

4. Заверение контента

Для доказывания многих преступлений и правонарушений необходимо доказать распространение или обнародование некоторой информации. Возбуждение межнациональной розни, клевета, пропаганда наркотиков, распространение порнографии, нарушение авторских прав — в состав этих и других преступлений входит такое действие, как распространение информации или произведения. Разумеется, в данной книге речь пойдет только о распространении через компьютерные сети, прежде всего Интернет.

Как доказать факт наличия определенной информации в сети в определенный период времени, а также ее общедоступность? Как установить лицо, разместившее информацию, и доказать этот факт?

Сложности в доказательстве таких фактов суть следующие:

- невозможно произвести непосредственный осмотр размещенной информации (произведения), поскольку видеть можно лишь изображение на экране, возникшее вследствие сложных и не контролируемых процессов передачи, и преобразования изначально размещенной информации;
- подавляющее большинство веб-страниц — динамические, их контент зависит от времени, местоположения пользователя, его браузера, ряда случайных факторов;
- доступ к информации в Сети производится через посредство множества технических средств, о большинстве из которых не известно ничего определенного;
- во многих случаях доступ производится в интерактивном режиме, то есть для получения информации требуется проявление инициативы со стороны пользователя;
- существует много способов ввести в заблуждение пользователя, просматривающего информацию, — относительно самого факта размещения информации, ее содержания, адреса, времени;
- размещенную информацию в ряде случаев довольно просто и быстро убрать либо она уничтожается сама с течением времени;
- Интернет рассматривается многими как некая область особенной свободы или экстерриториальная зона, поэтому там существует много средств и возможностей для анонимизации, сокрытия следов, круговой поруки;
- существующие процессуальные нормы рассчитаны были исключительно на офлайновые* документы и доказательства, в них редко учтены технические особенности компьютерных сетей.

Методы фиксации доказательств тем не менее существуют. Рассмотрим наиболее распространенные методы размещения информации в Сети и укажем для каждого из случаев его особенности и приемлемые методы фиксации.

Размещение на веб-сайте

В простейшем случае размещение на веб-сайте сводится к помещению файла в соответствующую директорию на сервере.

В более сложных случаях для размещения информации могут потребоваться также следующие действия:

- регистрация или приобретение доменного имени*, настройка DNS-серверов* для него;
- установка и запуск веб-сервера*;
- приобретение услуги провайдера по организации и поддержанию веб-сервера (хостинг* или колокация*);
- настройка веб-сервера;
- создание или модификация исходного кода* веб-страницы на языке HTML, PHP и др.;
- создание или модификация CGI-скриптов* для поддержания работы веб-сайта;
- создание или заказ художественного оформления (дизайна) веб-сайта;
- настройка аутентификации и авторизации на веб-сайте;
- сообщение каким-либо способом адреса (URL) размещенного файла или соответствующей веб-страницы заинтересованным лицам, рекламирование такого адреса;
- отслеживание работы веб-сайта, его статистики посещений, трафика, количества скачиваний размещенной информации, отзывов посетителей и т.д.;
- обновление, актуализация размещенной информации;
- удаление или блокирование размещенной информации.

Каждое из указанных действий оставляет «цифровые» следы. Чем больше таких действий совершал злоумышленник, тем легче его идентифицировать и впоследствии доказать его вину.

Как видно, следы могут быть достаточно многочисленными. Впрочем, в данной главе речь идет не о поиске и изобличении лица, разместившего информацию, а о доказательстве наличия в Сети самой этой информации.

Практика

В российской практике применялись следующие способы удостоверения содержимого веб-сайта для судебных целей:

- распечатка веб-страниц через браузер*;
- распечатка + рапорт сотрудника милиции;
- осмотр веб-сайта следователем с понятыми;
- такой же осмотр, но с участием специалиста;
- ответ оператора связи (провайдера) на запрос о содержимом сайта;
- экспертиза;
- нотариальное удостоверение (осмотр сайта нотариусом).

Каждый из способов безупречен. Хотя браузер и вся система WWW ориентированы на неподготовленных лиц, все же специальные знания требуются для того, чтобы убедиться в отсутствии ошибок и намеренных фальсификаций. Поэтому без участия специалиста корректность результата не гарантирована. Применение же экспертизы вроде бы избавляет от возможных ошибок. Но вызывает сомнение тот факт, что объект экспертизы (веб-страница, веб-сервер) находится не в распоряжении эксперта, а довольно далеко от него.

Просмотр

Цепочка преобразования информации на пути ее от сервера к пользователю дается следующей схемой:

**информация на диске сервера — веб-сервер —
браузер — изображение на экране**

Разумеется, информация при прохождении указанной цепочки претерпевает значительные изменения. Они касаются не только ее формы представления, но и содержания. Преобразования формы в этой цепочке настолько многочисленны и многовариантны, что описать их все не представляется возможным. Постараемся упомянуть хотя бы те преобразования, которые затрагивают содержание информации.

Динамические веб-страницы

В самом начале эры WWW, в первой половине 1990-х, веб-страница была эквивалентна файлу на диске веб-сервера. То есть, например, при запросе пользователем веб-страницы «<http://example.com/folder/page.html>» сервер, расположенный по адресу «example.com», брал с локального диска из директории «folder» файл «page.html» и отправлял его содержимое пользователю, лишь добавив в начало служебный заголовок. Такие HTML-страницы называются статическими.

Затем появились динамические веб-страницы. По запросу пользователя веб-сервер не просто берет определенный файл, а исполняет более сложную последовательность действий. Из файла или группы файлов или

из базы данных веб-сервер выбирает не просто HTML-код, а программу. Затем эта программа выполняется, а результат ее исполнения отображается браузером пользователя. Причем исполнение программы может производиться: (а) веб-сервером или одним из его модулей; (б) внешней программой на стороне веб-сервера; (в) браузером пользователя или одним из его модулей; (г) внешней программой на стороне пользователя. Понятно, что вид динамической веб-страницы будет зависеть от многих факторов, в том числе от конфигурации ПО на стороне пользователя. В настоящее время практически все веб-страницы в Интернете — динамические.

Особенности браузера

Следует принимать во внимание, что передаваемый от веб-сервера к браузеру код (HTML-код с различными включениями) не воспринимается человеком непосредственно. Этот код — лишь набор команд браузеру по генерации изображения, которое уже воспринимается человеком, а следовательно, может вызывать какие-либо правовые последствия. Хотя HTML и другие используемые на веб-страницах языки стандартизованы [30, 72], один и тот же код может интерпретироваться по-разному в разных условиях. Отличия в интерпретации (представлении) одного и того же кода разными браузерами, как правило, невелики. Некоторые мелочи и нюансы в стандартах не описаны. Некоторые браузеры немного отклоняются от стандартов или имеют собственные расширения к стандартизованному формату. Все это не может привести к принципиальным отличиям во внешнем виде страницы.

Но есть моменты, которые могут привести к принципиальным, то есть содержательным отличиям. Это прежде всего включенные в HTML-код программы на других языках или объекты, отображаемые другими, внешними приложениями. Получив в составе веб-страницы такой объект, браузер пытается найти и загрузить модуль либо внешнее приложение для выполнения такого кода и отображения результатов. Такие внешние (по отношению к браузеру) модули и приложения значительно менее стандартизованы и могут показывать пользователю существенно отличающиеся изображения или не показывать ничего, если соответствующего модуля или внешнего приложения не нашлось.

Поэтому, фиксируя вид веб-страницы, следует установить, каким именно браузером формируется это изображение и отметить в протоколе версию браузера. Еще более важно установить, только ли браузер формирует изображение на экране, участвуют ли в этом иные модули или внешние программы, а если участвуют, то какие именно.

Адресация

Кроме изменений, связанных с передачей размещенной информации от сервера к пользователю, следует также упомянуть о возможных проблемах, связанных с адресацией.

Утверждение «В Интернете по такому-то адресу (URL) размещена такая-то информация» не всегда четко и однозначно задает место размещения этой информации.

В URL [28], как правило, используется доменное имя*. Оно является средством адресации. Распространено мнение, что каждому доменному имени соответствует определенный IP-адрес. Браузер получает доменное имя, затем при помощи DNS* разрешает его в IP-адрес и обращается к сайту по этому IP-адресу. Это верно лишь в первом приближении. На самом деле адресация эта, во-первых, не статична, а во-вторых, не всегда однозначна. Кроме того, пользователь может быть перенаправлен на иной веб-сервер в зависимости от разных обстоятельств. Для иллюстрации приведем два примера.

В первом примере показывается динамическое разрешение доменного имени в IP-адрес, так называемый механизм «Round robin DNS». При разрешении доменного имени «cnn.com» на несколько сделанных подряд запросов возвращаются восемь различных IP-адресов, причем в разной последовательности:

```
fnn@home$>host cnn.com
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com has address 64.236.29.120
cnn.com mail is handled by 10 atlmail3.turner.com
cnn.com mail is handled by 10 atlmail5.turner.com
cnn.com mail is handled by 20 nycmail2.turner.com
cnn.com mail is handled by 30 nycmail11.turner.com
fnn@home$>host cnn.com
cnn.com has address 64.236.29.120
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com mail is handled by 10 atlmail5.turner.com
cnn.com mail is handled by 20 nycmail2.turner.com
cnn.com mail is handled by 30 nycmail11.turner.com
```

```

cnn.com mail is handled by 10 atlmail13.turner.com
fnn@home$>host cnn.com
cnn.com has address 64.236.24.28
cnn.com has address 64.236.29.120
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com mail is handled by 10 atlmail13.turner.com
cnn.com mail is handled by 10 atlmail15.turner.com
cnn.com mail is handled by 20 nycmail12.turner.com
cnn.com mail is handled by 30 nycmail11.turner.com

```

Веб-сайт cnn.com обслуживается сразу несколькими серверами. При разрешении доменного имени DNS-сервер выдает сразу восемь различных IP-адресов. Браузер может выбрать любой из них, но обычно выбирается первый. Выдавая IP-адреса в разном порядке, DNS-сервер пытается равномерно распределить нагрузку на эти сервера.

В данном случае все сервера, обслуживающие веб-сайт, имеют одинаковый контент* (информационное наполнение). Но могли бы иметь разный.

Второй пример показывает зависимость видимой веб-страницы от IP-адреса пользователя. Автор запросил одну и ту же веб-страницу «www.google.com» с двух различных компьютеров. У первого из них IP-адрес зарегистрирован за российским провайдером, у второго — за немецким. Ответы веб-сервера были различными.

```

-bash-2.05b$ lynx -noredir -source www.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.ru/">here</A>.
</BODY></HTML>

```

```

fnn@home$>lynx -noredir -source www.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.de/">here</A>.
</BODY></HTML>

```

При совершенно одинаковом запросе в первом случае пользователь был перенаправлен на веб-сайт «www.google.ru», во втором случае — на веб-сайт «www.google.de». Содержимое этих сайтов существенно различается. И не только языком.

Понятно, что контент* одного и того же веб-сайта (на взгляд одного и того же пользователя) может зависеть от времени суток, от просматриваемого сайта пользователя, от некоторых случайных факторов.

Размещение в телеконференции (newsgroup)

Телеконференции* представляют собой систему серверов, объединенных между собой протоколом NNTP [53] и содержащих примерно один и тот же контент. Контент представляет собой множество сообщений (обычно коротких), организованных в группы с иерархической структурой имен [54]. Сообщения — короткоживущие, каждое из них, появившись на любом из серверов, за короткое время (минуты) распространяется по всем остальным, а через несколько дней устаревает и автоматически удаляется. Пользователь может подключиться по тому же протоколу NNTP к любому из серверов и получить с него все или только интересующие группы и отдельные сообщения, а также опубликовать свое сообщение.



Ньюсридер. Слева расположен список групп (телеконференций), на которые подписан пользователь, справа сверху — список доступных сообщений в выбранной телеконференции, справа внизу — выбранное сообщение

Вследствие особенностей используемого протокола, система телеконференций дает относительную анонимность пользователя. Возможно, из-за этого в телеконференциях присутствует значительное количество незаконного и сомнительного контента* — порнографии, контрафактной музыки. Правда, «тяжелый» контент для телеконференций неудобен. Например, фотография объемом 20-50 кбайт вполне помещается в одно сообщение. Музыкальное произведение в формате MP3 объемом 4-5 Мбайт должно быть разделено на несколько сообщений. Чем больше сообщений, тем труднее потом «читателю» собрать вместе исходный файл. Поэтому произведения большого объема, порядка десятков мегабайт и выше, в телеконференциях не публикуются.

Из служебных заголовков сообщения телеконференции можно установить, через какой сервер этой системы (они обычно именуются ньюс-серверами или NNTP-серверами) сообщение было опубликовано. IP-адрес пользователя, опубликовавшего сообщение, в заголовках обычно не фиксируется. Системы аутентификации и авторизации в протоколе NNTP не предусмотрено, только ограничения на основании IP-адреса. Логи, в которых фиксируется, какой пользователь какое сообщение прочитал или опубликовал, серверами ведутся, но далеко не всегда. А когда ведутся, их объем редко позволяет хранить историю более чем за несколько суток.

Ниже приведен пример исходного кода сообщения в телеконференцию со всеми служебными заголовками (часть строк в середине пропущена).

```
Path:
newsfeed.rtcomm.ru!newsfeed.gamma.ru!Gamma.RU!newscon06.news.prodigy.net!pro
digy.net!border1.nntp.dca.giganews.com!nntp.giganews.com!nx01.iad01.new
shosting.com!newshosting.com!post01.iad01!news.usenethost.com!not-for-mail
From: <B-Girl> <wacu28jd@msn.com>
Newsgroups: alt.bainaries.pictures.lolita.fucking
Subject: I filmed myself and want to find another sexy young girl to have
sex fun 00000029.jpg
X-Priority: 3
X-MSMail-Priority: Normal
Date: Thu, 14 Dec 2006 05:19:27
Lines: 848
Message-ID: <457fdd83$0$29368$5ec1c3@news.usenethost.com>
Organization: usenethost
X-Complaints-To: abuse@removethis-usenethost.com
Xref: newsfeed.rtcomm.ru alt.bainaries.pictures.lolita.fucking:21155
```

```
begin 664 47100000029.jpg
M_JC_X`''02D9)1E@!`'0````0`#_VP!#```,`@,`#@,%P,$P,$!0e%!00$
M!OH!P8(#H,#L*"PL-#A(0#Xl#eL+$!80$1,4%145$!~&!84&!(4%13
MVP!#0,$,!$!4!0D%!0D4#0L-!`#4%!04%!04%!04%!04%!04%!04%!04%!04%
N%!04%!04%!04%!04%!04%!04%!04%!3_P`1``'@H`#2(`A$!Q$_\0`
M'0``04!`0$!``````````!`(!08`'0`("?$_%0`'$P,'!0(!P0&
```

MRK&J]"L%#5AP#)9#<' [JK):,'ZXT>-V@0-L'AE[. `X55T^EF9TSOC]7TYP#\AK7>I])9I6A/HR/, <TW+CV6>BAF=25+:+U,=: [2@3/_9

end

<http://www.USENETHOST.com> 100% Uncensored, 100% Anonymous, 5\$/month Only!

Первый служебный заголовок «**Path**» указывает все ньюс-сервера, через которые это сообщение было передано (справа налево, разделенные восклицательным знаком). Видно, что публикация сообщения произведена через сервер **news.usenethost.com**, об этом же свидетельствуют заголовок «**Message-ID**» и подпись в последней строке сообщения. Никаких идентификационных данных пользователя не указано; правда, в поле «**From**» стоит адрес электронной почты, но это поле заполняется пользователем по собственному усмотрению и не проверяется.

В самом сообщении, как видно, кроме последней строчки с автоматической подписью содержится лишь изображение в формате JPEG, кодированное по алгоритму UUENCODE. В телеконференциях для кодирования бинарных данных (протокол NNTP умеет передавать только текст) применяются два алгоритма: «UUENCODE» и «yEnc» [W19]. Первый используется еще с 1970-х, второй введен относительно недавно, в 2001-м.

Для удостоверения наличия определенного контента в телеконференциях можно использовать один из способов, рекомендуемых в предыдущей главе «Размещение на веб-сайте», то есть провести осмотр, нотариальный осмотр или экспертизу. Для проведения осмотра или экспертизы придется подключиться к любому из ньюс-серверов, совсем не обязательно к тому же самому, на котором сообщение было впервые обнаружено. Их контент различается между собой лишь постольку, поскольку различается время хранения сообщений на разных серверах.

Бывают анонимные NNTP-сервера, владельцы которых утверждают, что не ведут логов, и этим стараются привлечь подписчиков.

Чтобы установить источник конкретного сообщения в телеконференцию, надо предпринять следующие действия:

- Получить само сообщение со всеми служебными заголовками. Эти заголовки обычно не показываются программой просмотра (ньюс-ридером*), чтобы их увидеть, надо специально включить соответствующий режим. Как это сделать, зависит от типа ньюс-ридера.
- По заголовкам установить, через какой сервер это сообщение было введено. Заголовок может быть и подложным, если источник предпринимал специальные меры для сохранения анонимности. Для надежности можно получить то же сообщение через несколько ньюс-серверов и сравнить их заголовки.
- Обратиться к администратору того сервера, через который сообщение

было опубликовано, и затребовать логи за соответствующий период. По ним можно установить IP-адрес, с которого сообщение опубликовано.

- Также можно поискать в телеконференциях другие сообщения, принадлежащие, судя по их содержанию, тому же источнику. Если первая попытка установить автора сообщения была неудачной, возможно, он попадет на следующем своем сообщении.

Когда источник установлен, следует изъять компьютер, с которого предположительно публиковалось сообщение в телеконференцию. Экспертиза может установить факт публикации, факт создания сообщения, факт наличия на этом компьютере того же контента, что и в сообщении.

Со стороны сервера факт публикации должен подтверждаться протоколом осмотра или экспертизы логов ньюс-сервера.

Также возможен перехват трафика. По протоколу NNTP сообщения передаются в незашифрованном виде. Экспертиза перехваченного трафика также будет доказательством размещения сообщения.

Если ожидается публикация сообщения в телеконференцию и при этом известен сервер, через который сообщение будет опубликовано, или же известна сеть, из которой оно придет, установить источник можно при помощи ОРМ «снятие информации с технических каналов связи», задействовав для этого СОПМ.

Сообщение в телеконференцию не является сообщением от человека к человеку, поскольку оно адресовано неопределенному кругу лиц. Следовательно, это сообщение не охватывается правом на *тайну связи* (ч. 2 ст. 23 Конституции). Поэтому для отслеживания сообщений лица в телеконференции и его NNTP-трафика не надо получать судебного решения.

Размещение в файлообменных сетях

Термином «файлообменные сети*» (также «пиринговые сети», «P2P-сети») называют семейство программ и протоколов, позволяющих создавать одноранговые¹ сети в пределах глобальной компьютерной сети для обмена файлами, а также сами эти сети. Целями создания и функционирования таких сетей являются надежность, независимость от какого бы то ни было центра, относительная анонимность, возможность функционирования на персональных компьютерах и «узких» каналах связи.

Файлообменные сети возникли в конце 1990-х как реакция сетевой общественности на репрессии по поводу распространения в Интернете контрафактного и иного незаконного и неэтичного контента. Его рас-

¹ Одноранговой называется сеть без выделенных узлов, то есть сеть из равноправных участников (узлов), которые взаимодействуют друг с другом на одинаковых основаниях. Каждый узел в таких сетях выполняет функции как клиента, так и сервера.

пространение через веб- и FTP-сервера легко отслеживается, распространители наказываются, а сервера закрываются.

При распространении файлов через одноранговые пиринговые сети отключение любого числа узлов не влияет на работоспособность сети в целом.

Наиболее известные файлообменные сети:

- Napster — одна из первых файлообменных сетей, ныне не работающая; имела единый центр, из-за чего была закрыта по иску правообладателей;
- eDonkey2000 (сокращенно ed2k) — крупнейшая гибридная файлообменная сеть; поиск выполняют специализированные серверы, связанные между собой; клиенты самостоятельно обмениваются файлами по протоколу MFTP;
- Overnet, Kad — децентрализованные технологии на базе протокола Kademlia, обслуживающие поиск по сети eDonkey (ed2k);
- Bittorrent — сеть, специализированная для распространения файлов большого объема;
- FastTrack, iMesh — первоначально была реализована в KaZaA;
- OpenFT — OpenFastTrack поддерживается клиентами giFT (KCeasy), mlDonkey;
- Gnutella — сеть, использующая протокол, разработанный компанией Nullsoft;
- Gnutella2 — сеть на расширенном протоколе Gnutella;
- Ares — файлообменная сеть для любых файлов с преобладанием музыкальных;
- Freenet, Entropy — анонимные сети;
- MP2P (Manolito P2P) — поддерживается клиентами Blubster, Piolet, RockItNet;
- NEOnet — файлообменная сеть, клиент — Morpheus;
- MUTE — клиенты: MFC Mute, Napshare;
- Nodezilla — анонимная файлообменная сеть.

Всего известно более 40 общедоступных пиринговых сетей.

Каждый желающий участвовать в файлообменной сети устанавливает на свой компьютер программу-клиент, одновременно являющуюся и сервером. Как правило, такие программы создаются энтузиастами и распространяются свободно. Для каждой из сетей существует по несколько различных программ-клиентов под разные операционные системы. Некоторые клиенты поддерживают взаимодействие по нескольким протоколам одновременно.

Клиентской программе достаточно соединиться с одним узлом файлообменной сети, чтобы получить возможность взаимодействовать с лю-

бым ее узлом. После подключения к Сети пользователь получает возможность скачивать к себе на компьютер любые имеющиеся в Сети файлы, а одновременно с этим другие пользователи получают возможность скачивать файлы, имеющиеся у него.

Наиболее известные программы-клиенты файлообменных сетей [W20] (в скобках указаны поддерживаемые сети/протоколы):

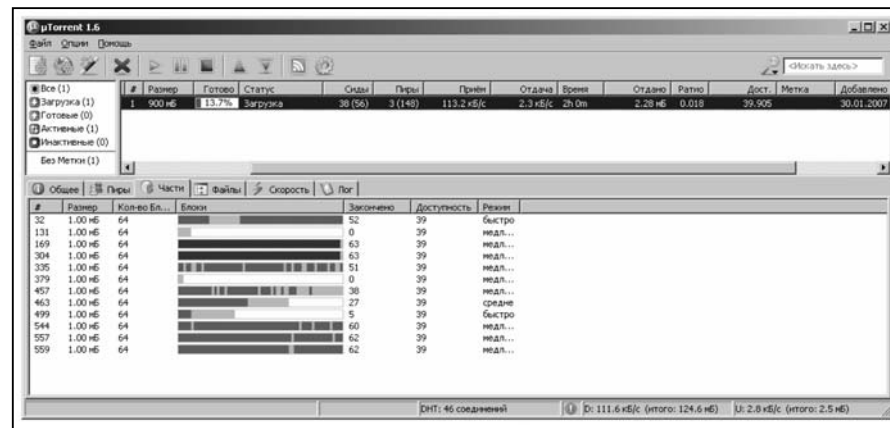
- aMule (eDonkey network, Kad network)
- eMule (eDonkey network, Kad network)
- Shareaza (BitTorrent, eDonkey, Gnutella, Gnutella2)
- FileScope (eDonkey network, Gnutella, Gnutella2, OpenNAP)
- MLDonkey (BitTorrent, Direct Connect, eDonkey network, FastTrack, Gnutella, Gnutella2, Kad Network, OpenNap, SoulSeek, HTTP/FTP)
- Napshare (Key network, MUTE network)
- giFT (eDonkey network, FastTrack, Gnutella)
- Gnucleus (Gnutella, Gnutella2)
- iMesh (FastTrack, eDonkey network, Gnutella, Gnutella2)
- KCeasy (Ares, FastTrack, Gnutella, OpenFT)
- Kiwi Alpha (Gnutella, Gnutella2)
- Morpheus (NEO Network, Gnutella, Gnutella2, BitTorrent)
- Zultrax (Gnutella, ZEPP)

Хотя указанные сети могут оперировать любым контентом*, по понятным причинам, основным контентом в них является незаконный, а также полузаконный, оскорбительный, неэтичный и другой проблемный контент. Обычно распространяются музыкальные MP3-файлы, фильмы, фотографии, дистрибутивы программного обеспечения.



Интерфейс клиента файлообменной сети «e-Mule»

В таких сетях можно найти практически любые произведения, пользующиеся хотя бы минимальным спросом. В том числе самые свежие, только что выпущенные в прокат кинофильмы и музыкальные альбомы. Правообладатели и власти постоянно предпринимают как попытки воспрепятствовать распространению контрафактного контента через такие сети, так и попытки прекратить функционирование файлообменных сетей вообще. Результаты этих усилий пока невелики.



Интерфейс клиента файлообменной сети «Torrent»

Следует заметить, что наряду с описанными файлообменными сетями, ориентированными в основном на контрафактный контент, существуют и небольшие, зато сугубо «законопослушные» сети, действующие с благословения правообладателей. Они используют такие же или сходные технологии, но являются коммерческими проектами. Естественно, имеют встроенные механизмы контроля за авторскими правами на передаваемый контент. Среди таких новых пиринговых сетей можно назвать «YouSendIt», «MediaMax» и «Xunlei» [W21].

Доказательство наличия контента

Доказательством наличия определенного контента в файлообменной сети могут служить свидетельские показания или заключение эксперта.

Поскольку присоединиться к такой сети может любой желающий, а для обычного использования файлообменного ПО специальных знаний не требуется, то не должно возникнуть проблем с обеспечением доказательств наличия контента. Сложнее обстоит дело с выявлением источника этого контента.

Выявление источника

Прежде всего следует заметить, что, поскольку файлообменные сети децентрализованные, понятие «источник файла» в них достаточно условно. Пока какой-либо файл лежит на единственном узле такой сети, этот узел можно назвать источником. При этом информация о файле (индексная информация) распространяется по всей сети. Но каждый узел, который начинает загрузку этого файла, сам в тот же момент становится его источником, неотличимым от первичного. По окончании полной загрузки файла узел либо продолжает служить его источником, либо прекращает — в зависимости от решения пользователя. Понятно, что пользующийся спросом файл, только появившись в файлообменной сети, сразу же начинает закачиваться множеством узлов и приобретает в их лице множество источников.

Поэтому не имеет смысла говорить о первичном источнике какого-либо файла.

Можно говорить лишь о нахождении файла (фрагментов файла) на конкретном узле и его доступности другим.

Передача же файла происходит обычно напрямую между узлами. Тогда можно определить IP-адрес узла-источника. Другой информации об этом узле, как правило, получить не удастся.

Некоторые файлообменные сети не позволяют легко определить источник файла. Любой узел в таких сетях может выступать посредником при передаче, скрывая истинный источник. Это посредничество — чисто техническая особенность, не зависящая от воли пользователя. Поэтому хотя узел с технической точки зрения является посредником, с юридической точки зрения его владелец или оператор посредником не является, не имеет прямого умысла на такое посредничество и даже косвенного умысла не всегда имеет.

Таким образом, в ряде случаев мы имеем возможность относительно просто определить IP-адрес узла файлообменной сети, являющегося источником определенного файла. В других случаях (с узлами-посредниками) определение источника сильно затруднено. Определить же первичный или оригинальный источник файла не представляется возможным.

Доказательство использования

Доказательством того факта, что известное лицо использовало файлообменные сети, может служить следующее:

- протокол экспертизы компьютера интересующего нас лица, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей и это ПО использовалось по назначению;

- показания иного участника файлообменной сети о том, что он взаимодействовал в этой сети с узлом, имеющим тот же IP-адрес, что использовался интересующим нас лицом;
- протокол экспертизы компьютера иного участника файлообменной сети, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей, это ПО использовалось по назначению и обнаружены следы взаимодействия с IP-адресом интересующего нас лица;
- протокол осмотра или экспертизы компьютера оператора связи (провайдера), где зафиксировано наличие логов, отражающих информацию о трафике IP-адреса интересующего нас лица, причем в этом трафике присутствовали характерные для файлообменных сетей особенности (протоколы, порты, IP-адреса популярных узлов).

Следует упомянуть, что трафик файлообменных сетей не является тайной связи (ч. 2 ст. 23 Конституции), поскольку не относится к общению между человеком и человеком. Следовательно, для ознакомления с ним не требуется судебного решения. Однако такой трафик является тайной частной жизни (ч. 1 ст. 23 Конституции).

Виды преступлений

Некоторые считают файлообменные сети принципиально криминальными, поскольку легальный контент в них встречается редко, а основной трафик составляет в той или иной степени нелегальный. Утверждают, что именно ради такого контента файлообменные сети созданы и только ради него существуют.

Такая точка зрения не является общепринятой. Оппоненты возражают, что нелегального контента там не так уж много, а созданы файлообменные сети не только ради безнаказанности. Они имеют существенные преимущества перед другими способами распространения файлов, а именно, возможность быстро распространять большие объемы информации одновременно многим пользователям при использовании слабых и ненадежных каналов связи при периодической недоступности многих узлов.

Как бы то ни было, действующие на сегодня файлообменные сети сами по себе не поставлены под запрет ни в одной стране. Преследуются только правонарушения, совершаемые с их использованием.

Основными преступлениями, связанными с этими сетями, являются: нарушение авторских прав и распространение порнографии.

Контент и доменное имя

Правовая защита домена

Система доменных имен была придумана для облегчения запоминания человеком сетевых адресов. С массовым развитием системы WWW и с коммерциализацией Интернета доменное имя приобрело коммерческую ценность. А ценности нуждаются в законодательной защите. Тем более что стоимость самых дорогих доменных имен может исчисляться миллионами долларов. И законодательная защита была дана. Ныне домен — не просто удобная для человека форма сетевой адресации, но объект интеллектуальной собственности.

В одних странах отношения по поводу доменных имен сети Интернет напрямую регулируются законодательством, в других странах домены охраняются в числе прочих средств индивидуализации. В России доменное имя упоминается в законе «О товарных знаках...». В проекте части 4 Гражданского кодекса (вступает в силу с 2008 года) сначала присутствовала целая глава о доменных именах, но она была исключена при втором чтении. Тем не менее упоминание доменных имен как объекта регулирования осталось.

Путаница сайта и ДИ

Часто отождествляют веб-сайт и доменное имя, под которым этот сайт живет. На самом деле веб-сайт и домен — разные сущности как с технической, так и с правовой точки зрения.

Описанная путаница — следствие не только слабого понимания технических вопросов функционирования веб-сайтов. Неверному пониманию и отождествлению доменного имени и веб-сайта способствуют некоторые юристы, представляющие истцов по гражданским делам, связанным с веб-сайтами и информацией на них.

Как известно, обязанность найти ответчика лежит на истце. Его следует не просто найти, а представить суду доказательства того, что веб-сайт принадлежит ему. Веб-сайты не подлежат обязательной регистрации, нет никакой системы учета сайтов и их владельцев. А провайдеры (операторы связи) весьма неохотно сообщают данные о своих клиентах, ссылаясь на коммерческую тайну или защиту персональных данных.

В противоположность этому владельца доменного имени 2-го уровня узнать легко. Сведения о нем содержатся в общедоступной базе данных регистраторов доменных имен. Получить письменную справку с такими сведениями также несложно — распечатку с публичными данными сервиса whois легко заверит любой регистратор.

Таким образом, обстоятельства диктуют представителям истцов реше-

ние — назначить ответчиком не владельца веб-сайта, а владельца соответствующего домена.

Надо признать, что в большинстве случаев владелец домена 2-го уровня и владелец живущего на этом домене веб-сайта — одно и то же лицо. В большинстве случаев, но далеко не всегда. Кроме того, большинство веб-сайтов живут на домене не 2-го уровня, а 3-го. То есть на домене вида «www.example.com». Несмотря на то, что «www» — это стандартное имя 3-го уровня для веб-сайта, владельцы «www.example.com» и «example.com» могут быть разными.

Также далеко не всегда совпадают владелец веб-сайта и владелец размещенного на этом сайте контента*.

Для гражданских дел можно попытаться возложить ответственность за контент сайта на владельца этого сайта, на оператора связи или даже на владельца доменного имени. За то, что создали условия размещения, не воспрепятствовали и т.д. В ряде случаев такое возложение ответственности истцам удавалось. Но для уголовных дел подобная натяжка не пройдет. Ответственность может нести только лицо, разместившее информацию на веб-сайте. В отношении владельца сайта, его провайдера, владельца домена можно говорить лишь о соучастии, и то — в весьма редких случаях.

Примеры

Ниже приводится образец нотариального протокола осмотра веб-сайта. Как указывалось ранее, нотариус не в состоянии обеспечить полную достоверность при фиксации содержимого (контента) веб-сайта. Нотариус не проверяет правильность разрешения доменного имени, не может противостоять различным способам подмены контента, не контролирует актуальность содержимого (отсутствие кэширования), не проверяет, отличается ли контент, отдаваемый пользователям из разных регионов, и так далее. Тем не менее достоверность такого осмотра — на достаточном уровне. Автору не известны случаи, чтобы суд отклонял такое доказательство по вышеуказанным мотивам.

Тем не менее, чтобы застраховаться от возможных ошибок или злонамеренных действий, в осмотре может участвовать и специалист. Ниже приводится образец протокола осмотра веб-сайта нотариусом совместно со специалистом.

**ПРОТОКОЛ
ОСМОТРА ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ**

Город Москва, двадцать седьмое февраля две тысячи седьмого года.

Я, Карпов Николай Васильевич нотариус г. Москвы, руководствуясь ст. ст. 102, 103 Основ законодательства РФ о нотариате, с участием заинтересованного лица — СЕРГО АНТОНА ГЕННАДЬЕВИЧА, 21 января 1978 года рождения, проживающего по адресу: г. Москва, [адрес], паспорт [номер], выдан паспортным столом № 1 ОВД района Теплый стан г. Москвы 13 сентября 2002 года, действующего от юридической фирмы АНО «Интернет и Право», произвел осмотр вещественных доказательств с использованием персонального компьютера, подключенного к сети Интернет с использованием программы Microsoft Internet Explorer по адресу:

- [http://www.\[адрес\].ru](http://www.[адрес].ru)
- и по ссылкам:
- Ссылка «О компании»: [http://www.\[адрес\].ru/index.html](http://www.[адрес].ru/index.html)
- Ссылка «Каталог продукции»: [http://www.\[адрес\].ru/catalog.html](http://www.[адрес].ru/catalog.html)
- Ссылка «Сертификаты»: [http://www.\[адрес\].ru/sertifikat.html](http://www.[адрес].ru/sertifikat.html)
- Ссылка «Проекты»: [http://www.\[адрес\].ru/proekt.html](http://www.[адрес].ru/proekt.html)
- Ссылка «Перспективы»: [http://www.\[адрес\].ru/prospekt.html](http://www.[адрес].ru/prospekt.html)
- Ссылка «Контакты»: [http://www.\[адрес\].ru/contact.html](http://www.[адрес].ru/contact.html)

При введении в строку адреса программы Microsoft «Internet Explorer» интернет-адреса [http://\[адрес\].ru](http://[адрес].ru) произошел автоматический переход на сайт [http://www.\[адрес\].ru](http://www.[адрес].ru). То есть при вводе [http://\[адрес\].ru](http://[адрес].ru) пользователь Интернет автоматически оказывается на сайте [http://www.\[адрес\].ru](http://www.[адрес].ru), который называется: «[название]» - дистрибьютор компании [название].

Затем был осуществлен переход по ссылкам:

- «О компании» (Интернет-адрес: [http://www.\[адрес\].ru/index.html](http://www.[адрес].ru/index.html)),
- «Каталог продукции» (Интернет-адрес: [http://www.\[адрес\].ru/catalog.html](http://www.[адрес].ru/catalog.html)),
- «Сертификаты» (Интернет-адрес: [http://www.\[адрес\].ru/sertifikat.html](http://www.[адрес].ru/sertifikat.html)),
- «Проекты» (Интернет-адрес: [http://www.\[адрес\].ru/proekt.html](http://www.[адрес].ru/proekt.html)),
- «Перспективы» (Интернет-адрес: [http://www.\[адрес\].ru/prospekt.html](http://www.[адрес].ru/prospekt.html)),
- «Контакты» (Интернет-адрес: [http://www.\[адрес\].ru/contact.html](http://www.[адрес].ru/contact.html))

Все указанные страницы озаглавлены одинаково: «[название]» - дистрибьютор компании [название].

Все осматриваемые на интернет-сайте страницы распечатаны, прошиты и скреплены печатью.

Осмотр вещественных доказательств производился по заявлению АНО «Интернет и право» в лице СЕРГО АНТОНА ГЕННАДЬЕВИЧА от 22 февраля 2007 года, в помещении нотариальной конторы по адресу: г. Москва, Ленинградский пр-кт, д. 75/16.

Другие заинтересованные лица, разместившие вышеуказанную информацию на интернет-сайте, не извещены о предстоящем осмотре вещественных доказательств по заявлению АНО «Интернет и право» в лице СЕРГО АНТОНА ГЕННАДЬЕВИЧА. Просьба обоснованна тем что, уничтожение заинтересованным лицом вышеуказанной информации является единственной возможностью уйти от ответственности, кроме того, само уничтожение не представляет трудности, а значит, реальна степень угрозы невозможности получения доказательств в будущем.

Осмотр был произведен 27 февраля 2007 года в 16 часов 00 минут и окончен в 16 часов 15 минут. Настоящий протокол осмотра вещественных доказательств с распечатанными страницами интернет-сайтов составлен в двух экземплярах, один из которых хранится в делах нотариуса г. Москвы Карпова Н.В. по адресу: г. Москва, Ленинградский п-кт, д. 75/16, а другой выдается СЕРГО АНТОНУ ГЕННАДЬЕВИЧУ.

Серго Антон Геннадьевич



Город Москва, двадцать седьмое февраля две тысячи седьмого года.

Личность СЕРГО АНТОНА ГЕННАДЬЕВИЧА, подписавшего протокол установлена, дееспособность проверена.

Зарегистрировано в реестре за № 1-6192

Взысканно тарифу 500 руб. + 3000 руб. прав. тех. усл.

Нотариус

Заключение к разделу 4

Для доказательства факта размещения той или иной информации в Сети до сих пор не выработано единого подхода. Применяются различные методы: свидетельские показания, протоколы осмотра, нотариальные протоколы, заключения эксперта. Ни один из этих методов нельзя назвать безупречным. Главная трудность в том, что между размещенной информацией и глазами пользователя (нотариуса, эксперта) находятся многочисленные технические посредники. Проходя через них, данные претерпевают неоднократные преобразования, сложным образом маршрутизируются, переадресовываются, декодируются, представляются. В результате то изображение, которое предстает на экране компьютера, может относиться к оригинальной размещенной в сети информации весьма опосредованно. И к тому же варьироваться в зависимости от различных неконтролируемых пользователем факторов.

Поэтому на сегодняшний день задача заверения сетевого контента решается не вполне строго. Автор рекомендует компенсировать эту нестрогость дополнительными независимыми доказательствами, дополнительными источниками, просмотром из различных точек Сети, различными средствами. Иными словами, восполнять недостаток качества количеством.