с помощью элементов, включенных в систему с этой целью.

29. Традиционное уголовно-процессуальное право, как правило, предусматривает наложение ареста на все компьютерные системы и их замораживание, равно как и в отношении любых других доказательств. В то же время, если это не представляется возможным, надлежащие юридические полномочия для расследования содержания компьютерной системы против воли владельца (владельцев) могут отсутствовать. Наложение ареста на всю компьютерную систему может быть невозможным с технической точки зрения или может быть непропорциональной мерой в условиях среды с большим числом пользователей и заинтересованности таких пользователей в содержании данных. Традиционных полномочий может быть недостаточно для того, чтобы попытаться обеспечить защиту данных для проведения конкретных расследований по таким причинам, как: a) проблемы, связанные с получением доступа к компьютерной системе; b) нематериальный характер данных; и c) тот факт, что данные могут храниться в соединенной системе, размещенной за пределами помещений, подвергаемых обыску.

30. Если в помещениях, подвергаемых обыску, находится компьютерная система, то законом, как правило, допускается получение правоохранительными органами доступа к ней и права на ознакомление с ее содержанием. Об этом может идти речь, если данная система функционирует, заинтересованное лицо добровольно открывает ее или если в помещении обнаружены средства, обеспечивающие доступ. Во всех других обстоятельствах возникает вопрос о том, предусмотрено ли законом право получения правоохранительными органами доступа к системе против воли заинтересованного лица.

31. Компьютерные системы, программы или содержащие данные файлы могут быть защищены в целях предотвращения несанкционированного доступа. В таких случаях доступ обеспечивается, как правило, на основе процедур идентификации и опознания, предусматривающих введение пользователем пароля вручную или с использованием электронной карточки-микропроцессора, на основе обоих этих способов или с согласия на проверку биометрических стандартов. Защита данных обычно предусматривает их кодирование, которое обеспечивает установление личности и защиту конфиденциальности, а также использование алгоритма кодирования и одного или нескольких ключей защиты. В данном случае возникает серьезный риск того, что без добровольной помощи со стороны администратора системы или уполномоченного лица будет невозможно получить доступ ни к компьютерной системе, ни к необходимым данным. Поэтому в соответствии с рядом законов предусмотрено, что администраторы системы должны обеспечивать доступ к системе или данным, а несоблюдение таких требований влечет за собой привлечение к ответственности за нарушение судебных норм. В то же время такие законы могут быть неприменимыми, если оператор системы является также подозреваемым в совершении преступления лицом, поскольку это нарушало бы нормы или принципы, запрещающие самообвинение. Лица, имеющие иные юридические основания не сотрудничать с правоохранительными органами, такие как родственники подозреваемого лица, или лица, имеющие служебные обязательства хранить тайну, также могут освобождаться от применения таких норм. В некоторых случаях в условиях

отсутствия какого-либо лица, которому можно отдать приказ оказывать содействие, в таких целях может привлекаться любое другое лицо (как правило, внешний эксперт). Если данные закодированы, то недостаточно просто получить доступ. В таких случаях законодательство может предусматривать необходимость дальнейшего сотрудничества для преобразования данных в пригодный для чтения формат.

32. Данные сами по себе нематериальны, поэтому традиционные полномочия, касающиеся наложения ареста, как правило, неприменимы. В ходе уголовного расследования на материальные предметы может накладываться арест и они изымаются либо принимаются меры, обеспечивающие, что лишь следственные органы могут распоряжаться такими предметами. В случае данных обычно достаточно делать копии. В то же время, если данные представляют опасность, являются незаконными или ценными и если существует возможность нанесения пострадавшей стороне или следствию дополнительного ущерба, может возникать необходимость в принятии дополнительных мер. Для урегулирования такой ситуации в законодательстве могут предусматриваться полномочия, позволяющие следственным органам стирать данные или препятствовать их дальнейшему использованию. В целях защиты данных может требоваться их копирование для последующего восстановления в первоначальном состоянии по распоряжению судьи. Если заинтересованное лицо подает жалобу, связанную с копированием и дальнейшим использованием данных, в законодательстве может содержаться требование относительно выдачи официальной справки об изъятых данных.

33. Обыск компьютерной системы обычно происходит в рамках обыска помещений или иных мест. Правомочие на производство обыска обычно ограничено физическими границами места, подвергаемого обыску. Компьютерная сеть может размещаться и не в одном месте, а быть соединена с другими частями сети посредством постоянных или периодически включаемых линий связи. В таких случаях возникает вопрос о том, допускается ли законом обыск в соединенных системах, если такие системы расположены вне помещений, подвергаемых обыску. Если не производить тщательный обыск, возникает риск уничтожения данных в период, пока будет получено разрешение на дополнительный обыск места, где данные физически размещены. В крупных сетях может быть практически невозможно установить точное физическое местоположение данных.

34. Ниже в сжатой форме изложены правовые основания, дающие право проводить тщательный обыск. Лицо, проживающее в помещениях, подвергаемых обыску, имеет право получать доступ к соединенной компьютерной системе и использовать ее функции и возможности хранения данных. Такое лицо может осуществлять контроль над данными, не покидая свои помещения. В момент обыска такое лицо несет юридическое обязательство предоставить для целей обыска помещения, физически находящиеся под его или ее контролем. Можно утверждать, что аналогичные правила должны применяться к данным, к которым данное лицо имеет фактический доступ, даже если эти данные могут находиться в других местах. Из этого может следовать, что рамки такого тщательного обыска будут ограничены действиями, которые данное лицо имеет право предпринимать в отношении подсоединенной системы и данных, и права этого лица не могут ущемляться в большей степени, чем это допускается базовым обыском. Такие полномочия могут быть ограничены случаями расследований серьезных преступлений или случаями, когда необходимо принять срочные меры для предотвращения утраты доказательств, либо в обоих таких случаях. Когда подсоединенная система или данные, представляющие интерес для целей обыска, размещены в иностранном государстве, могут применяться и другие ограничения (см. пункт 59 ниже).

35. В связи с поиском и отбором данных в компьютерной системе возникает ряд дополнительных правовых проблем. Первая из них заключается в том, насколько конкретным должно быть судебное распоряжение в отношении характера и формата представляющих интерес данных, не выходя за рамки законности. Национальным законодательством в данном

случае могут предусматриваться различные ограничения. Кроме того, неукоснительное и четкое исполнение судебного распоряжения может требовать непропорционально большого объема времени, в результате чего правоохранительные органы могут копировать такое количество данных, которое представляется целесообразным для проведения дальнейшего анализа. Подобная практика может быть разрешена или запрещена национальным законодательством. Другой важный вопрос заключается в том, необходимо ли информировать заинтересованное лицо о копируемых и изымаемых данных, насколько подробная информация должна представляться и должно ли такое лицо иметь юридическое право оспаривать изъятие данных. Еще одна проблема возникает в том случае, если данные носят конфиденциальный характер или пользуются иной правовой защитой. Вопрос состоит в том, каким образом можно идентифицировать и защитить такие данные в случаях, когда правоохранительные органы копируют значительный массив данных для дальнейшего изучения.

36. Следует также отметить, что данные могут иметь недолговечный характер. Их легко изъять, стереть или изменить, не оставляя четких следов. Распределенная обработка данных - это не единственный фактор, обусловливающий недолговечность данных. Электронная обработка данных предполагает обработку значительных массивов данных недолговечного характера, стираемых как только потребность в них исчезает. В качестве примеров таких данных можно привести файлы регистрации и данные коммуникационного обмена. При отсутствии информации о "первоначальном" наборе данных (если этот термин имеет какое-либо значение в обработке данных) трудно выявить манипуляции и невозможно будет восстановить уничтоженные файлы, если не обеспечивается сохранение исходной дублирующей информации. В связи с характером данных возникают проблемы, если идет речь о физическом обыске:

a) в большинстве случаев для поиска данных, хранимых или передаваемых в электронной среде, необходима оперативность и своевременность, с тем чтобы предотвращать создание помех для такого поиска или модификацию данных;

b) необходимо принимать особые меры предосторожности, позволяющие представлять данные в качестве доказательства в суде. Необходимо устанавливать целостность данных с момента загрузки или копирования из компьютерной системы, подвергаемой обыску, до их использования в суде.

37. Проведение технических и правовых различий между изъятием хранимых данных и перехватом данных, передаваемых с помощью сети, также стало весьма трудной задачей. Данные обрабатываются с помощь компьютерной системы, иногда именуемой устройством для автоматизированной обработки данных. Обработка данных включает в себя ввод, передачу на периферийное оборудование (например, видеоэкран) и промежуточную среду хранения, фактическую обработку, передачу результатов на периферийное устройство для хранения и конечный результат или дальнейшую передачу на другие системные компоненты. Перехват данных в компьютерной системе обычно сводится к поиску хранимых в памяти данных, который осуществляется за счет использования системных функций или конкретных компьютерных программ. Поиск передаваемых данных может осуществляться с помощью системных средств (мониторинг), если это предусмотрено, или путем технического перехвата потока данных в средствах передачи. Поскольку во многих случаях данные одновременно могут находиться в стадии как хранения, так и передачи, либо зачастую переходить из одной стадии в другую, работники следственных органов легко смогут воспользоваться приемами изъятия или перехвата для получения одних и тех же данных. В этой связи могут возникать проблемы правового характера, поскольку стандарты или гарантии, применимые к перехвату сообщений и изъятию хранимых данных, во многих государствах могут быть неодинаковыми. Перехват данных на стадии их передачи нередко подпадает под более жесткий стандарт, так как перехват представляет собой скрытную операцию, его целью могут быть данные, отсутствовавшие в момент выдачи разрешения на обыск или в момент его начала, и в большинстве случаев

заинтересованным сторонам не известно о перехвате и их могут информировать о перехвате лишь спустя длительный период времени или вообще не информировать об этом. Тот факт, что сетевые данные могут либо изыматься, либо перехватываться, в некоторых случаях может ущемлять права подозреваемых лиц, поскольку это позволяет правоохранительным органам применять менее ограничительные правомочия на производство обыска при проведении определенных операций, приближающихся по своему характеру к перехвату.

38. В отношении электронных данных, копируемых из файлов данных или регистрируемых при передаче данных, необходимо, как правило, принимать особые меры предосторожности и иные меры с целью сохранения их в качестве доказательства в суде, если они вообще могут использоваться как таковые. В рамках многих правовых систем в соответствии с принципом одновременности, предусматривающим, что все доказательства подлежат представлению в суде, необходимо, чтобы доказательственные материалы соответствовали исключительно высоким стандартам. В некоторых странах могут действовать формальные требования, ограничивающие или не допускающие использование электронных данных в качестве доказательств. Согласно некоторым законам, например, материалы должны представляться в письменной форме, с тем чтобы их можно было зачитать в суде. В некоторых странах под эту категорию не подпадают данные в аудиоформате или в виде изображений, и поэтому такие данные становятся неприемлемыми. На неприемлемость также, как правило, могут повлиять любые сомнения в достоверности доказательных материалов. Поскольку электронные данные можно без труда модифицировать, не оставив следов, это создает серьезные проблемы для правоохранительных органов в процессе сбора таких доказательств в соответствии с прозрачными и надежными процедурами, позволяющими устанавливать их подлинность. Для проверки подлинности суд должен быть в состоянии проанализировать надежность процесса копирования и регистрации доказательств, начиная от первоначального носителя данных или канала данных. Суд должен также быть в состоянии проверить a) действенность процедуры сохранения данных и надежность самого процесса сохранения; b) любой анализ материала; и c) соответствие представленных в суд материалов тем материалам, на которые первоначально был наложен арест и которые были защищены.

39. В дополнение к обычным или устанавливаемым исполнительной властью полномочиям на обыск помещений во многих правовых системах допускается вынесение судебных распоряжений о предъявлении материальных предметов. В некоторых случаях могут также предусматриваться параллельные полномочия издавать распоряжение относительно представления конкретных данных. Такие полномочия могут быть ограниченными и обусловленными конкретными положениями, не применимыми к обычным распоряжениям о представлении материальных предметов, с тем чтобы они не могли использоваться в качестве средства для получения какой-либо иной, кроме конкретно оговоренной, информации. Без таких мер контроля, в частности, в соответствии с распоряжением частное лицо может быть обязано собирать, обрабатывать или отбирать любые другие данные, помимо хранящихся данных и данных, находящихся под его или ее контролем. Такое обязательство выходило бы за рамки и смысл распоряжения о представлении материальных доказательств. При направлении запроса на выдачу распоряжения о представлении материальных доказательств и в процессе его исполнения было бы, возможно, полезным для правоохранительных органов включать не только данные, представляющие интерес, но и файлы регистрации компьютерной системы. В таких файлах регистрируются все операции в системе в хронологическом порядке, фиксируется информация о таких параметрах, как время, продолжительность и терминалы, с которых был осуществлен доступ к данным или их изменение.

40. Согласно традиционным законам многих стран допускается выдача судебным или иным органом распоряжения, касающегося перехвата и последующей записи телекоммуникаций в публичных сетях. Некоторые страны распространили такие полномочия на частные сети, конкретные новые виды телекоммуникаций, такие как мобильные системы или спутниковые

системы связи и компьютерные сети. Такие законодательные меры обосновываются тем, что если сообщения поддаются перехвату в рамках одной сети, но это невозможно в других сетях, то преступники будут использовать такую систему, которая обеспечивает минимальный риск перехвата правоохранительными органами. Для законного перехвата конкретных сообщений требуются специальные технические средства, в том числе четкая юридическая основа для установки таких средств и оперативное исполнение судебного распоряжения осуществлять перехват.

41. Для идентификации подлежащих перехвату сообщений и лиц, участвующих в передаче таких сообщений, необходимо сотрудничество операторов сетей, в частности операторов телекоммуникационных сетей и поставщиков услуг Интернет. Информацией о подписчиках владеют лишь такие операторы. При необходимости в национальном законодательстве может предусматриваться юридическое обязательство о предоставлении операторами и поставщиками услуг данных о подписчиках незамедлительно по распоряжению компетентных органов. Четкие юридические обязательства такого рода призваны обеспечивать также защиту частных лиц и компаний от гражданской ответственности перед своими подписчиками.

42. Операторы телекоммуникационных сетей и поставщики услуг Интернет, как правило, располагают данными об информационном обмене сообщениями в прошлом, которые можно получить с помощью оборудования, регистрирующего конкретные аспекты информационного обмена, включая время, продолжительность и дату любого сообщения, участвующие стороны и вид услуг или деятельности. (Прослеживается параллель с примером, приведенным в пункте 37 выше, относительно файла регистрации компьютерной системы.) Такие данные хранятся обычно в течение ограниченного периода времени, зависящего от коммерческих потребностей оператора или поставщика услуг, а также юридических (в Европейском союзе) или коммерческих требований, касающихся неразглашения частной информации. Национальное законодательство многих стран разрешает правоохранительным органам или судебным органам издавать распоряжение, касающееся сбора данных информационного обмена будущими сообщениями. В то же время в тех случаях, когда данные информационного обмена являются частью сообщения, например "шапка" сообщений, передаваемых по электронной почте, сбор таких данных может рассматриваться как перехват самого сообщения и по этой причине подпадать под юридические ограничения. В других случаях сбор данных информационного обмена без перехвата содержания самого сообщения может считаться меньшим вторжением в частную жизнь заинтересованных людей и поэтому менее жестко регулироваться в правовом отношении.

43. В случаях, связанных с хакерством или несанкционированным электронным доступом, возникает конкретная необходимость оперативного перехвата электронного сообщения, а также оперативного получения доступа к данным информационного обмена и данным о подписчиках, с тем чтобы отследить источник сообщения, сохранить данные и в конечном счете застать преступника на месте преступления и получить конкретные доказательства. В случае введения уголовной ответственности за хакерство в соответствии с рядом законов такие действия могут и не считаться достаточно серьезным преступлением, оправдывающим применение мер перехвата. Схема действий хакеров, как правило, связана с совершением других более серьезных деяний, которые могут быть выявлены в момент обнаружения их действий. Это может считаться еще одной причиной, допускающей перехват в случаях несанкционированного доступа в источники электронной информации.

44. Перехват электронного сообщения может быть затруднен фактом кодирования сообщений. Использование кодирования позволяет устанавливать подлинность сообщения, идентифицировать отправителя и определять целостность сообщения. Вторая функция кодирования состоит в обеспечении конфиденциальности сообщения (путем его защиты от прочтения третьими сторонами). Возможная политика в области кодирования обсуждается в

последнее время рядом международных организаций. Стороны, заинтересованные в оказании содействия правоохранительным органам и органам, ведущим борьбу с преступностью, испытывают озабоченность в связи с трудностью получения законного доступа к закодированным данным, а стороны, заинтересованные в обеспечении неприкосновенности частной жизни и охране коммерческих интересов, стремятся использовать кодирование для защиты личной и коммерческой информации.

45. Многие из тем таких обсуждений выходят за рамки настоящего доклада, однако в данном контексте заслуживают рассмотрения два конкретных вопроса. Некоторые занимающиеся вопросами кодирования страны изучают возможность введения контроля за распространением шифровальных продуктов, с тем чтобы лишить группы преступников или террористов возможности получать к ним доступ, используя, в частности, лицензионные требования в отношении продуктов, достаточно "защищенных", что затрудняет доступ к ним сотрудников правоохранительных органов. Некоторые страны пытаются также применять практические меры, стремясь обеспечить законный доступ к закодированным электронным сообщениям. Круг таких мер включает использование специальных компьютерных микросхем, системы хранения у третьих сторон (в которых сообщения хранятся у доверенных третьих сторон, с помощью которых на них может быть наложен законный арест в целях получения доступа) или специальные усилия по расшифровке закодированных сообщений с использованием технических средств. Осуществлению такой политики препятствуют технологические трудности и сторонники неприкосновенности частной жизни и защиты коммерческих интересов.

46. Обеспечение доступа к зашифрованным сообщениям или хранящимся данным в ходе уголовного расследования представляет очевидный интерес для правоохранительных органов всех стран. Меры, направленные на частичное решение этой проблемы, уже могут приниматься в некоторых странах. Во многих случаях операторы телекоммуникационных и электронных сетей самостоятельно используют кодирование для защиты собственных систем и сообщений своих клиентов. В тех случаях, когда такие операторы несут юридическое обязательство сотрудничать с правоохранительными органами в перехвате конкретных сообщений, представляется разумным исходить из того, что такое обязательство включает (или могло бы включать) обязанность снятия любой использованной ими в этом случае кодировки. Однако такая обязанность не будет распространяться на кодировку, примененную непосредственно клиентом, которую, как правило, оператор не в состоянии расшифровать. Еще один возможный вариант заключается в рассмотрении национальными законодателями возможности возложить на лица, участвующие в использовании зашифрованной связи, обязательство обеспечивать дешифровку по распоряжению компетентного судебного органа. В целях защиты от самообвинения такое распоряжение не должно использоваться в отношении подозреваемых или иных лиц, к которым применяется освобождение от юридической ответственности.

47. Как указано в пункте 37 выше, в большинстве стран проводится различие между перехватом передаваемых данных и наложением ареста на хранимые данные, однако такое разграничение сомнительно в случае электронной почты, поскольку в такой почте комбинируются как передача данных, так и их хранение. В момент отправления сообщения оно передается поставщиком услуг отправителя поставщику услуг адресата. Сообщение после его получения хранится в почтовом ящике адресата до его открытия. Адресат имеет доступ к сообщению и определяет продолжительность его сохранения в почтовом ящике. Таким образом, находящиеся в почтовом ящике сообщения контролируются как адресатом, так и поставщиком услуг, и правоохранительные органы могут, как правило, получить доступ к ним, применив в отношении любой из сторон меры принудительного характера. Предпочтительным, по их мнению, являются действия в отношении поставщика услуг Интернет, поскольку при этом адресату ничего не известно о возбуждении расследования. В таких случаях правомочия на перехват сообщения и проведение физического обыска помещений и любых расположенных в них компьютеров вполне могут становиться взаимозаменимыми. В этом контексте может

ставиться под сомнение правомочность распоряжения представлять имеющиеся сообщения и сообщения, поступающие в течение определенного периода времени, если такое распоряжение не соответствует юридическим стандартам (обычно более высоким) для перехвата. Тот факт, что данные контролируются одновременно поставщиком услуг и клиентом, также может вызывать постановку вопросов, связанных с тем, чьи права на частную жизнь, имущество или прочие права или интересы должны учитываться при получении юридического разрешения на проведение обыска или осуществление перехвата.

V. Международное сотрудничество национальных правоохранительных органов

A. Формы сотрудничества и международные инициативы

48. С учетом международных масштабов электронных сетей становится все менее вероятным, что все элементы киберпреступности будут ограничены территорией отдельного государства. В процессе проведения расследований правоохранительные органы различных государств должны будут сотрудничать между собой, причем как официально, используя такие рамки и структуры взаимной правовой помощи, как Международная организация уголовной полиции (Интерпол), так и неофициально, предоставляя потенциально полезную информацию непосредственно органам другого государства. В целом международное сотрудничество органов полиции предполагает предварительное согласие органов заинтересованных государств. В зависимости от отношений между заинтересованными государствами, характера соответствующей информации или других факторов может также возникать потребность в разработке полномочий и процедур в международном соглашении.

49. В 1997 году на встрече Группы восьми стран в составе глав правительств Группы семи ведущих промышленно развитых стран и Российской Федерации был принят ряд правовых принципов и общий план действий по борьбе с так называемыми "преступлениями с использованием высоких технологий"[7]. В этих документах содержится ряд предложений, касающихся практического сотрудничества между правоохранительными органами, а также разработки правовых принципов взаимной правовой помощи. Круг обсужденных элементов практического сотрудничества включал в себя следующее:

a) меры, направленные на обеспечение наличия достаточного числа подготовленных сотрудников, имеющих достаточный опыт сотрудничества в области оснащения и подготовки персонала правоохранительных органов;

b) сотрудничество в разработке судебных стандартов поиска и установление подлинности электронных данных.

50. В целях содействия своевременному реагированию на просьбы об оказании помощи, поступающей от другого государства, Группа восьми стран постановила создать систему контактных пунктов, действующих круглосуточно и без выходных ("24 часа/7 дней"), которая в настоящее время создана. Функции этих контактных пунктов весьма многогранны. По запросу контактные пункты будут предоставлять фактическую информацию, которая может способствовать распространению следственных действий на другое государство или опираться на его помощь и принимать все другие необходимые меры с целью скорейшего реагирования на официальную просьбу об оказании правовой помощи или принимать необходимые меры, предусмотренные национальным законодательством, до получения такой просьбы. Указанные контактные пункты не ограничены Группой восьми стран, а созданы также на добровольной основе во многих других государствах. В некоторых странах создание таких специализированных подразделений неосуществимо из-за отсутствия специальных знаний и опыта или финансовых ресурсов. В других государствах борьба с киберпреступностью может

не входить в число приоритетных задач. Очевидно, что чем большее число государств будет готовить и соответственно оснащать персонал и предоставлять соответствующие услуги на круглосуточной основе, тем более эффективной будет такая система.

51. В рамках Интерпола создано несколько рабочих групп экспертов по преступности, связанной с информационной технологией. Европейская рабочая группа по преступности, связанной с информационной технологией, разработала руководство по компьютерной преступности (имеется на CD-ROM). В нем содержатся инструкции с изложением путей расследования случаев, связанных с компьютерной преступностью, описание средств и методов поиска и защиты электронных материалов, а также информация о соответствующих материальных и процессуальных правовых нормах различных стран. Рабочие группы занимаются разработкой конкретных средств программного обеспечения в целях выявления конкретных преступлений в сети Интернет. Проведен ряд учебных курсов для сотрудников следственных органов, занимающихся компьютерными преступлениями.

52. Организация Объединенных Наций опубликовала Руководство по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними, целью которого являются согласование как материального, так и процессуального права, а также международное сотрудничество в борьбе с преступностью, связанной с использованием компьютеров. В Руководстве содержится глава, посвященная информационной безопасности и предупреждению киберпреступности[8].

53. Внимания заслуживают как согласованные подходы, так и подходы, основанные на инициативах, принимаемых отдельными государствами, и необходимо в максимально возможной степени использовать преимущества обоих подходов. В этой связи важное значение имеет проведение на регулярной основе международных совещаний, позволяющих представителям подразделений, занимающихся вопросами киберпреступности, встречаться и обмениваться практической информацией и опытом. Улучшению обмена информацией могут способствовать и другие постоянно действующие средства, такие как банки данных, информационные web-узлы и дискуссионные группы[9].

54. Третий элемент плана действий Группы восьми стран согласован на основе сотрудничества между промышленностью и государством и охватывает следующие аспекты:

a) содействие разработке нормотворческими органами стандартов, призванных обеспечить надежность и безопасность телекоммуникаций и технологий обработки данных;

b) разработку информационных и телекоммуникационных систем, способных выявлять злоупотребления в сетях, отслеживать лиц, совершающих такие злоупотребления, и собирать соответствующие доказательства.

Поскольку уголовные расследования в компьютерной среде могут создавать проблемы для промышленности, важно и необходимо сотрудничать и координировать действия с промышленным сектором. Такая деятельность охватывает многие аспекты - от информационной безопасности и разработки продуктов до фактического сотрудничества в исполнении судебных распоряжений. Переговоры между правительственными органами и промышленными организациями могут осуществляться в рамках секторальных договоренностей или других не имеющих обязательную юридическую силу или подлежащих исполнению соглашений.

B. Договоры о взаимной правовой помощи и другие международные договоры

55. Развертывание международного сотрудничества в рамках взаимной правовой помощи требует заключения международного соглашения или иной аналогичной договоренности, например законодательство, основанное на принципах взаимности. Подобные правовые положения как многостороннего, так и двустороннего характера возлагают на органы участвующих сторон обязательства реагировать на просьбу об оказании правовой помощи в согласованных случаях. Исполнение такой просьбы допустимо лишь в том случае, если она соответствует внутреннему праву запрашиваемого государства или, при отсутствии конкретных норм, если такая просьба не противоречит внутреннему праву.

56. Эффективность сотрудничества государств в вопросах уголовного права повышается, если они разделяют общие интересы, отраженные во взаимных уголовных статутах или кодексах либо в практике обеспечения исполнения уголовного законодательства в соответствующих государствах. В рамках многих международных конвенций по вопросам уголовного права общие интересы воплощены в норме "двойной преступности". Государство не может сотрудничать с другим государством в отношении расследования и судебного преследования определенных деяний, не криминализованных в запрашиваемом государстве. В принятых ранее конвенциях отсутствие "двойной преступности" является поэтому основанием для отказа в помощи. В принятых позже конвенциях такая формальная оговорка не предусмотрена, но содержится критерий целесообразности. Может считаться нецелесообразным удовлетворять просьбу об оказании правовой помощи, если, например, данное преступление заключается в совершении незначительного правонарушения или касается определенного вида поведения, не криминализованного в запрашиваемом государстве.

57. Следовательно одним из путей совершенствования международного сотрудничества в вопросах уголовного права является согласование определенных материальных норм уголовного права. В силу различий культурного, социального и экономического характера между государствами политика в области уголовного правосудия может быть разной. В этом отношении меньшие проблемы могут возникать в ходе международных переговоров, направленных на согласование правонарушений, связанных с обеспечением конфиденциальности, целостности и наличия данных (см. пункт 15), в частности обсуждением положений технологического характера, чем в связи с намеренным согласованием правонарушений по их содержанию, поскольку они затрагивают права человека (например, свобода выражения). Как представляется, исключением, доказывающим такое правило, является детская порнография, в отношении борьбы с которой имеется широкий консенсус.

58. В настоящем контексте взаимная правовая помощь затрагивает любой вид правовой помощи. Как правило, такая помощь связана с конкретными полномочиями на принудительные действия в связи с расследованием киберпреступлений. Помимо просьб об оказании традиционной помощи, предусматривающей, в частности, допрос свидетелей, ее цель заключается в получении определенных данных, хранящихся в компьютерной системе, расположенной на территории другого государства, или передаваемых электронным способом через сеть и поддающихся мониторингу или перехвату на территории указанного государства.

59. Государства определяют в своем национальном законодательстве, какие из их полномочий могут применяться при оказании помощи другим подписавшим соответствующий документ государствам. Государства не всегда предоставляют возможность использовать все внутренние средства в интересах расследования уголовных дел другими подписавшими государствами. В некоторых случаях помощь может оказываться в рамках того или иного конкретного дела с учетом взаимных интересов соответствующих государств на исключительной, а не на регулярной или обычной основе. Взаимная правовая помощь в конечном счете регулируется также в рамках международного права принципом взаимности. По этой причине, а также по

иным соображениям государства в процессе переговоров о рамках взаимной правовой помощи с другими государствами не всегда проявляют готовность в полной мере использовать возможности, допускаемые внутренним правом. Двойная преступность - требование, согласно которому правонарушение, в связи с которым запрашивается помощь, должно квалифицироваться как преступление в обоих заинтересованных государствах, - может также напрямую или косвенно использоваться в качестве основы для отказа в оказании взаимной правовой помощи. Кроме того, в международных соглашениях об оказании взаимной помощи могут содержаться исключения, касающиеся случаев непредоставления такой помощи. Исключения представляют определенные виды правонарушений, такие как фискальные, политические или военные преступления, а также преступления, не считающиеся достаточно серьезными (в силу потенциальных предусмотренных мер наказания), с тем чтобы оправдать затраченные усилия.

60. В связи с правовой помощью при расследовании международной киберпреступности могут возникать дополнительные проблемы. Если в соответствии с внутренним правом одной из сторон не предусмотрены конкретные полномочия на поиск доказательств в электронной среде, такая сторона не в состоянии реагировать (или адекватно реагировать) на просьбу об оказании помощи. По этой причине важным условием международного сотрудничества является согласование полномочий принимать принудительные меры.

61. Кроме того, вопрос об оказании взаимной правовой помощи может носить более безотлагательный характер в случае киберпреступлений, чем при расследовании обычных дел, поскольку, если электронные доказательства не будут защищены оперативно, потенциально это может привести к утрате электронных данных. В то же время принятие безотлагательных мер не всегда может быть возможным по формальным или практическим соображениям. Для принятия необходимых мер может требоваться, например, судебное распоряжение в запрашиваемом государстве. Во избежание утраты доказательств в таких случаях можно разрабатывать системы оперативных предварительных мер, требующих соблюдения минимально возможных формальностей, за которыми могут следовать более привычные разбирательства, как только данные будут защищены в целях определения целесообразности их передачи запрашивающему государству. В соответствии с такой системой внутренним законодательством могли бы предусматриваться как защита данных по неофициальному запросу, так и их сохранение до получения официальной просьбы об их разглашении в соответствии с соглашением о взаимной правовой помощи. Если такая просьба не поступает в надлежащие сроки или если такая просьба отвергается как несоответствующая, защищенные данные будут уничтожаться. Возможно создание аналогичной системы в связи с сохранением данных информационного обмена хранимых операторами телекоммуникационных сетей и поставщиками услуг Интернет.

62. Международные компьютерные сети позволяют осуществлять деятельность на такой территории, где может действовать (намеренно или непреднамеренно) принцип экстерриториальности. Например, правоохранительные органы одного государства могут получать данные из компьютерной сети в рамках правомерного поиска компьютерной информации в этом государстве, но при этом устанавливать, что некоторые из полученных данных были сохранены в рамках сети другого государства и защищены законами этого государства. Аналогичным образом государство может правомерно перехватывать электронные сообщения, проходящие через ее территорию, даже если такими сообщениями обмениваются лица, расположенные в других государствах, где они пользуются правовой защитой от произвольного вмешательства такого государства в сферу частной связи. Работающие в сети сотрудники правоохранительных учреждений также могут осуществлять скрытные действия в соответствии с законодательством своих стран на условиях, в которых такие действия или методы не допускались бы законодательством других государств, где они действуют. Все эти сценарии являются новыми и не имеют параллелей, и в международном праве в настоящее

время не предусмотрены оказание существенной помощи или рекомендации в отношении решения возникающих проблем.

63. Кроме того, в настоящее время отсутствует широкий консенсус в отношении возможного устранения трансграничных последствий правомерно применяемых следственных действий внутреннего характера. Общепризнанно, что государство правомочно применять на своей территории, на которой оно обладает исключительной юрисдикцией, следственные действия или принудительные меры в отношении любых своих граждан. В результате применения таких полномочий могут возникать случаи, когда размещенные на другой территории данные считываются и копируются или, возможно, уничтожаются. С точки зрения государства, в котором велся поиск данных, такие действия могут образовывать состав уголовного преступления в соответствии с внутренним уголовным правом, а также являться нарушением национального суверенитета. В то же время, согласно другому мнению, международное право не запрещает такое вмешательство, поскольку с технической точки зрения такие данные доступны и могут быть получены из государства, осуществляющего их поиск, без какой-либо помощи или вмешательства со стороны государства, где осуществляется поиск таких данных. Имеющиеся в любых разделах сети данные можно рассматривать как общедоступные, и по этой причине вопрос о доступе к ним из любого государства, в котором они в настоящее время находятся, регулируется исключительно внутренним, а не международным правом. С такой точки зрения обращение к государству, где осуществляется поиск данных, не является необходимым ни на одном из этапов деятельности. Согласно международному праву, по-прежнему неоднозначен вопрос о том, в какой мере данные являются или не являются общедоступными (например, лица, осуществляющие поиск данных, должны фактически загружать из их сервера одной страны в другую страну).

64. Что касается мнения, согласно которому любое вмешательство в функционирование компьютерной сети, расположенной на территории какого-либо государства, является нарушением территориальной целостности такого государства, то целесообразно рассмотреть два различных мнения о состоянии международного права. Одно из мнений основано на принципе, согласно которому государства не должны в одностороннем порядке иметь право на поиск, копирование или иную модификацию данных или компьютерных систем, расположенных в другом государстве, на том основании, что аналогичные действия, осуществленные посредством одностороннего физического присутствия, не допускаются. Для получения доказательственных данных от другого государства следует придерживаться действующих процедур взаимной правовой помощи. Это мнение основано на традиционных принципах, но в нем не признаются практические проблемы в связи с расследованием компьютерных преступлений.

65. Более прагматичную точку зрения выдвигают те, кто считает, что международное право в настоящее время не дает четкого ответа на вопросы о нарушениях национальных законов или ущемлении суверенитета. Сторонники этой позиции утверждают, что международное право может формироваться под воздействием достижения международного консенсуса о допустимости таких действий и четкого определения условий, при которых такие действия допускаются. В качестве одного из важных элементов такого решения проблемы предлагается уведомление государства, в котором осуществляется поиск данных.

66. В рамках международного сообщества можно было бы разработать и новые концепции формирования правовой нормы, позволяющей определять права заинтересованных государств в отношении совместного использования наземных, мобильных или спутниковых компьютерных сетей. До разработки такой нормы можно было бы согласовать прагматический подход в форме договора или другого международного документа об определенных процедурах, с помощью которых интересы государства, осуществляющего поиск данных, можно было бы должным

образом сбалансировать с интересами государства, где осуществляется поиск данных, и его населения.

VI. Заключения

67. В связи с растущим числом преступлений, связанных с использованием компьютеров, которому способствует создание глобальных международных и публичных электронных сетей, огромное значение приобретает международное сотрудничество и координация действий в этой области. Основные элементы таких международных действий могут быть основаны на следующих принципах:

a) Повышение осведомленности общественности. Просвещение и повышение осведомленности общественности может приводить к сокращению числа преступлений в электронной среде. Промышленность - изготовители аппаратного и программного обеспечения, поставщики услуг и другие стороны, - организации потребителей и правительства могут взять на себя общую задачу информирования общественности о соображениях безопасности и о других рисках, связанных с открытыми электронными средами, и подготовки соответствующих предложений о возможных путях защиты их интересов.

b) Разработка общей политики в отношении киберпреступности. Транснациональный характер преступности с использованием компьютерной сети дает основания считать, что разработка общей политики по основным вопросам должна быть частью любой стратегии борьбы с преступностью. Такая общая политика имеет важное значение для предотвращения возникновения "информационных убежищ", в частности в рамках тех правовых систем, в которых определенные действия не криминализованы. Разработка общей политики могла бы стать одним из аспектов деятельности Программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия в поддержку работы, уже проводимой международными организациями.

c) Совершенствование мероприятий, проводимых следственными органами. Следует разрабатывать эффективные меры в целях повышения потенциала расследования уголовных преступлений в сетевой среде, особенно в рамках дел, затрагивающих несколько правовых систем. Круг таких мер включает возможность удовлетворения потребностей, возникающих в рамках операций, которые должны проводиться достаточно оперативно во избежание утраты доказательств или доступа к ним. Для обыска компьютерных систем и надзора за компьютерными сетями могут потребоваться дополнительные полномочия, отсутствующие в данный момент в традиционном уголовно-процессуальном праве. Серьезные проблемы, обусловленные неприкосновенностью частной жизни и смежными аспектами, могут также возникать в связи с объемом данных, обнаруженных в компьютерных системах, и степенью возможного доступа к ним лиц, проводящих обыск. В процессе разработки и осуществления новых правомочий необходимо тщательным образом учитывать права человека соответствующих лиц и обеспечивать их сбалансированность.

d) для расследования киберпреступлений требуются персонал, обладающий конкретным судебным и техническим опытом и знаниями, а также наличие конкретных процедур. Для этого необходимо разработать учебную программу и программные средства для расследований. Необходимо разрабатывать международные программы подготовки кадров и обмениваться опытом и знаниями между государствами. Организация Объединенных Наций в рамках Программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия могла бы изучить вопрос о целесообразности пересмотра своего руководства по предупреждению преступлений, связанных с компьютерами, и дальнейшей поддержке работы, уже осуществляемой другими международными организациями.

e) Совершенствование трансграничной координации и помощи. Киберпреступления совершаются в глобальной электронной среде и не всегда ограничены территорией отдельного государства. Для эффективного расследования таких преступлений государства могут нуждаться в помощи со стороны других государств. Такая помощь охватывает как сотрудничество персонала правоохранительных органов в рабочем порядке, так и официальную взаимную правовую помощь, оказываемую через центральные органы. С учетом того факта, что содержащиеся в компьютерных сетях данные могут быть недолговечными, возможность оказания такой помощи на оперативной и эффективной основе приобретает более важное значение, чем в случае многих других правонарушений. Эффективная помощь в расследовании киберпреступлений могла бы опираться на следующие меры:

i) создание контактных пунктов, аналогичных контактным пунктам, созданным Группой восьми ведущих государств, в целях извещения запрашивающих государств о помощи, которая может быть оказана, и в целях принятия мер, необходимых для выполнения запросов в соответствии с нормами внутреннего права;

ii) обзор систем оказания правовой помощи в контексте киберпреступности. Необходимо изучить традиционные потребности и практику в области правовой помощи и на этой основе выяснить, отвечают ли они потребностям проводимых в настоящее время расследований киберпреступлений, а также выявить возможности совершенствования такой помощи. Области, которые следовало бы изучить, охватывают общую адекватность полномочий проводить уголовные расследования в рамках компьютерных сетей, а также возможность принятия оперативных мер в целях защиты данных от имени органов других государств, осуществляющих уголовное расследование.

Примечания

[1] Примеры ассоциаций или обществ включают в себя следующее: Ассоциацию поставщиков услуг Интернет Соединенных Штатов Америки (ЮСИПА), Канадскую ассоциацию поставщиков услуг Интернет (КАИП), Панъевропейскую ассоциацию поставщиков услуг Интернет, включающую ассоциации стран Европейского союза. Имеются национальные ассоциации в ряде таких европейских стран, как Бельгия, Германия, Испания, Италия, Нидерланды, Соединенное Королевство Великобритании и Северной Ирландии и Франция.

[2] http://www/nua.ie/surveys/how_many_online, 18 октября 1999 года.

[3] См. технические определения данных Международной организации по стандартизации.

[4] Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986.

[5] Council of Europe (1989), Recommendation No. R.(89)9.

[6] "Global Information Networks: Realising the Potential", Ministerial Conference, Bonn, July 1997.

[7] См. Коммюнике встречи министров юстиции и внутренних дел восьми промышленно развитых стран, Вашингтон, 9-10 декабря 1997 года <http://www.usdoj.gov/criminal/cybercrine/communiae.htm>. План действий был одобрен главами государств и правительств в 1998 году. План действий был рекомендован другим международным организациям, таким как Организация американских государств и Европейский союз.

[8] Международный обзор международной политики, №№ 43 и 44, 1994 год (издание Организации Объединенных Наций, в продаже под № R.94.IV.5).

[9] Например, the World Justice Information Network <http://www.justinfo.net> или the Police Officer Internet Directory <http://www.officer.com/c_crimes.htm>.

This archiving project is a collaborative effort between the United Nations Office on Drugs and Crime and the American Society of Criminology, Division of International Criminology. Any comments or questions should be directed to Cindy J. Smith at cjsmithphd@comcast.net or Emil Wandzilak at emil.wandzilak@unodc.org.