УДК 519.7

В.А. Голубев

Запорожский национальный университет, Запорожье

НЕКОТОРЫЕ ПРОБЛЕМЫ БОРЬБЫ С ИНТЕРНЕТ-ПРЕСТУПНОСТЬЮ

Расширение возможностей Интернета делает общество уязвимым перед угрозой кибертерроризма и компьютерной преступности. Специалисты Центра реагирования на инциденты, связанные с киберпространством (Cyber Terror Response Center), обращают внимание на то обстоятельство, что количество уголовных дел, возбужденных в 2009 году по фактам совершения компьютерных преступлений в Интернете возросло до 60000. Это приблизительно в 500 раз больше, нежели в 2001 году. По прогнозам специалистов в 2010 году к Интернету будет подключено более 1 млрд. компьютеров. Ежеквартальный объем данных, передаваемых через Интернет, удваивается, и сегодня уже можно говорить о реальной зависимости развитых стран от надежности международной информационной инфраструктуры.

Учитывая фактор глобализации Интернет-преступности, все более очевидным становится то, что ни одно государство сегодня уже не способно самостоятельно противостоять этой опасности. В связи с чем неотложной проблемой становится необходимость активизации международного сотрудничества в этой сфере. Существенное место в таком сотрудничестве принадлежит международно-правовым механизмам регулирования и взаимодействия правоохранительных органов в вопросах противодействия и расследования компьютерных преступлений.

Транснациональный характер киберпреступности дает основания считать, что разработка общей политики по основным вопросам должна быть частью любой стратегии борьбы и противодействия. Такая общая политика имеет важное значение для предотвращения возникновения "правовой крыши", в частности, в рамках тех правовых систем (юрисдикций), в которых определенные действия не криминализованы.

Большую роль в вопросах международного сотрудничества в борьбе с киберперступностью продолжает играть Организация Объединенных Наций, в рамках которой на протяжении последних 10 лет подготовлено и принято ряд очень важных документов по вопросам предупреждения преступлений, связанных с применением компьютеров и борьбе с ними, а также ряд международных соглашений направленных на сотрудничество в противодействии компьютерной преступности.

Международные компьютерные сети позволяют осуществлять деятельность на такой территории, где может действовать (намеренно или непреднамеренно) принцип экстерриториальности. Например, правоохранительные органы одного государства могут получать данные из компьютерной сети в рамках правомерного поиска компьютерной информации в этом государстве, но при этом устанавливать, что некоторые из полученных данных были сохранены в рамках сети другого государства и защищены законами этого государства.

Аналогичным образом государство может правомерно перехватывать электронные сообщения, проходящие через ее территорию, даже если такими сообщениями обмениваются лица, расположенные в других государствах, где они пользуются правовой защитой от произвольного вмешательства такого государства в сферу частной связи. Работающие в сети сотрудники правоохранительных учреждений

также могут осуществлять скрытные действия в соответствии с законодательством своих стран на условиях, в которых такие действия или методы не допускались бы законодательством других государств, где они действуют. Все эти сценарии являются новыми, не имеют параллелей и в международном праве в настоящее время не предусмотрено оказание существенной помощи или рекомендаций в отношении решения возникающих проблем.

Кроме того, отсутствует широкий консенсус в отношении возможного устранения трансграничных последствий правомерно применяемых следственных действий внутреннего характера. Общепризнано, что государство правомочно применять на своей территории, на которой оно обладает исключительной юрисдикцией, следственные действия или принудительные меры в отношении любого из своих граждан. В результате применения таких полномочий могут возникать случаи, когда размещенные на другой территории данные считываются и копируются или, возможно, уничтожаются. С точки зрения государства, в котором велся поиск данных, такие действия могут образовывать состав уголовного преступления в соответствии с внутренним уголовным правом, а также являться нарушением национального суверенитета.

В то же время, согласно другому мнению, международное право не запрещает такое вмешательство, поскольку с технической точки зрения такие данные доступны и могут быть получены из государства, осуществляющего их поиск, без какой-либо помощи или вмешательства со стороны государства, где осуществляется поиск таких данных. Имеющиеся в любых разделах сети данные можно рассматривать как общедоступные, и по этой причине вопрос о доступе к ним из любого государства, в котором они в настоящее время находятся, регулируется исключительно внутренним, а не международным правом. С такой точки зрения обращение к государству, где осуществляется поиск данных, не является необходимым ни на одном из этапов деятельности. Согласно международному праву, по-прежнему неоднозначен вопрос о том, в какой мере данные являются или не являются общедоступными (например, лица, осуществляющие поиск данных, фактически должны загружать их из сервера одной страны в другую страну).

В заключение необходимо особо подчеркнуть, что киберпреступность все чаще приобретает транснациональный и трансграничный характер. С использованием глобальной информационной сети Интернет такие виды преступлений не имеют государственных границ и могут легко совершаться с компьютерной системы одного государства в отношении субъектов другого государства. С учетом этого, стратегия борьбы с Интернет-преступностью должна строится на посылке о том, что данной проблемой необходимо заниматься целостно, а это, в свою очередь, требует тесного сотрудничества, как на национальном, так и на международном уровне.