В. Л. Никитина

О КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ И УГРОЗ В СЕТИ ИНТЕРНЕТ

Информационные отношения в глобальной сети Интернет могут быть классифицированы по признакам субъектного состава (потребитель — посредник — государственный орган, или абонент (пользователь) — оператор связи — госорган) и по признакам информационного процесса (рецепция — интерпретация — коммуникация, или получение — использование — распространение), посредством которого удовлетворяются информационные интересы в информационных отношениях. Информационный процесс в сети Интернет — это явление, включающее в себя хотя бы один из следующих элементов: прием информации, использование информации, распространение (в том числе и передача) информации. По каждому такому элементу между субъектами сети Интернет возникают информационные отношения.

При осуществлении правового регулирования информационных отношений возникают информационные правоотношения, характеризующиеся юридически закрепленными правами и обязанностями субъектов таких отношений, возможностью юридической защиты своих информационных интересов.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах (в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ):

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только законами;

3) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица и др.

С целью выявления юридически значимых свойств таких отношений необходимо рассмотреть содержание информационных отношений абонента и оператора интернет-связи. В него входят информационные интересы (мотивы), которые обусловливают деятельность абонента и оператора интернет-связи, направленную на осуществление информационного обмена, и действия, реализующие эти информационные интересы. Действия абонента и оператора интернет-связи, направленные на реализацию их информационных интересов, взаимосвязаны и выражаются в виде услуг интернет-связи.

Существует определенное разделение операторов интернет-связи по типу оказываемых услуг. Первый тип операторов интернет-связи оказывает услугу, суть которой заключается в создании соединения между компьютером абонента и сетью Интернет, а также в обеспечении передачи данных. При этом используются как обычные телефонные, так и специально проведенные (выделенные) линии. Абонент может просматривать содержание веб-страниц, получать и отправлять электронные сообщения и файлы. Второй тип операторов интернет-связи помимо услуги доступа предоставляет абоненту еще и услугу пользования приложениями (программными средствами), размещенными на аппаратных средствах оператора интернет-связи. Это операторы доступа к приложениям. Поскольку в качестве абонента в нашем случае подразумевается физическое лицо, не осуществляющее коммерческую деятельность через Интернет, оно заинтересовано только в одной услуге, которую может предоставить данный оператор, — размещение и поддержка веб-страницы (или веб-сайта). Эта задача может быть выполнена абонентом при пользовании услугой, называемой хостингом.

Рассмотрев услуги, оказываемые оператором интернет-связи абоненту, а также их действия в отношениях между собой, следует уделить внимание возможным действиям указанных субъектов при взаимоотношениях с государственными правоохранительными органами.

Под государственными правоохранительными органами в данной работе будут пониматься органы МВД РФ, ФСБ РФ и иные органы, к обязанностям которых относится защита информационных интересов граждан, общества и государства. Указанные органы наделены государством полномочиями по охране интересов граждан, организаций и государства. При нарушении информационных интересов субъектов информационного обмена в сети Интернет правоохранительный орган может потребовать интересующую его информацию, которая имеет отношение к абоненту Интернета или его деятельности в Глобальной сети, как от оператора интернет-связи, так и от абонента.

Для личности существует достаточно много угроз ее информационной безопасности. Такие угрозы существуют как в реальной окружающей среде, так и в виртуальной компьютерной.

Все угрозы, возникающие в процессе реализации информационных отношений, можно разделить на угрозы уничтожения информации абонента и угрозы воздействия вредной информации на абонента. Под вредной информацией следует понимать такую информацию, восприятие которой может нанести ущерб психическому, психологическому, нравственному, физическому, материальному состоянию личности. К числу действий, в результате осуществления которых могут возникнуть данные угрозы, можно отнести: просмотр веб-страниц, получение электронных сообщений, отправку электронных сообщений, опубликование веб-страницы в Интернете и др.

Угрозы, перечисленные ниже, относятся к ситуации, когда абонент сам выполняет все указанные действия. *Всего таких угроз 9: в случае*

просмотра абонентом веб-страниц

1) вредная информация, размещенная непосредственно на странице (фото, видео, аудио, текстовые данные),

2) вредные программные коды, активизируемые при обращении по ссылке, расположенной на странице;

получения электронных сообщений

3) вредная информация, размещенная в электронном сообщении,

4) получение вирусов,

5) получение незапрашиваемой информации (СПАМ);

отправки электронных сообщений

6) несвоевременная отправка или недоставка сообщений,

7) просмотр содержания письма;

опубликования веб-страницы

8) недоступность веб-страницы,

9) изменение информации, содержащейся на веб-странице, или полное уничтожение таковой.

Существуют также угрозы информационной безопасности личности, реализация которых происходит независимо от действий абонента. К числу таких угроз относятся диффамация, нарушение авторских прав и распространение персональных данных (без согласия лица). Диффамация — распространение порочащих сведений, но, в отличие от клеветы, порочащие сведения могут и не носить клеветнического характера.

Следует сказать еще об одной угрозе, которая в равной степени может как зависеть, так и не зависеть от действий абонента в сети Интернет. Речь идет об угрозе несанкционированного доступа к информации, находящейся в компьютере абонента. Такая угроза может быть реализована путем подключения к компьютеру абонента через сеть Интернет. В этом случае от абонента не требуется никаких действий, кроме как установления связи с сетью Интернет.

Рассмотрим примеры из практики информационных отношений и угроз в сети Интернет.

1. Возложение на операторов интернет-связи обязанностей по контролю за содержанием передаваемой информации. Япония выразила намерение вести борьбу с опасной информацией в сети Интернет. К информации, которой не место в он-лайне, относятся, например, призывы к коллективным самоубийствам и инструкции по созданию взрывных устройств. В правительстве создана специальная рабочая группа для выработки соответствующих рекомендаций. В частности, планируется стимулировать использование операторами интернет-связи специального программного обеспечения, отфильтровывающего нежелательный контент.

2. Размещение незаконной информации в сети Интернет. Двадцатилетний Шерман Остин, опубликовавший в Сети информацию по классификации взрывчатых веществ и изготовлению самодельных бомб, осужден окружным судом Лос-Анджелеса на годичный срок заключения в тюрьме. Шерман отметил, что не задумывался о возможных последствиях, когда делал свой сайт. Собрав опубликованные ссылки о бомбах и взрывчатых веществах, использовавшихся на демонстрациях антиглобалистов, он ставил перед собой цель показать людям «зверства полиции».

Подводя итог вышесказанному, следует отметить, что в современном мире информация и информационные отношения получают все большее распространение и становятся неотъемлемой частью нашей жизни. Особенно стремительно этот процесс начал развиваться с появлением глобальной сети Интернет. Вместе с этим растет и число угроз различных масштабов, связанных с нарушением прав участников информационных отношений. Для их предотвращения необходимо осуществлять контроль за использованием и распространением информации. Для этого должны появиться новые технологические стандарты по целому ряду направлений, в первую очередь в сфере интернет-технологий, равно как необходимо внести изменения в ряд действующих федеральных законов: КоАП РФ, закон «О защите прав потребителей», УК РФ и др.

СПИСОК ЛИТЕРАТУРЫ:

1. Япония будет бороться с опасной информацией в Интернете. URL: http://net.compulenta.ru/189500/.
2. Создатель анархического веб-сайта осужден на год тюремного заключения. URL: http://www.compulenta.ru/2003/8/5/41179/.
3. *Крылов Г. О.* Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации. АКД. М., 2007.