Организация Объединенных Наций A/CONF.203/14

Одиннадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию

Distr.: General
14 March 2005

Russian
Original: English

Бангкок, 18–25 апреля 2005 года

Пункт 3 предварительной повестки дня*
Эффективные меры по борьбе с транснациональной организованной преступностью

Семинар-практикум 6: Меры по борьбе против преступлений, связанных с использованием компьютеров**

Справочный документ***

Резюме

Распространение по всему миру новых информационно-коммуникационных технологий породило множество различных преступлений, связанных с использованием компьютеров, что чревато угрозой не только для конфиденциальности, целостности или доступности компьютерных систем, но и для безопасности важнейших элементов инфраструктуры. Кроме того, технологические новшества порождают и непохожие друг на друга тенденции в области "криминальной инновации"; соответственно, несхожесть угроз, которые несут в себе преступления, связанные с использованием компьютеров, отражает различия, прослеживающиеся по всему спектру так называемого "разрыва в цифровых технологиях". В ходе борьбы с такого рода преступлениями и перед следователями, и перед прокурорами и судьями встают многочисленные проблемы судебно-правового характера, обусловленные отчасти нематериальностью и недолговечностью электронных улик. Кроме того, для эффективного расследования и наказания в судебном порядке преступлений, связанных с использованием компьютеров, часто

* A/CONF.203/1.

** Генеральный секретарь выражает свою признательность за содействие в организации Семинара-практикума 6 Корейскому институту криминологии и правительству Канады.

*** Настоящий документ был представлен с опозданием в связи с необходимостью проведения дополнительных исследований и консультаций.

V.05-82261 050405 060405

необходимо отслеживать преступную деятельность и ее последствия через цепочку поставщиков услуг интернета или компаний, иногда в разных странах, в результате чего могут возникать сложные вопросы относительно юрисдикции и суверенитета.

Сложность проблем, которые характерны для преступности, связанной с использованием компьютеров, делает необходимым международное сотрудничество, для чего страны должны в конечном счете располагать соответствующими правовыми, процессуальными и нормативными средствами. Для разработки действенных методов эффективного международного сотрудничества в деле борьбы с преступностью, связанной с использованием компьютеров, на региональном и межрегиональном уровнях в последние годы был принят ряд мер, что позволило получить определенные значимые результаты. Чтобы эти усилия были эффективными, необходимо оказывать содействие проведению масштабных исследований по широкому спектру проблем борьбы с преступностью, связанной с использованием компьютеров, и активно развивать партнерские отношения между органами государственного управления и частным сектором.

В настоящем справочном документе выделены проблемы, которые сопутствуют преступлениям, связанным с использованием компьютеров, чтобы участники Семинара-практикума 6 могли рассмотреть рекомендации региональных подготовительных совещаний к одиннадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и наметить пути эффективных ответных действий в глобальном масштабе.

Содержание

I. Введение

1. Информационно-коммуникационные технологии преобразуют жизнь общества повсюду в мире. Инновации создают новые рынки товаров и услуг. Такие технологии вносят революционные изменения в процессы труда, повышают производительность в традиционных отраслях и увеличивают скорость движения капитала и объемы его потоков. Однако изменения в экономике – лишь одна сторона вопроса. Общества переживают глубокие изменения в сфере культуры, формируя средства массовой информации, которые, в свою очередь, формируют общества, а также адаптируясь к лавинообразному росту интернета. Быстрое развитие новых информационно-коммуникационных технологий по всему миру имеет и свою негативную сторону: создаются возможности для появления новых форм эксплуатации, новых разновидностей преступной деятельности и даже новых форм преступности.

2. Четыре региональных подготовительных совещания к одиннадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию вынесли на обсуждение одиннадцатого Конгресса ряд рекомендаций, в том числе: a) изучить современный опыт и существующие национальные правовые системы и механизмы сотрудничества между государствами, а также между поставщиками интернет-услуг и государствами; b) изучить наиболее приемлемые пути развития сотрудничества, обмена опытом, знаниями и ноу-хау между правительствами и частным сектором в целях создания и использования механизмов по предупреждению преступности, связанной с использованием компьютеров, борьбе с ней и обеспечению безопасности компьютерных сетей и систем связи, а также по принятию надлежащих ответных мер; c) изучить пути и средства повышения потенциала правительств в сфере разработки и применения соответствующих специальных методов расследования и судебного преследования, в том числе путем разработки и осуществления комплексных учебных программ для должностных лиц системы уголовного правосудия; d) рассмотреть вопрос использования компьютерных технологий в целях эксплуатации женщин и детей, особенно в связи с порнографией и педофилией; e) изучить вопрос о практической целесообразности создания глобальной целевой группы по проблемам интернета, которая могла бы содействовать международному сотрудничеству в борьбе с преступностью, связанной с использованием компьютеров; и f) рассмотреть возможность разработки новой конвенции против киберпреступности в целях создания основы для принятия эффективных коллективных мер борьбы с этой формой преступной деятельности.

Определение понятия "преступление, связанное с использованием компьютеров" или аналогичных ему, таких как "киберпреступление", обсуждалось на протяжении последних 30 лет. Впервые подобный термин был использован в одном из докладов Стэнфордского исследовательского института[1], а затем, в слегка измененном виде, он вновь появился в документах 1979[2] и 1989 годов[3]. Эта классификация широко употреблялась в опубликованных позже статьях по киберпреступности: компьютер как субъект преступления; компьютер как объект преступления; или компьютер как инструмент (четвертый вариант, предложенный в 1973 году, – компьютер как символ – по-видимому, вышел из употребления в 1980-х годах). Возможно, полезно по-иному сформулировать эту концептуальную модель,

рассматривая преступления, связанные с использованием компьютеров, как запрещаемое законом и/или судебной практикой поведение, которое a) направлено собственно на компьютерную сферу и коммуникационные технологии; b) включает использование цифровых технологий в процессе совершения правонарушения; или c) включает использование компьютера как инструмента в процессе совершения иных преступлений, и, соответственно, компьютер выступает при этом как источник электронных процессуальных доказательств[4]. В законах и договорах, в том числе в принятой Советом Европы Конвенции по киберпреступлениям[5], даны определения различных видов преступлений, связанных с использованием компьютеров (таких, как преступления против конфиденциальности, целостности или доступности компьютерных систем, правонарушения в отношении контента и правонарушения в отношении интеллектуальной собственности).

II. Преступления, связанные с использованием компьютеров

3. Существует ряд связанных с использованием компьютеров преступлений, объектом которых являются собственно информационно-коммуникационные технологии. Иногда такого рода преступления классифицируются как преступления против конфиденциальности, целостности или доступности компьютерных систем. К такого рода преступлениям относятся различные виды незаконного использования услуг электросвязи и незаконного использования компьютерных услуг путем применения разного рода хакерских технологий (в зависимости от технологии, к такого рода преступлениям относятся несанкционированный доступ, взлом кодов и паролей, цифровое клонирование, хищение средств с кредитных карт и т. п.). Серверы и веб-сайты могут стать объектом атак с целью спровоцировать отказ в обслуживании. Иногда такие преступления становятся результатом распространенных атак с целью спровоцировать отказ в обслуживании, в ходе которых десятки и сотни зараженных компьютеров используются в качестве "зомби" для массовой отправки на объект атаки запросов, которые становятся столь многочисленными, что удовлетворить запрос оказывается невозможным. В других случаях отказ в обслуживании становится следствием "пакетной лавины", возникающей из-за стремительного размножения сверхбыстрых "червей" (самовоспроизводящихся компьютерных программ), которые за считанные минуты создают миллиарды собственных копий; с таким объемом данных не справляются и мощнейшие оптико-волоконные кабели, что приводит к параличу компьютерных систем крупных компаний. Мировые эпидемии компьютерных вирусов в последние двадцать лет нарушали работу сетей, обслуживающих компании и потребителей, а время от времени ситуация еще более осложнялась вследствие появления новых, особенно мощных и вредоносных штаммов "червей" и вирусов. Примеры из недавнего прошлого свидетельствуют о наличии двух крайностей в специализации "червей": с одной стороны, существуют "черви", ориентированные на заражение десятков миллионов компьютеров и распространяющиеся через наиболее популярные операционные системы и приложения; с другой – "черви", созданные

только для атак на наиболее высококачественные защитные приложения, эксплуатируемые всего лишь на нескольких тысячах платформ.

Два жителя Мельбурна (Австралия) разослали от 6 млн. до 7 млн. сообщений по электронной почте на адреса в Австралии и Соединенных Штатах Америки, а также разместили множество сообщений на досках объявлений крупнейших поставщиков интернет-услуг. Цель этой операции заключалась в том, чтобы убедить граждан приобретать акции некоей американской компании, которые обращались в системе автоматической котировки Национальной ассоциации фондовых дилеров (НАСДАК). В этих сообщениях, рассылавшихся под фальшивыми именами и передававшихся в Соединенные Штаты через сторонние серверы, предсказывалось повышение цен на акции этой компании почти на 900 процентов. Вскоре объем продаж этих акций возрос в 10 раз, а их цена увеличилась вдвое, после чего торги были приостановлены, а компания объявила, что утверждения, содержавшиеся в ряде сообщений, не соответствуют действительности.

Эти двое австралийцев использовали классическую схему "вздуть и сбросить": один из сообщников, акционер компании, знал, что он сообщает ложную информацию, а когда цены на акции компании повысились, он с прибылью продал свою долю акций.

Эти двое лиц нарушили законы как Австралии, так и Соединенных Штатов. Помимо рыночных махинаций с акциями объем трафика, созданного носящими характер спама электронными сообщениями, был достаточен для создания помех правомерному использованию компьютера. Австралийская комиссия по ценным бумагам и инвестициям (АКЦБИ) приняла меры в ответ на жалобы, поступившие от австралийских пользователей, и на информацию, переданную властями Соединенных Штатов. На нарушителей удалось выйти, отследив распространявшуюся через сети электронную почту не подозревавших об этом компаний, а также пути прохождения платы за интернет-услуги.

Как это обычно бывает в случае такого рода правонарушений, Комиссия по ценным бумагам и биржам Соединенных Штатов потребовала принятия таких мер, как возврат незаконно присвоенного имущества и временный и бессрочный судебный запрет, чтобы предотвратить возобновление сообщниками такого рода деятельности. Им было предписано вернуть полученный обманным путем доход и дать обещание никогда впредь не совершать такого рода поступков. Власти Соединенных Штатов были убеждены в том, что Австралия способна осуществить судебное преследование на своей территории. АКЦБИ предъявила этим двум лицам обвинение по 19 пунктам. Оба признали себя виновными в распространении информации, которая являлась ложной или существенным образом вводящей в заблуждение и могла побудить к приобретению ценных бумаг, а также во вмешательстве в правомерное использование компьютеров, нарушении такого использования или препятствовании ему. Каждый из них был приговорен к двум годам лишения свободы с отсрочкой наказания (в отношении исполнителя преступления отсрочка вступила в силу после отбытия им трехмесячного тюремного заключения).

4. Применительно к компаниям лишение доступа к данным варьируется от ситуации, когда данные поддаются восстановлению (например, имеет место атака со стороны недовольного сотрудника, который производит несанкционированное шифрование файлов данных), до необратимого разрушения данных (под которым подразумевается не только простое удаление данных, но и физическое изъятие или уничтожение жестких дисков или других носителей информации, на которых находятся файлы). Беспроводные локальные вычислительные сети (ЛВС), которые компании активно внедряли в последние годы, могут оказаться уязвимыми для атак с целью спровоцировать отказ в обслуживании (например, путем создания помех) даже в случае, если они защищены от несанкционированного доступа[6].

5. Важно также знать, каким образом компьютеры используются как инструменты или орудия для совершения преступлений. Существует множество видов преступлений, связанных с изменением данных; некоторые из них, как, например, электронный вандализм, предполагают преступно причиненный вред (порча веб-сайта), а другие представляют собой профессионально выполненные подлоги или подделки. Существуют веб-сайты, посвященные теме "кардинга" (подделки кредитных карточек), куда относится и высококачественное изготовление поддельных денежных знаков и паспортов. Хищение данных[7] охватывает широкий спектр деяний – от информационного пиратства и промышленного шпионажа до нарушений авторского права (хищение интеллектуальной собственности путем тиражирования "пиратского" программного обеспечения, музыкальных файлов в формате MP3, цифровых видеозаписей и т. п.)[8]. Хищение данных может являться не только экономическим преступлением: недавно появившаяся категория преступлений, связанная с хищением личных данных, может также нарушать право на неприкосновенность частной жизни и смежные права физических лиц.

6. Существует много видов преступлений, связанных с использованием компьютеров, в рамках которых имеет место хищение денежных средств: это, например, атаки хакеров на банки или финансовые системы либо мошенничества, связанные с переводом "электронных денег". Высказывалась также озабоченность по поводу электронного отмывания денег и сопутствующих ему проблем, таких как уклонение от уплаты налогов.

7. Компьютеры используются также в интересах совершения широкого спектра махинаций в сфере телемаркетинга и инвестиций, сопряженных с мошеннической практикой. Мошенничество при проведении аукционов представляет собой наиболее распространенный, судя по жалобам потребителей, вид мошенничества, связанного с использованием компьютеров: по данным подготовленного в Соединенных Штатах всеобъемлющего доклада за 2003 год, такого рода правонарушения упоминаются в 61 проценте поданных заявлений о мошенничестве[9]. Другие виды обмана потребителей подпадают под более общую категорию "непоставка товаров или невыполнение платежей" после совершения сделки через интернет. Мошенничество с ценными бумагами, которое ассоциируется с биржевыми махинациями с малоценными бумагами, пока еще встречается относительно редко на уровне потребителей.

15-летний канадец получил в феврале 2000 года возможность контролировать ряд компьютеров и использовал их для организации распределенных атак типа "отказ в обслуживании" на Yahoo, Amazon.com и на другие известные сайты электронной торговли. Замедляя или ограничивая доступ на эти веб-сайты, он причинил владельцам ущерб на миллионы долларов вследствие потери клиентуры, снижения капитализации и затрат на обновление систем безопасности. После того как юноша похвастался этими атаками на чатах в интернете, Федеральное бюро расследований Соединенных Штатов установило его личность и передало это дело Канадской королевской конной полиции. Немногие страны (если таковые вообще существуют) готовы экстрадировать несовершеннолетних, и в данном случае законодательство Канады исключало возможность экстрадиции данного подростка. В сентябре 2001 года он был приговорен к восьми месяцам пребывания в молодежном исправительном центре.

8. "Фишинг" (или спам в форме дезинформации) – это рассылка по электронной почте сообщений с соответствующих веб-страниц, созданных таким образом, что они производят впечатление реально существующих потребительских сайтов. Миллионы подобных электронных сообщений мошеннического характера распространяются, подобно спаму, однако, вместо того чтобы напрямую предлагать приобрести товары или услуги, они маскируются под сообщения от банков, интерактивных аукционов или других законных сайтов и стремятся ввести пользователей в заблуждение, вынудив их сообщить в ответе свои личные данные, финансовые данные или пароли. Затем подобного рода частная информация используется для совершения покупок жульническим путем (иногда после ее продажи третьей стороне).

9. Такие "традиционные" виды преступлений, как вымогательство (угроза разгласить частную информацию или личные данные либо нанести ущерб данным или системам) и преследование, также существуют и в "сетевых" вариантах. Возбуждались и успешно доводились до суда дела о диффамации и клевете.

10. С использованием компьютеров совершается ряд преступлений, связанных с информационным наполнением, "контентом", в частности распространение незаконных и причиняющих вред материалов. Предметом особой озабоченности международного сообщества является детская порнография. Хотя детская порнография существовала в течение многих десятков лет (в форме фотографий, журналов, фильмов и видео), в конце 1980-х годов наметилась тенденция к увеличению объемов распространения детской порнографии посредством разного рода компьютерных сетей, использующих разнообразные интернет-услуги, в том числе веб-сайтов, тематических конференций (Usenet) и чатов (IRC) в интернете, а также одноранговых сетей (P2P)[10]. Такие сети используются в целях обмена информацией, торговли фотографиями и видео с детской порнографией, денежных транзакций и распространения информации о секс-туризме, объектом которого являются дети. Определенная доля детской порнографии распространяется с коммерческими целями (не считая бесплатных обменов между педофилами), и это связано с транснациональной организованной преступностью. Имеется и менее четко определенная "серая зона", в которой незаконность проникает в сферу в целом допустимого, поскольку интернет в течение последних 25 лет используется для

распространения порнографии, значительная часть которой во многих странах является разрешенной, а немалая часть носит коммерческий характер и часто именуется "индустрией развлечений для взрослых"[11]. Однако встречаются и другие случаи, более четко определенные, и некоторые изображения, являющиеся порнографией (будь то в форме цифровых изображений или видео), законодательство многих стран относит к числу непристойных, а распространение подобных непристойных материалов является преступлением. Интернет использовался также для совершения и других преступлений, связанных с контентом, таких как пропаганда ненависти и распространение материалов ксенофобского характера[12].

К числу случаев, получивших наибольшую известность в 1990-х годах, относится и атака на "Ситибэнк", совершенная молодым человеком из Российской Федерации, который получил несанкционированный доступ к серверам банка в Соединенных Штатах. С помощью ряда сообщников он открыл банковские счета в разных странах мира и затем дал компьютеру команду перевести средства на различные счета. Когда эта схема была обнаружена, а предполагаемый виновник установлен, один из федеральных судов Соединенных Штатов выдал ордер на его арест. В то время между Российской Федерацией и Соединенными Штатами не существовало договора об экстрадиции, однако обвиняемый допустил ошибку, отправившись на компьютерную выставку в Соединенное Королевство. Согласно договоренностям об экстрадиции, заключенным между Соединенным Королевством и Соединенными Штатами, британские власти могли оказывать содействие в той мере, в какой преступление, в котором обвинялось данное лицо, имеет аналог в британском законодательстве. Обвиняемый, оспаривая экстрадицию, потребовал применения habeas corpus, аргументировав это, в числе прочего, тем, что факт присвоения средств имел место в Российской Федерации, где находится клавиатура его компьютера, а не в Соединенных Штатах. Суд решил, что физическое присутствие обвиняемого в Санкт-Петербурге имеет меньше значения, нежели тот факт, что он работал с магнитными дисками, расположенными в Соединенных Штатах. Кроме того, деяние, в котором обвинялось данное лицо, имело прямые соответствия в Законе Соединенного Королевства о ненадлежащем использовании компьютера 1990 года, и если бы обвиняемый действовал с территории Соединенного Королевства, а не Российской Федерации, его деяние подпадало бы под юрисдикцию британского суда. Обвиняемый был экстрадирован в Соединенные Штаты, где он был осужден и отправлен в тюрьму.

11. В последние годы все больше внимания уделялось связи между терроризмом и интернетом, хотя и здесь имеют место разноплановые процессы. Существуют признаки того, что интернет используется для содействия финансированию терроризма, а также в качестве инструмента планирования и осуществления террористических актов. Все больше внимания уделяется и роли интернета в пропаганде терроризма, а также его использованию для вербовки. Такого рода действия отличаются от кибертерроризма, которому Центр защиты национальной инфраструктуры Соединенных Штатов дает следующее определение: "преступное деяние, совершенное посредством компьютера, результатом которого стали насилие,

смерть и/или разрушение, а также насаждение страха с целью принудить правительство изменить его политический курс"[13]. Существуют два четких основания для беспокойства: посягательства на важнейшие данные и посягательства на важнейшие элементы инфраструктуры.

12. Все глубже осознается значимость важнейших элементов информационной инфраструктуры, сетей, которые не только дают возможность поддерживать связь, но и используются для управления и контроля над важнейшими составляющими других ключевых элементов инфраструктуры, таких как энергетика, транспорт, продовольственное снабжение и здравоохранение. Во многих странах мира важнейшие элементы инфраструктуры могут находиться в частной собственности и быть особенно уязвимыми, поскольку многие их распределенные системы контроля и системы диспетчерского контроля и получения данных подключены к интернету, через который их функционирование можно нарушить. С учетом растущей взаимозависимости в современном обществе кибератаки на эти инфраструктуры могут оказать непосредственное серьезное воздействие на экономические и политические системы стран, а также привести к глубоким транснациональным последствиям. Важно иметь возможность противостоять атакам (по мотивам терроризма или других видов преступной деятельности), направленным на важнейшие элементы информационной инфраструктуры, с тем чтобы свести к минимуму серьезный риск цепной реакции, затрагивающей другие наиболее необходимые элементы инфраструктуры, имеющие важное значение для общества.

13. Проблемы разработки широкодоступной системы криптостойкого шифрования, привлекавшие внимание международной общественности на протяжении последних пяти лет, пока еще не нашли своего решения, и сегодня появилось новое поколение квантовой криптографии[14]. Хотя криптография играет важную роль в бизнесе и электронной торговле, ею пользуются и преступники. Проблема "технологий двойного назначения" выходит за рамки стеганографии и распространяется на разнообразные бесплатные программы одноранговых коммуникаций, оснащенные криптостойким шифрованием и чрезвычайно устойчивые к цензурированию (такие, как Freenet). Такие технологии способствуют утверждению свободы слова и могут внести вклад в дальнейшее развитие демократических свобод, но их же могут применять и преступники с целью маскировки связей между собой или для распространения материалов противоправного содержания.

III. Разрыв в цифровых технологиях и преступления, связанные с использованием компьютеров

14. Когда информационно-коммуникационные технологии распространяются в различных частях мира, это распространение происходит по-разному. Если в одном регионе, возможно, используются волоконно-оптические кабели с высокой пропускной способностью, то в другом наблюдается стремительный рост сетей подвижной и беспроводной связи. Различия в характере внедрения новых технологий делают регионы уязвимыми, и в зависимости от ситуации появляются конкретные виды преступлений, связанных с использованием компьютеров.

15. Происшедшие изменения носили радикальный характер: ошеломляющий рост оборудования на основе информационных и компьютерных технологий (в мире сегодня насчитывается около 2 млрд. компьютеров и других устройств на базе микропроцессоров); экспоненциальный рост количества сетевых подключений;

революционные процессы в сфере компьютерной техники, как, например, прорывы в области миниатюризации, скорости и хранения данных; появление интеллектуальных систем и роботов; а также расширение взаимодействия между человеком и компьютером. Однако такие технологические преобразования не только пронизывают среду, в которой мы живем, невиданным ранее образом связывая людей, объекты и информацию, но и представляют собой новое поколение угроз и факторов уязвимости в цифровой сфере, что вызывает необходимость кардинального пересмотра представлений о преступности в XXI веке.

16. Ввиду этого в 2002 году Генеральная Ассамблея призвала международное сообщество усилить помощь государствам-членам в борьбе с преступностью, связанной с использованием компьютеров. В документе "Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века", прилагавшемся к резолюции 56/261 Генеральной Ассамблеи от 31 января 2002 года, имеется особый раздел под названием "Меры по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров". В нем содержатся ориентированные на принятие конкретных мер программные рекомендации по предотвращению такого рода преступлений и борьбе с ними. В резолюции 57/170 от 18 декабря 2002 года Генеральная Ассамблея предложила Комиссии по предупреждению преступности и уголовному правосудию при разработке рекомендаций относительно одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию в соответствии с резолюцией 56/119 Генеральной Ассамблеи от 19 декабря 2001 года учитывать прогресс, достигнутый в реализации дальнейших мер по осуществлению Венской декларации и планов действий.

17. Признание и учет наличия разрыва в цифровых технологиях были одной из основ вклада Организации Объединенных Наций в начале XXI века. Общий контекст обозначен в Декларации тысячелетия Организации Объединенных Наций, принятой Генеральной Ассамблеей в ее резолюции 55/2 от 8 сентября 2000 года. В Цель 8 Целей в области развития на пороге тысячелетия, содержащихся в приложении к докладу Генерального секретаря под названием "План осуществления Декларации тысячелетия Организации Объединенных Наций" (A/56/326), включена задача 18: "В сотрудничестве с частным сектором принимать меры к тому, чтобы все могли пользоваться благами новых технологий, особенно информационно-коммуникационных". В Декларации принципов, принятой на Всемирной встрече на высшем уровне по вопросам информационного общества, которая состоялась в Женеве 10–12 декабря 2003 года, изложено общее представление об информационном обществе (A/C.3/59/3, глава I, раздел A): "Мы также в полной мере осознаем, что сегодня преимущества революции в области информационных технологий неравномерно распределены между развитыми и развивающимися странами, а также внутри стран. Мы полны решимости превратить этот разрыв в цифровых технологиях в цифровые возможности для всех, прежде всего для тех, кому грозят отставание и дальнейшая маргинализация"[15].

К концу 2004 года доступ к интернету в Китае имели 94 млн. человек, или примерно 7,2 процента населения страны, причем 45,5 процента из них использовали для доступа широкополосные линии. Количество хост-компьютеров оценивалось в 41,6 млн., численность адресов IPv4 – в 60 млн., доменных имен – в 432 077, а веб-сайтов в домене .cn – в 668 900[16]. При приросте, составляющем примерно 18 процентов в год, в 2008 году численность китайских пользователей интернета превысит численность пользователей в Северной Америке, но уже сегодня она больше, чем в Республике Корея и Японии, вместе взятых. В 1999 году число пользователей составляло всего 8,9 млн. человек; в 2001 году это число увеличилось до 33,7 млн. Количество хост-компьютеров возросло с 3,5 млн. в 1999 году до 33,7 млн. в 2001 году.

18. На конец 1985 года число хост-компьютеров интернета превысило 2 тыс.; в 1989 году оно достигло 100 тыс., а в 1990 году превзошло 300 тыс. Оно достигло 1 млн. в середине 1992 года, 10 млн. – в конце 1995 или в начале 1996 года и 100 млн. – в конце 2000 года; к июлю 2002 года оно составляло более 162 млн.[17] В 2002 году в развивающихся странах было только 4,1 пользователя интернета и 3,3 персональных компьютера на 100 жителей, тогда как в развитых странах на 100 жителей приходилось 33,3 пользователя интернета и 36,2 персональных компьютера (E/2004/62 и Corr.1). На пятую часть населения земли, проживающую в странах с наивысшим уровнем доходов, приходилось 81,9 процента общего количества персональных компьютеров в мире, 76,2 процента общего числа пользователей интернета и 97,5 процента общего числа хост-компьютеров интернета[18].

19. Во многих развивающихся странах нет сектора электросвязи, способного поддерживать подобные динамичные, современные и эффективные информационно-коммуникационные системы. В 2000 году Организация Объединенных Наций сообщила, что доступом к сетям располагало только примерно 4,5 процента населения земного шара по сравнению с 44 процентами жителей Северной Америки и 10 процентами европейцев, в то время как в Азии, Африке и Южной Америке эти показатели колебались в пределах от 0,3 до 1,6 процента[19]. В настоящее время на региональном уровне более 98 процентов общемировых полос рабочих частот на базе интернет-протокола замкнуты на входе и выходе на Северную Америку. 99 процентов общемировых затрат на производство информационных технологий приходится на 55 стран (E/2000/52, пункты 50–51). Это свидетельствует об очевидном повороте к экономике, основанной на знаниях, однако такие не относящиеся к сфере развития факторы, как структура и стоимость доступа к услугам электросвязи, влияют на показатели доступа и пользования.

20. Однако по мере все более широкого распространения благ информационно-коммуникационных технологий повсюду в мире будет необходимо также повышать уровень информированности относительно сопутствующих угроз и факторов уязвимости, связанных с преступностью в компьютерной сфере. Разрыв в цифровых технологиях не только характеризует разницу в уровнях экономического развития между развитыми странами, развивающимися странами и странами с переходной экономикой[20], но и демонстрирует различия в характере угроз и факторов уязвимости, являющихся результатом киберпреступности. Информационно-

коммуникационные технологии внедряются в различных регионах в разное время вследствие не только расхождений между богатыми и бедными, но и влияния таких факторов, как география регионов. Например, в некоторых странах с гористой местностью стоимость прокладки подземных кабелей электросвязи может быть запредельно высокой, а установка вышек и антенн микроволновой радиорелейной системы позволяет эффективно внедрять сети беспроводной телефонии. Таким образом, схемы информационно-коммуникационных технологий в одной стране или регионе могут существенно отличаться от таких схем в соседних странах или регионах. Различия в методах внедрения новых технологий приводят и к неодинаковым тенденциям в области "криминальной инновации" и, соответственно, порождают разные угрозы, источником которых является преступность, связанная с использованием компьютеров.

21. Развивающаяся страна, обладающая минимальной инфраструктурой электросвязи, может быть использована в качестве плацдарма для организации атак или в качестве страны транзита, через которую проходит маршрут атак, особенно если в такой стране не предусмотрено правовых санкций, которые отбивали бы охоту к совершению преступлений с использованием компьютеров или предусматривали бы судебное преследование по делам такого рода. Что касается развивающихся стран, то внедренные и поддерживаемые здесь виды технологий могут породить новые для данного региона факторы угрозы. Можно предположить, что вновь возникающие и пока еще хрупкие структуры информационных технологий могут оказаться чрезмерно уязвимыми, пока эти системы не окрепнут, а стандарты безопасности не внедрятся более широко[21].

22. Тип компьютеров и их количество, а также масштабы соответствующих сетей в компаниях или в государственных учреждениях могут весьма отличаться от характеристик аналогичных устройств у пользователей или частных лиц. По мере распространения информационно-коммуникационных технологий в обществе появляются новые целевые группы, уязвимые в отношении конкретных видов преступлений, связанных с использованием компьютеров, начиная с заражения вирусами и вторжения в компьютер и заканчивая различными разновидностями обмана потребителей. Когда страны начинают внедрять информационно-коммуникационные технологии, различные слои общества подвергаются опасности разного рода преступлений, связанных с использованием компьютеров.

IV. Преодолевая границы: трансграничная преступность и компьютерно-техническая судебная экспертиза

23. При расследовании преступлений, связанных с использованием компьютеров, возникает ряд проблем в сфере судебной экспертизы. Часть проблем, возникающих при реконструкции какого-либо инцидента, который дает основания подозревать совершение киберпреступления, связаны с тем, что улики зачастую являются неосязаемыми и недолговечными. При расследовании киберпреступлений делается попытка получить не материальные свидетельства, а следы в цифровой среде, которые зачастую быстро исчезают и сохраняются в течение лишь короткого промежутка времени. Одна из причин такой неустойчивости заключается в том, что некоторые виды электронных данных об адресации и маршрутизации (то есть "данные трафика") не хранятся на постоянной основе. Такая информация может

сохраняться в памяти компьютерной системы лишь в течение короткого времени, а затем поверх нее записывается другая информация о маршрутизации.

24. Новые технологии не только порождают новые проблемы, но и предоставляют тем, кто ведет расследование, новые возможности, позволяя реконструировать маршруты в цифровой среде. Есть много условий, при которых данные трафика и другие виды информации по управлению сетями могут записываться в сетевых журналах, а не просто стираться. В интернете и в других компьютерных сетях разного рода информация по сетевому управлению обычно хранится, чтобы проанализировать ее в дальнейшем с целью ведения отчетности в сети, повышения надежности услуг и сетевого оборудования, анализа случаев сбоев, тенденций в функционировании и прогнозировании пропускной способности сетей. Помимо этого такие данные могут быть также использованы для маркетинга и анализа пользователей (например, запросы тех или иных страниц на веб-сайтах розничной торговли могут помочь определить пользующиеся наибольшей популярностью продукты, тенденции покупательского поведения или характеристики потребителей).

25. Существует, однако, ряд обстоятельств, определяющих, будут ли данные или аналогичная информация сохранены. Одним из таких факторов, например, является тип услуги. При оказании услуги по обеспечению доступа к интернету (например, с использованием Протокола службы удаленной аутентификации пользователей по телефонным линиям – RADIUS) определенные сведения об абонентах и некоторые данные трафика могут быть сохранены, чтобы обеспечить абонентам доступ к интернету. Это особенно важно при повременной оплате услуг, предполагающей необходимость фиксировать, когда и как долго абонент находился в сети. Наоборот, при оказании услуг, обеспечивающих анонимность или конфиденциальность, такое сохранение будет сведено к минимуму[22].

26. В электронной почте, которая восходит к началу существования интернета (она стала доступной в 1971 году по сети ARPANET), обычно содержатся информация об адресации и другие данные трафика, размещаемые в полях заголовков[23]. Часть такой информации создается клиентской программой конечного пользователя, а часть – сервером электронной почты (где применяется Упрощенный протокол передачи электронной почты – SMTP).

27. Наиболее известной интернет-услугой является, по всей вероятности, "Всемирная паутина" (World Wide Web), в значительной части которой для установления соответствия между доменными именами (указанием местонахождения веб-сайтов) и адресами по интернет-протоколу (цифровыми адресами ресурсов, между которыми перемещаются пакеты) применяется система доменных имен (DNS). На сетевых серверах может храниться большой объем данных трафика, показывающих, какие страницы были запрошены и кем (то есть с какого IP-адреса). Такая практика более распространена на коммерческих серверах, поскольку объемы хранящейся информации могут быстро выйти на уровень, исчисляемый в гигабайтах, и их хранение может стать дорогостоящим.

28. При оказании услуги передачи файлов информация об абонентах может сохраняться либо не сохраняться в журналах регистрации, в зависимости от того, каким образом оказывается эта услуга. Обычно передача файлов осуществлялась с использованием протокола передачи файлов (FTP), хотя при защищенной передаче все чаще применяется шифрование с использованием протокола Secure Shell (SSH). Недавно централизованные файловые серверы начали заменяться одноранговыми

(P2P) системами, позволяющими вести обмен файлами между большим числом пользователей (примерами децентрализованных ресурсов, распределяемых по сетям временных серверов, являются Napster, KaZaA, Morpheus, Gnutella и Freenet). Некоторые виды P2P позволяют легко получить доступ к данным трафика, тогда как другие их виды предусматривают создание помех для анализа таких данных.

29. К числу других услуг относятся около 100 тыс. тематических конференций в сети Usenet, на которых обсуждаются буквально любые темы. Доступ на них можно получить через всемирную сеть серверов с промежуточным хранением, управляемую Протоколом передачи новостей по сети (NNTP), – некоторые данные трафика можно получить с сервера, а другие будут сохраняться в локальном персональном компьютере. Существует также множество чатов в режиме реального времени – от IRC до систем мгновенной передачи сообщений (Instant Messaging).

30. Различные интернет-услуги обычно оказываются через разные сетевые устройства (такие, как маршрутизаторы или серверы). В зависимости от конфигурации сайта поставщика услуг те или иные журналы учета операций могут храниться в множестве разных машин, которые могут контролироваться различными юридическими лицами, а иногда и размещаться в разных странах.

31. С учетом широты спектра возможных услуг, различных ниш на рынке и еще ряда факторов, в том числе и стоимости хранения данных[24], можно утверждать, что у предпринимателей или в отрасли нет единой позиции относительно сбора и хранения данных о трафике и об абонентах. Очевидно, что сохранение определенных данных о трафике и об абонентах может помочь правоохранительным органам в отслеживании преступников в интернете, и некоторые страны недавно приняли законы, предусматривающие обязательное сохранение данных. Даже в случае отсутствия законов, предусматривающих сохранение данных о трафике, судебным следователям важно понять применяемые поставщиками услуг интернета систему учета в сети и практику сетевого управления, чтобы определить, в какой степени их обычная практика соответствует требованиям правоохранительных органов[25]. Сотрудничество со стороны поставщиков услуг интернета может оказать неоценимую помощь в тех случаях, когда власти проводят следствие и возбуждают судебное преследование по делам о преступлениях, связанных с использованием компьютеров.

32. Для эффективного расследования и судебного разбирательства по делам о преступлениях, связанных с использованием компьютеров, зачастую необходимо отслеживать преступную деятельность через ряд поставщиков услуг интернета и компаний, имеющих подключенные к интернету компьютеры. Чтобы добиться успеха, следователи должны пройти по всей коммуникационной цепи до источника и компьютеров или других устройств, принадлежащих пострадавшим, работая при этом с промежуточными поставщиками услуг в разных странах. С целью выхода на источник преступления правоохранительные органы часто вынуждены ориентироваться на регистрационные записи о том, когда и кем были установлены те или иные соединения. Иногда правоохранительным органам необходимо отследить соединение в момент его осуществления. Если поставщик услуг находится вне территориальной юрисдикции проводящего расследование органа (что случается нередко), правоохранительным органам необходима будет помощь партнеров в других странах. Обычные и даже принимаемые в экстренном порядке меры взаимной правовой помощи нередко предусматривают получение архивных данных и информации, касающихся только двух стран (например, стран местонахождения

пострадавшего и правонарушителя), в режиме реального времени. Если преступник направляет свои сообщения через три, четыре или пять стран, процесс оказания правовой помощи проходит через определенные этапы, прежде чем правоохранительные органы получат данные от каждого поставщика услуг, задействованного в цепочке соединений, и это увеличивает риск того, что данные будут недоступны или утеряны, а преступник останется неустановленным и сможет продолжать свою преступную деятельность[26].

33. Для оказания содействия в расследовании дел о преступлениях, связанных с использованием компьютеров, Подгруппа "группы восьми" по высокотехнологичной преступности приступила в 1997 году к составлению списка круглосуточных контактных пунктов по делам о международных преступлениях, связанных с высокими технологиями и использованием компьютеров, – списка подразделений, занимающихся делами о связанных с использованием компьютеров преступлениях, установить контакт с которыми правоохранительные ведомства могут в любой день и в любое время суток (по принципу "круглосуточно без выходных"). В контактную сеть входят 40 стран, она является неотъемлемой частью Конвенции Совета Европы по киберпреступлениям, предоставляющей следственным органам инструментарий для борьбы с любыми преступлениями, совершенными против компьютерных систем, внутри них и/или с их использованием.

34. Ввиду наличия большого числа вирусов, "червей" и хакеров, использующих уязвимые места в компьютерных системах, необходимо также иметь механизмы, позволяющие немедленно принимать ответные меры. В десятках стран по всему миру созданы центры реагирования на компьютерные инциденты (CERT). В число их основных задач входит:

a) создавать целостную картину методов атаки, факторов уязвимости и воздействия атак на информационные системы и сети; предоставлять сведения по тенденциям и характеристикам компьютерных инцидентов и уязвимости;

b) создавать инфраструктуру непрерывного повышения квалификации специалистов по вопросам безопасности, способных быстро реагировать на атаки на подключенные к интернету системы и защищать свои системы от сбоев систем защиты;

c) разрабатывать методы оценки, совершенствования и поддержания безопасности и жизнеспособности сетевых систем;

d) совместно с продавцами повышать защищенность продуктов, готовых к использованию[27].

35. Если нарушитель находится в одной стране, атака была предпринята с компьютера, расположенного в другой стране, а последствия наступают в третьей стране, очевидно, что помимо недолговечности данных возникают правовые проблемы, связанные с вопросами границ и юрисдикции. При расследовании и судебном преследовании преступлений, связанных с использованием компьютеров, крайне необходима взаимная правовая помощь. Однако вопрос суверенитета – лишь одна из многих проблем, возникающих при проведении обысков и наложении ареста на имущество в другой стране. При отсутствии надлежащей взаимной правовой помощи существует риск того, что сотрудники правоохранительных органов одного государства, разыскивая информацию в компьютерах, размещенных в другом государстве, будут проводить трансграничные исследования в компьютерных

системах, не получив на это соответствующего разрешения. Однако еще до рассмотрения вопросов, связанных с оказанием взаимной правовой помощи, необходимо проанализировать внутреннее законодательство. В конце концов, для международного сотрудничества прежде всего необходимо, чтобы в странах уже имелись законы, позволяющие решать проблемы компьютерных преступлений.

V. Национальное законодательство: необходимое предварительное условие

36. В некоторых случаях определенные виды преступлений, связанных с использованием компьютеров, распространяются подобно эпидемии, невзирая на национальные границы. В иных случаях элементы того или иного преступления распространяются на другие страны в рамках тщательно продуманной стратегии запутывания следов и сокрытия истинного местонахождения правонарушителей. Возрастание масштабов распространения информационно-коммуникационных технологий с целью использования преимуществ информационного общества также увеличивает частоту совершения в стране преступлений, связанных с использованием компьютеров. Таким образом, принимая законы о борьбе с преступлениями, связанными с использованием компьютеров, страны исходят из интересов своей экономической и общественной безопасности.

37. Национальное законодательство развивалось на протяжении столетий, тогда как интернет – всего считанные десятилетия. Конечно, право постоянно эволюционирует сообразно изменениям в обществе. Модернизация национального законодательства, возможно, потребуется и для решения проблем преступности, связанной с использованием компьютеров. Зибер (Sieber) выделил шесть основных этапов формирования законодательства о борьбе с компьютерными преступлениями, принятого в разных странах начиная с 1970-х годов[28]: a) защита данных и защита неприкосновенности частной жизни; b) уголовное законодательство о борьбе с экономическими преступлениями, связанными с использованием компьютеров; c) защита интеллектуальной собственности; d) защита от противозаконного и вредного контента; e) уголовно-процессуальное законодательство; и f) правовое регулирование защитных мер, таких как криптография и требования в отношении аутентификации[29].

38. Для решения проблем преступности, связанной с применением компьютеров, необходим ряд элементов: a) убедиться, что в законе содержится определение таких преступлений; b) законодательно определить полномочия по ведению расследования в целях борьбы с киберпреступностью; и c) осуществлять эти полномочия таким образом, чтобы обеспечивались гарантии соблюдения основополагающих прав человека и свобод.

A. Преступления в области материального права

39. Были разработаны всеобъемлющие перечни преступлений против конфиденциальности, целостности или доступности компьютерных систем[30]. Существует также множество правонарушений, связанных с контентом (таких, как производство и распространение детской порнографии и материалов ксенофобского характера), которые относятся к числу преступлений, связанных с применением компьютеров.

Бюро по надзору за информационной безопасностью Министерства общественной безопасности Китая сообщило, что в 2001 году было зарегистрировано немногим менее 5 тыс. преступлений, связанных с применением компьютеров, тогда как в 2000 году их было около 2,9 тыс., а в 1999 году – примерно 400. К середине 2002 года Бюро сообщило уже о более чем 3 тыс. случаев, и, по некоторым оценкам, до конца 2002 года будет рассмотрено еще 350 дел о проникновении в компьютер и более 800 дел – о нанесении ущерба компьютерным системам[31]. Количество случаев, выявленных Бюро, росло с огромной скоростью, хотя многие случаи так и остались незамеченными либо о них не поступало сообщений. Большинство правонарушителей были молодыми людьми (в возрасте от 18 до 30 лет), большинство атак велось из интернет-кафе, а правонарушители скрывали свою личность, входя в сеть через прокси-серверы по протоколам http или Sock, используя поддельные IP-адреса или применяя средства криптографии или стеганографии. Вследствие этого в Китае начали принимать более строгие меры при регистрации интернет-кафе и по надзору за ними.

40. Когда государства попытались адаптировать нормы, разработанные для вещественных объектов, к неосязаемому и эфемерному миру электронных объектов, возник целый ряд вопросов.

41. При разработке норм следует проявлять осторожность, чтобы не допустить отнесения правомерных деяний к разряду криминальных. При модернизации уголовного законодательства необходима осмотрительность при отделении общего от частного. Возможно, что слишком конкретно сформулированные положения могут устареть с появлением новых технологий. Соответственно, желательно использовать "технологически нейтральные" термины.

B. Процессуальные полномочия

42. В последние годы в силу все большего распространения электронной документации многим странам пришлось рассматривать вопросы определения понятия "документы". Даже такие основополагающие понятия, как "место" проведения обыска, могут вызвать правовые проблемы в случаях, когда данные распределены по компьютерной сети (то есть может проводиться обыск компьютера в офисе, расположенном в одном месте, а данные могут храниться в компьютере, физически расположенном в другом месте, хотя "виртуально" они доступны пользователю и лицу, ведущему следствие).

43. При определении процессуальных полномочий полезно провести различие между тремя видами информации: a) фактическое содержание электронных сообщений; b) данные трафика; и c) сведения об абонентах (подписчиках). Проводить различие между этими тремя видами информации желательно, потому что, соответственно, могут по-разному решаться вопросы защиты неприкосновенности частной жизни или защиты данных или же могут быть затронуты другие основные права и свободы человека.

44. Одной из первых правовых проблем является разработка определения понятий "данные трафика" и "информация о подписчике". Например, в принятой Советом Европы Конвенции по киберпреступлениям[32] "данные трафика" определяются как

"любые компьютерные данные, связанные с операциями по передаче данных посредством компьютерной системы, которые созданы компьютерной системой, являвшейся звеном в цепочке передачи данных, и указывают на источник сообщения, его назначение, маршрут, время, дату, размер, длительность или тип лежащей в его основе услуги" (статья 1). Конвенция определяет "информацию о подписчике" как "любую информацию в форме компьютерных данных или в любой иной форме, которой обладает поставщик услуг относительно подписчика его услуг, и отличную от данных трафика или данных о содержании, с помощью которой можно установить:

a) тип используемой коммуникационной услуги, примененные для этого технические средства и срок предоставления услуги;

b) личность подписчика, его почтовый или географический адрес, номер телефона или иного средства доступа, информация о выставлении счетов и их оплате, доступная на основании соглашения или договора об обслуживании;

c) любая иная информация о месте установки коммуникационного оборудования, доступная на основании соглашения или по договору об обслуживании" (пункт 3 статьи 18).

45. Вопрос относительно определений рассматривался в Руководстве Организации Объединенных Наций по предупреждению преступлений, связанных с использованием компьютеров, и борьбе с ними[33], и к нему обращались Европейский совет (в своем "рамочном решении" относительно атак на информационные системы), а также законодатели ряда стран[34].

46. Во внутреннем законодательстве многих стран определенные виды контента могут пользоваться более высокой конституционной защитой в свете таких концепций, как "тайна переписки" и "свобода выражения мнения". Таким образом, может оказаться необходимым провести правовое и процедурное разграничение между содержанием различных видов обмена сообщениями в интернете (тех, которые являются частными, а не публичными) и данными трафика. Возможно также при определенных обстоятельствах увязать определенные элементы данных трафика и информации о подписчике[35] с положениями о защите данных, поскольку они представляют собой важную информацию биографического характера, которая может охраняться согласно нормам о защите неприкосновенности частной жизни.

47. Следует отметить, что сбор и последующее сохранение данных чреваты столкновением интересов и несовпадением ценностей различных заинтересованных сторон, и может быть целесообразным попытаться достичь баланса между различными законными интересами. В некоторых странах сбор данных жестко ограничивается требованиями добросовестной информационной практики, иногда зафиксированными в законах о защите данных или о защите неприкосновенности частной жизни, согласно которым сведения можно собирать только в ограниченных целях, использовать только в точно определенных целях, при условии получения информированного согласия и при соблюдении иных ограничительных норм (таких, как проверки целостности информации, наличие установленных сроков уничтожения сведений и доступ субъекта данных к собранным о нем сведениям)[36].

48. Технологии с промежуточным хранением могут, как правило, порождать разного рода правовые проблемы в странах, где действуют разные правовые режимы в отношении мониторинга контента в режиме реального времени (например,

положения о прослушивании телефонных разговоров), в противоположность обыскам и выемке. Что касается преступлений, связанных с использованием компьютеров, то здесь может возникать проблема в отношении электронной почты, когда может понадобиться разрешение на мониторинг содержания электронного письма в режиме реального времени, если письмо находится в процессе передачи, однако, если оно находится в состоянии покоя (например, хранится на почтовом сервере или на жестком диске конечного пользователя), может потребоваться ордер на обыск и выемку. Поскольку электронное письмо, по сути, является в обеих ситуациях одним и тем же, может возникнуть проблема в связи с использованием двух различных правовых инструментов, порядок применения которых может регламентироваться законом с различной степенью жесткости.

49. В целях содействия расследованию преступлений, связанных с использованием компьютеров, разработан ряд правовых инструментов, в том числе предписание об обеспечении сохранности и предписание о представлении материальных доказательств. Предписание об обеспечении сохранности – это оперативный обеспечительный механизм, предписывающий поставщикам услуг собирать и сохранять имеющиеся данные по конкретной транзакции или по конкретному клиенту. Подобный процессуальный механизм важен в отношении электронных улик, поскольку такие улики проще поддаются удалению или уничтожению, нежели документы в физической форме. В сущности, предписание об обеспечении сохранности – это распоряжение "не удалять данные". Предписание об обеспечении сохранности[37] по своей природе является временным и издается с учетом ожидаемого получения правоохранительными органами необходимых законных полномочий на получение данных (например, ордера на изъятие данных либо предписания о представлении материальных доказательств, обеспечивающего раскрытие данных).

50. Предписание о представлении материальных доказательств обязывает хранителя документов предоставить документы правоохранительным органам или открыть последним доступ к этим документам в течение определенного срока. Предписания о представлении материальных доказательств подобны ордерам на обыск, хотя по получении предписания о представлении материальных доказательств обыск проводит хранитель документов, а не полиция. Такое распоряжение в меньшей степени вносит дезорганизацию, поскольку хранитель документов чаще лучше знает точное местонахождение соответствующих документов. В современной деловой практике корпорации часто хранят данные за пределами тех стран, где они ведут дела, нередко для того, чтобы воспользоваться преимуществами более низких расценок на хранение данных. В этой ситуации традиционный ордер на обыск может оказаться не соответствующим ситуации, тогда как предписания о представлении материальных доказательств дают возможность владельцу данных или их хранителю получить документы или архивные данные.

VI. К поиску решений на основе международного сотрудничества

51. Чтобы эффективно реагировать на запросы о помощи, поступающие от других государств, или получать помощь от других государств, может оказаться необходимым адаптировать национальные законы к задачам борьбы с киберпреступлениями. Совместимость с законами других государств является

важной целью при разработке законодательства о борьбе с преступлениями, связанными с использованием компьютеров. С целью соблюдения суверенных прав государств и содействия международному сотрудничеству необходимо в конечном счете изучить те возможности, которые предоставляют официальные международные механизмы, такие как конвенции. Для того чтобы взаимная правовая помощь была эффективной, определения основных преступлений и процессуальные полномочия, существующие в одной стране, должны соответствовать аналогичным положениям, действующим в другой стране.

52. Международное сообщество еще только начинает решать те многочисленные проблемы, которые возникают в этой области. Массированные атаки типа "отказ в обслуживании", когда сотни зараженных компьютеров в нескольких странах используются для атак на коммерческие веб-сайты в другой стране или когда вирус или "червь", пройдя через две трети стран мира, причиняет огромный ущерб, ставят фундаментальные вопросы, например, относительно того, где было совершено преступление и против кого следует возбуждать судебное преследование. Другая важнейшая проблема – это то, насколько эффективность действий в конечном счете будет определяться волей и желанием того или иного государства самому заняться расследованием и возбуждением судебного преследования. Очевидно, что транснациональная преступность, связанная с использованием компьютеров, готова воспользоваться пробелами вследствие расхождений в правовой базе и возможностях систем уголовного правосудия. Некоторые могут счесть это нарушением суверенитета, тогда как другие будут настаивать на том, что происходят изменения в понимании суверенитета по мере повсеместного развития информационного общества.

53. При подобных сценариях немедленно возникает сложный вопрос экстрадиции, который сам по себе способен создать ряд проблем. Например, из-за отсутствия функциональной совместимости определений основных преступлений данное преступление может трактоваться таким образом, что соблюдение требований об обоюдном признании данного деяния уголовно наказуемым правонарушением окажется невозможным. В то же время все бóльшую поддержку находит понимание того, что в случаях, когда требуется обоюдное признание деяния уголовно наказуемым, необходимо совпадение основополагающих элементов правонарушения или поведения, лежащего в его основе, а не только той формы, в которой данное правонарушение описано в законодательстве соответствующих стран. Даже если в том или ином конкретном случае проблем в связи с признанием данного деяния уголовно наказуемым правонарушением не возникает, данный вид преступления, связанного с применением компьютера, может сам по себе не рассматриваться как достаточно серьезный вид преступления (например, с точки зрения соответствующих положений о мерах наказания), дающий основания для экстрадиции.

54. Несмотря на эти проблемы, в период после 2000 года, когда состоялся десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, удалось добиться ряда впечатляющих результатов, в том числе принятия двух новых правовых актов: Конвенции Совета Европы по киберпреступлениям и Конвенции Организации Объединенных Наций против транснациональной организованной преступности. Последний документ имеет глобальный масштаб, но косвенно в нем рассматриваются и проблемы

киберпреступлений, если они совершаются организованными преступными группировками.

55. На международном уровне такие организации, как Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК), Международная организация уголовной полиции (Интерпол), Организация международного сотрудничества и развития (ОЭСР) и "группа восьми", а также такие региональные организации, как Европейский союз, Совет Европы, Организация американских государств, Ассоциация государств Юго-Восточной Азии и Азиатско-Тихоокеанская ассоциация экономического сотрудничества (АТЭС), обеспечивают политические и технические знания и опыт, необходимые для развития международного сотрудничества. В отличие от того, что было несколько лет назад, сегодня можно говорить о наличии международного консенсуса в отношении борьбы с киберпреступностью, особенно в ее транснациональных формах, которые она часто принимает. Таким образом, наконец имеется позитивный "моральный климат", благоприятствующий совместному принятию мер гражданского, уголовного или административного характера, и такое сотрудничество основано на том, что социологи называют "обществами одной судьбы"[38].

56. Конвенция по киберпреступлениям была открыта для подписания 23 ноября 2001 года; ее подписали 30 государств и ратифицировали 8 государств. К Конвенции могут присоединиться и государства, расположенные за пределами Европы, и четыре таких государства (Канада, Соединенные Штаты, Южная Африка и Япония) уже подписали ее. Конвенция вступила в силу 1 июля 2004 года. Этот документ обязывает государства, являющиеся его сторонами, гармонизировать национальные законы в отношении определения основных преступлений. К их числу относятся преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, а также преступления, связанные с использованием компьютеров, такие как подлоги и компьютерное мошенничество, преступления, связанные с нарушением авторского права, и преступления в сфере детской порнографии, совершенные с использованием компьютерных систем. Кроме того, Конвенцией предусматривается важный комплекс процессуальных полномочий, в том числе предписания о представлении материальных доказательств и предписания об обеспечении сохранности, разработанные для упрощения расследований и возбуждения судебного преследования в условиях существования глобальных компьютерных сетей. В Конвенцию также включены положения, позволяющие создать оперативную и эффективную систему международного сотрудничества. И наконец, проблема "преступлений, совершенных из ненависти", стала причиной принятия Факультативного протокола к Конвенции по киберпреступлениям, касающегося введения уголовной ответственности за деяния расистского или ксенофобского характера, совершенные с помощью компьютерных систем[39], который был открыт для подписания 28 января 2003 года. Факультативный протокол был подписан 20 и ратифицирован 2 государствами.

57. В 2002 году министры юстиции государств – членов Содружества наций приняли модельный закон под названием "Закон о компьютерных преступлениях и преступлениях, связанных с использованием компьютеров"[40]. Модельный закон, который исходит из тех же принципов, что и Конвенция по киберпреступлениям, обеспечивает правоохранительные органы современными и эффективными средствами борьбы с киберпреступностью. Прокуроры, следователи и законодатели могут дать оценку материалам, разработанным на международном уровне, таким как

руководящие принципы, руководства по правовым и техническим вопросам, примеры наилучшей практики и типовое законодательство, чтобы помочь властям при разработке национального законодательства.

58. Начиная с восьмого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, состоявшегося в 1990 году, Организация Объединенных Наций активно занимается рассмотрением различных аспектов процессов в сферах, связанных с использованием компьютеров[41]. В 1994 году при значительной содержательной и финансовой поддержке со стороны правительства Канады и ряда экспертов, представляющих правительства других стран и неправительственные организации, было опубликовано Руководство Организации Объединенных Наций по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними[42].

59. В 2000 году в рамках десятого Конгресса был проведен семинар-практикум по преступлениям, связанным с использованием компьютерных сетей[43]. В 2001 году Генеральный секретарь представил Комиссии по предотвращению преступности и уголовному правосудию выводы исследования по вопросу об эффективных мерах предотвращения высокотехнологичных и компьютерных преступлений и борьбы с ними (E/CN.15/2001/4).

60. По итогам первого этапа Всемирной встречи на высшем уровне по вопросам информационного общества, прошедшего в Женеве в декабре 2003 года, Генеральный секретарь учредил в 2004 году Рабочую группу по управлению использованием интернета, в задачи которой входит рассмотрение проблем спама, кибербезопасности и других вопросов, связанных с использованием интернета, в рамках подготовки ко второму этапу этой Всемирной встречи на высшем уровне, который пройдет в Тунисе в ноябре 2005 года.

61. Преступления, связанные с использованием компьютеров, представляют собой явление международного масштаба, требующее принятия решений на международном уровне. Чтобы найти такие решения, международному сообществу следует тщательно проанализировать те средства укрепления международного сотрудничества, которыми оно располагает в настоящее время. Ему следует также попытаться углубить свои познания и понимание различных проявлений этого феномена, проблем, порождаемых этими проявлениями, и возможных и желательных путей предупреждения этого явления и борьбы с ним.

VII. Сотрудничество в изучении проблем преступности, связанной с использованием компьютеров

62. Задача создания доказательственной базы для последующей разработки политики весьма масштабна. Изучение проблем преступности, связанной с использованием компьютеров, находится в самом начале. Обладающие необходимыми знаниями лица и учреждения как государственного, так и частного сектора могут по причинам делового, политического характера или по соображениям национальной безопасности оказаться не готовыми делиться своими знаниями с исследователями. Информация, которая попадает в документы публичного характера, может зачастую быть неполной или неточной. Несмотря на это, необходимо формировать базу знаний, с тем чтобы усилия по преодолению разрыва в цифровых технологиях начали давать результаты.

63. Для того чтобы получить базовые данные о степени распространения и тяжести различных видов киберпреступлений, необходимо использовать широкий спектр методов исследований и сравнительного анализа. Кроме того, чрезвычайно важны исследования эффективности новых законов, стратегий охраны правопорядка и судебного преследования, проводимые на основе изучения конкретных дел и уровня снижения преступности. Исследования не должны ограничиваться данными, поступающими из полиции или судов, и такие источники нередко должны быть более конкретными и единообразными. Среди вопросов, безотлагательно нуждающихся в изучении, – поведение пострадавших и правонарушителей, а также отслеживание процессов в законодательной и правоприменительной сферах по всему миру[44].

VIII. Сотрудничество между государственным и частным секторами в борьбе с преступностью, связанной с использованием компьютеров

64. Правительства и представители частного сектора во все большей мере признают острую потребность в тесном сотрудничестве в борьбе с преступностью, связанной с использованием компьютеров. Ни одно, отдельно взятое, правительство или группа правительств и ни одна отдельная компания или отрасль не могут достичь успеха в одиночку; должно существовать тесное партнерство между государством и частным сектором на принципах открытости и прочной двусторонней связи. Организации частного сектора играли и будут играть жизненно важную роль в разработке технологий, направленных на предотвращение и расследование киберпреступлений. Однако помимо разработки технических решений частный сектор может также сыграть важную роль, помогая политикам определять приоритеты и находить решения в законодательной сфере. Опыт показал, что активные партнерские отношения между государством и деловыми кругами могут помочь эффективнее обеспечивать соблюдение законов о борьбе с киберпреступниками.

65. Обнадеживает тот факт, что количество партнерств с участием государственного и частного секторов непрерывно растет. Члены "группы восьми" уже давно признали, что для эффективной борьбы с киберпреступностью необходимо вывести сотрудничество между государством и деловыми кругами отрасли на беспрецедентный уровень, и приняли важные меры в этом направлении, в том числе оказывая содействие проведению конференций с участием представителей государств и частного сектора, на которых обсуждались представляющие общий интерес проблемы и возможные решения[45]. Организация Объединенных Наций, АТЭС, ОЭСР и другие многосторонние организации также прилагают усилия для более широкого вовлечения в эту деятельность частного сектора.

66. В декабре 2004 года представители ряда отраслей и международных правоохранительных учреждений объявили о создании электронной сети "Фишнет" (Digital PhishNet) – совместного правоохранительного мероприятия, в рамках которого отраслевые лидеры в сфере технологий, банковского дела, финансовых услуг и онлайновых аукционов совместно с правоохранительными органами борются с "фишингом" – губительной и все более распространяющейся формой похищения персональной информации в онлайновом режиме. Благодаря этой сети создается единая, унифицированная система связи между компаниями отрасли и

правоохранительными органами, что позволит собирать важнейшие данные, необходимые для борьбы с фишингом, и предоставлять их правоохранительным органам в режиме реального времени. Если другие отраслевые группы сосредоточили свое внимание на выявлении веб-сайтов, занимающихся фишингом, и на обмене опытом и информацией по конкретным случаям, то Digital PhishNet является первой в своем роде группой, занимающейся оказанием помощи правоохранительным органам и содействием в выявлении и организации судебного преследования виновных в совершении уголовных преступлений в отношении потребителей путем фишинга. Digital PhishNet объединяет ведущие корпорации отрасли: 9 из 10 крупнейших банков Соединенных Штатов, четырех из пяти крупнейших поставщиков интернет-услуг и пять компаний электронной торговли и технологий – и сотрудничает с основными федеральными и международными правоохранительными учреждениями.

67. За последние несколько лет ряд организаций частного сектора совместно с Университетом Гонконга провели ряд крупных конференций по проблемам киберпреступности. В работе этих конференций приняли участие ведущие сотрудники министерств юстиции и правоохранительных органов стран Азиатско-Тихоокеанского региона, а также видные ученые и представители авторитетных международных организаций, в том числе Организации Объединенных Наций, Совета Европы, Интерпола и АТЭС. На конференциях обсуждались проблемы в области защиты сетей, факторы угрозы электронной торговле, такие как спам, фишинг и другие формы онлайнового мошенничества, а также онлайновое пиратство.

68. В последние несколько лет сотрудники правоохранительных органов различных стран мира совместно с рядом известных компаний ведут расследования и судебное преследование действующих в сети мошенников и других киберпреступников, в том числе и некоторых наиболее известных в мире спаммеров.

69. Несмотря на эти успехи, можно сделать еще больше для дальнейшего углубления сотрудничества между правительствами и представителями отрасли, а также для придания большей четкости и регулярности диалогу и партнерским отношениям между государственным и частным секторами.

IX. Рекомендации

70. Возможно, одиннадцатый Конгресс пожелает рассмотреть следующие рекомендации, разработанные на двух совещаниях экспертов, которые были проведены в Сеуле под эгидой Корейского института криминологии, с учетом также соответствующих рекомендаций одиннадцатому Конгрессу, принятых на региональных подготовительных совещаниях:

а) Для решения проблем киберпреступности необходимо применять широкие, комплексные подходы, выходящие за рамки уголовного и уголовно-процессуального законодательства, а также правоприменения. В рамках такого подхода следует уделять внимание требованиям к безопасному функционированию киберэкономики, которые укрепляли бы доверие со стороны бизнеса и обеспечивали неприкосновенность частной жизни, равно как и стратегиям, направленным на продвижение и защиту нововведений, рост потенциала повышения благосостояния и возможностей информационных и компьютерных технологий, в том числе

механизмам раннего предупреждения и реагирования в случае кибератак. Помимо необходимости предотвращения преступлений, связанных с использованием компьютеров, и судебного преследования за их совершение появляется более глобальная задача – создание глобальной культуры кибербезопасности, в рамках которой учитывались бы потребности всех стран, включая развивающиеся, структуры информационных технологий в которых находятся в процессе становления и пока еще весьма уязвимы.

b) Следует и далее развивать международное сотрудничество на всех уровнях. Система Организации Объединенных Наций, будучи универсальной по своему характеру, должна, при условии усовершенствования ее внутренних координационных механизмов, к чему призывает Генеральная Ассамблея, играть ведущую роль в межправительственных мероприятиях, направленных на обеспечение функционирования и защиту киберпространства, чтобы преступники или террористы не могли злоупотреблять им или воспользоваться им в своих целях. В частности, системе Организации Объединенных Наций следует сыграть важную роль в разработке глобальных подходов к борьбе с киберпреступностью и процедур международного сотрудничества, имея целью предупреждение и смягчение негативного влияния, которое оказывает киберпреступность на важнейшие элементы инфраструктуры, устойчивое развитие, защиту неприкосновенности частной жизни, электронную коммерцию, банковское дело и торговлю.

c) Следует призвать все государства как можно быстрее обновить свое уголовное законодательство, чтобы учесть особый характер киберпреступности. Что касается традиционных видов преступлений, совершаемых с использованием новых технологий, то такое обновление может принять форму уточнения или изъятия норм, которые более не отвечают в полной мере сложившейся ситуации, например законов, которые не могут решать проблемы разрушения или хищения нематериальных активов, либо создания новых норм, касающихся новых видов преступлений, таких как несанкционированный доступ к компьютерам или компьютерным сетям. Такое обновление должно касаться также процессуального законодательства (например, касающегося отслеживания сообщений) и законов, договоров или положений о взаимной правовой помощи (например, по вопросам оперативного обеспечения сохранности данных). Следует призывать государства руководствоваться при определении степени суровости вновь принимаемых законов положениями Конвенции Совета Европы по киберпреступлениям.

d) Правительствам, частному сектору и неправительственным организациям следует проводить совместную работу по преодолению разрыва в цифровых технологиях, повышать информированность общества о факторах риска, связанных с киберпреступностью, и принимать соответствующие контрмеры, а также укреплять потенциал специалистов в области уголовного правосудия, в том числе сотрудников правоохранительных органов, прокуроров и судей. Для этого национальным судебным органам и юридическим учебным заведениям следует включать в свои учебные программы комплексные курсы по преступлениям, связанным с использованием компьютеров.

e) Одиннадцатому Конгрессу следует уделить значительное внимание разработке, совершенствованию и развитию существующих ныне практических механизмов обмена информацией в международном масштабе, раннего предупреждения и реагирования, а также способов уменьшения ущерба в рамках борьбы с киберпреступностью, используя в этих целях возможности Интерпола,

механизмов оперативного реагирования 24/7, разработанных "группой восьми", Конвенции по киберпреступлениям, Центров реагирования на компьютерные инциденты (CERT) и Форума центров компьютерной безопасности и реагирования на компьютерные инциденты (FIRST), которые пока распространяются лишь на отдельные, преимущественно развитые, страны. Эти механизмы следует сделать доступными на международном уровне, чтобы наладить обмен знаниями и информацией о путях и методах распознавания, защиты, недопущения и борьбы с новыми видами киберпреступлений и информировать общество об эффективных механизмах реагирования. Кроме того, особо следует позаботиться о том, чтобы эти практические механизмы были доступны развивающимся странам, и организовать соответствующее обучение.

f) Для того чтобы политика борьбы с киберпреступностью была эффективной и действенной, ее следует строить на доказательственной основе и подвергать строгой оценке. Поэтому на международном уровне следует предпринять целенаправленные и скоординированные усилия для создания механизмов финансирования в целях содействия практическим разработкам и пресечения многих видов вновь появляющихся киберпреступлений. Однако не менее важно, чтобы такие исследования координировались на международном уровне и чтобы результаты исследований были широкодоступными.

g) ЮНОДК следует вынести результаты работы Семинара-практикума по мерам борьбы с преступлениями, связанными с использованием компьютеров, который пройдет в рамках одиннадцатого Конгресса, на рассмотрение второго этапа Всемирной встречи на высшем уровне по вопросам информационного общества, который состоится в Тунисе в 2005 году.

Примечания

[1] D.B. Parker, S. Nycum and S.S. Oüra, *Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1973).

[2] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1979).

[3] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1989).

[4] Russell G. Smith, Peter N. Grabosky and Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

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

[6] В ряде стран, где беспроводные ЛВС используются частными лицами для получения доступа к интернету из дома, имели место случаи использования незащищенных ЛВС для получения несанкционированного доступа к интернету в различных целях. Это часто сочетается с "флибустьерством" (поиском и фиксацией таких точек беспроводного доступа, или "гнезд", при помощи ноутбука из движущегося автомобиля).

[7] В некоторых странах понятие "хищение" относится только к осязаемым объектам и подразумевает кражу у лица некоего материального предмета; следовательно, оно не распространяется на хищение неосязаемого объекта и не будет касаться акта изготовления копии электронного файла. В некоторых странах такие деяния не подлежат уголовному преследованию и уголовным санкциям,

но считается, что они подпадают под нормы гражданского права, в том числе под режимы авторского права.

[8] Разработанная Брэмом Коэном (Bram Cohen) программа одноранговых коммуникаций BitTorrent все шире используется для обмена объемными файлами данных как во вполне правомерных целях (например, для распространения программного обеспечения с открытыми исходными кодами, компьютерных игр или "одноранговой" трансляции телепрограмм в сети), так и видеопиратами. Обзор видеопиратства см.: Clive Thompson, "The BitTorrent effect", *Wired*, 13 January 2005; и Jeff Howe, "The shadow Internet", *Wired*, 13 January 2005.

[9] *IC3 2003 Internet Fraud Report*: *January 1, 2003-December 31, 2003* (Национальный центр борьбы с должностными преступлениями и Федеральное бюро расследований Соединенных Штатов).

[10] См. Michael D. Mehta, Don Best and Nancy Poon, "Peer-to-peer sharing on the Internet: an analysis of how Gnutella networks are used to distribute pornographic material". *Canadian Journal of Law and Technology*, vol. 1, No. 1 (January 2002); и United States of America, General Accounting Office, *File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (Washington, D.C., February 2003).

[11] Dick Thornburgh and Herbert S. Lin, eds., *Youth, Pornography and the Internet* (Washington, D.C., National Academy Press, 2003).

[12] Обзор законов 24 стран, касающихся распространения материалов расистского, ксенофобского и антисемитского характера, см. в документе по этому вопросу, который рассматривался на Конференции по проблемам антисемитизма Организации по безопасности и сотрудничеству в Европе (CIO.GAL/25/04/Rev.1), состоявшейся в Берлине 28–29 апреля 2004 года.

[13] Scott Berinato, "The truth about cyberterrorism", *CIO Magazine*, 15 March 2002.

[14] Относительно имеющихся в продаже продуктов, в которых для шифрования данных, передаваемых по сетям на основе волоконно-оптических линий связи или беспроводным сетям, применяется квантовая криптография, см. Gary Stix, "Best-kept secrets", *Scientific American,* January 2005.

[15] Анализ аспектов Целей в области развития на пороге тысячелетия, связанных с информационно-коммуникационными технологиями, см. в исследовании Международного союза электросвязи *Отчет о развитии всемирной электросвязи 2003 года: Показатели доступа для информационного общества,* 7-е издание (2003 год). В исследовании содержится любопытная оценка Целей в области развития на пороге тысячелетия, имеющих непосредственное отношение к информационно-коммуникационным технологиям; особенно многообещающе выглядит новый Индекс цифрового доступа (ИЦД).

[16] China Internet Network Information Center, *15th Statistical Survey Report on the Internet Development in China (Jan. 2005)* (www.cnnic.net.cn) (по состоянию на 25 января 2005 года).

[17] Консорциум интернет-систем (Internet Systems Consortium) (http://www.isc.org).

[18] Данные приводятся по *Всемирной базе данных Международного союза электросвязи по показателям развития электросвязи (International Telecommunications Union World Telecommunication Indicators Database),* 8-е изд. (2004 год).

[19] *Обзор мирового экономического и социального положения, 2000 год* (издание Организации Объединенных Наций, в продаже под № R.00.II.C.1).

[20] Статистический анализ комплексного характера проблемы разрыва в цифровых технологиях представлен в концептуальной структуре, содержащейся в работе под ред. Джорджа Сиадаса [George Sciadas, ed., *Monitoring the Digital Divide… and Beyond* (2003)].

[21] Замечено, что, по иронии судьбы, в силу этих обстоятельств разрыв в цифровых технологиях воссоздается на новом уровне именно в тот момент, когда он почти преодолен, что может поставить под вопрос доверие местных деловых кругов или исходную привлекательность инвестиций.

[22] Основная разница между оказанием услуг на анонимной основе и созданием псевдонима заключается в том, что в случае оказания услуги с созданием псевдонима (вымышленного имени) в течение определенного времени сохраняется некая идентификация (следовательно, может иметься более существенная связь между вымышленным именем, личностью абонента и "реальной" личностью). С другой стороны, оказание услуги на анонимной основе в ее наиболее чистом виде есть оказание единичной, разовой услуги. Существуют различные виды оказания услуг на анонимной основе и с созданием псевдонима, по большей части заключающиеся в предоставлении прокси-ресурсов, последовательностей ресурсов и смешанных сетей, позволяющих получить доступ к одной или нескольким типичным интернет-услугам, например к перенаправлению электронной почты, навигации по Всемирной паутине, интернет-чатам или тематическим конференциям Usenet. Степень анонимности или работы под псевдонимом может также зависеть не только от таких факторов, как характер программного обеспечения, используемого для шифрования и идентификации, но и от характера и защищенности сервера или сети серверов, обеспечивающих анонимность, процедуры создания псевдонимов, а в случае платности услуг – и от механизма расчетов.

[23] David H. Crocker, rev., *Standard for the Format of ARPA Internet Text Messages,* RFC 822 (13 August 1982).

[24] На семинаре-практикуме по сохранению данных, состоявшемся в рамках организованного Группой восьми промышленно развитых стран диалога между правительствами и деловыми кругами по вопросу безопасности и надежности виртуального пространства (Берлин, октябрь 2000 года), были отмечены следующие финансовые последствия сохранения данных: объемы хранимых журналов; выборка надлежащей информации; проектирование и разработка; административные и эксплуатационные расходы и расходы на обучение; обеспечение безопасности и неприкосновенности частной жизни; ответственность за поиск и предоставление данных правоохранительным органам; а также расходы, связанные с утраченными возможностями и доверием пользователей.

[25] Поставщики услуг могут хранить данные в течение различного времени в зависимости от бизнес-моделей, характера услуг и используемых технологий. Некоторые данные сохраняются для расчетов с абонентами, другие – для анализа производительности систем. Срок хранения варьируется от нескольких секунд до более длительных периодов времени, которые требуются или допускаются национальным законодательством стран их местонахождения для иных, нежели охрана правопорядка, целей. Кроме того, различные виды данных о трафике хранятся разное время; например, в отношении журналов учета сетевого доступа (по протоколу RADIUS или протоколу идентификации пользователя TACACS+) существуют иные требования в отношении ведения дел и хранения данных, нежели в отношении журналов учета по протоколу NNTP, так что первые в результате этого могут, в определенных случаях, быть доступны в течение более длительного времени. Контент обычно не хранится или недоступен.

[26] *Recommendations for Tracing Networked Communications across National Borders in Terrorist and Criminal Investigations* (http://canada.justice.gc.ca/en/news/g8/doc2.html).

[27] См. *CERT coordination Center, 2003 Annual Report* (www.cert.org); и Форум центров компьютерной безопасности и реагирования на компьютерные инциденты [Forum of Incident Response and Security Teams (www.first.org)].

[28] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study* (1 January 1998).

[29] Предложенная Зибером модель шести этапов формирования национального законодательства была применена к опыту Австралии Смитом, Грабоски и Урбасом: Russell G. Smith, Peter N. Grabosky and Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[30] Organization for Economic Development and Cooperation, *Computer-Related Crime: Analysis of Legal Policy*, ICCP Series, No. 10 (1986); см. также рекомендацию № R (89) 9, принятую Комитетом министров Совета Европы 13 сентября 1989 года.

[31] Национальный доклад, представленный Китаем на Азиатско-Тихоокеанской конференции по киберпреступности и информационной безопасности, которая состоялась в Сеуле с 11 по 13 ноября 2002 года и была организована Экономической и социальной комиссией ООН для Азии и Тихого океана и Министерством информации и связи Республики Корея. Численность правонарушителей может быть большей, учитывая, что в одном районе Пекина (Прокуратура района Хайдянь) в период с 2001 года по май 2004 года были арестованы 52 подозреваемых, 48,4 процента из которых – за хакерство.

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

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

[34] Закон Соединенного Королевства "О регулировании следственных полномочий" (2000 год) содержит (статья 2.9) определение данных о трафике, хотя в это определение включаются и сведения об абонентах. Определенная концепция данных о трафике содержится и в определениях "автоматического регистратора телефонных переговоров" и "устройства перехвата и слежения", существующих в законодательстве Соединенных Штатов (United States Code, title 18, sect. 3127) и обновленных в Законе об объединении и усилении Америки средствами, необходимыми для борьбы с терроризмом ("Патриотический закон") 2001 года.

[35] Что касается данных о подписчиках (абонентах), то в некоторых странах, возможно, уже существуют нормы на этот счет в области телефонной связи (сведения об имени и адресе клиента).

[36] Непосредственное отношение к этому вопросу имеют, например, такие международно-правовые акты, как Конвенция Совета Европы о защите частных лиц в связи с автоматизированной обработкой личных данных (Council of Europe, *European Treaty Series*, No. 108) или Руководящие принципы, регулирующие защиту неприкосновенности частной жизни и трансграничные потоки личных данных, принятые в 1980 году Организацией экономического сотрудничества и развития (ОЭСР). Они были направлены на установление принципов, согласно которым личные данные должны собираться на справедливой основе; использоваться только в изначально определенных целях; быть адекватными, относящимися к делу и не чрезмерными для указанных целей; быть точными и не устаревшими; быть доступными субъекту данных; храниться с соблюдением мер защиты; и уничтожаться по достижении цели их использования. Иногда эти требования были еще более ужесточены, например директивы о защите данных 95/46/EC и 97/66/EC, принятые Европейским парламентом и Советом Европейского союза. Опираясь на эти документы и во исполнение своих юридических обязательств о соблюдении стандартов, установленных в этих директивах, многие страны Европы ввели в действие более жесткое законодательство о защите данных. За пределами Европы также существуют правовые акты, содержащие аналогичные нормы об обращении с личными данными, например канадский Закон о защите личной информации и об электронных документах.

[37] Отметим, что "обеспечение сохранности данных" означает недопущение удаления имеющихся в наличии определенных сведений, относящихся к конкретному подписчику. Напротив, "сохранение данных" представляет собой требование общего характера, направленное на обеспечение сбора и сохранения всеми поставщиками интернет-услуг определенного набора сведений, касающихся всех подписчиков.

[38] Roderic Broadhurst, "Content crimes: criminality and censorship in Asia", материал, представленный на конференции "Вызовы со стороны киберпреступности" в рамках Программы Octopus (Страсбург, Франция, 15–17 сентября 2004 года).

[39] Council of Europe, *European Treaty Series*, No. 189.

[40] Текст этого модельного закона можно найти на веб-страницах Отдела правовых и конституционных вопросов Секретариата Содружества: (http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).

[41] В рамках восьмого Конгресса был проведен семинар-практикум по компьютеризации отправления уголовного правосудия (A/CONF.144/14). Уже в 1992 году Организация издала *Справочник по компьютеризации информационных систем по уголовному правосудию* (издание Организации Объединенных Наций, в продаже под № R.92.XVII.6). В рамках девятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, состоявшегося в 1995 году, был проведен семинар-практикум по вопросам международного сотрудничества и оказания помощи в управлении системой уголовного правосудия: компьютеризация операций по обеспечению уголовного правосудия и сбор, анализ и программное использование информации по вопросам уголовного правосудия (A/CONF.169/13) [см. также Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, *The Global Challenge of High-Tech Crime: Workshop on Crimes related to the Computer Network; Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 15 April 2000, Vienna, Austria* (Tokyo, April 2001)].

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

[43] См. Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети (A/CONF.187/10).

[44] Peter Grabosky and Roderic Broadhurst, "The future of cyber-crime in Asia", *Cybercrime: the Challenge in Asia*, Roderic Broadhurst and Peter Grabosky, eds., Hong Kong University Press, 2005, pp. 347-360.

[45] См. "G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace (Summary and Assessment)" (доступно по адресу: http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html); и Kuriko Miyake, "G8 concludes Tokyo high-tech crime meeting" (доступно по адресу: http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg).