

**Выступление М.И. Гришанкова на
Первом российском форуме по управлению Интернетом
(Москва, 13-14 мая 2010 года)**

**Уважаемые гости и участники Первого российского форума по
вопросам управления Интернетом!**

Прежде всего, хочу поблагодарить организаторов за приглашение к участию и отметить, что наш форум – это важный этап реализации планов построения глобального информационного общества на основе принципов, утвержденных на Всемирной встрече на высшем уровне по вопросам информационного общества. Россия активно участвует в этих процессах, как на государственном уровне, так и на уровне институтов гражданского общества.

Одним из принципов построения информационного общества является, как известно, укрепление доверия и безопасности при использовании информационно-коммуникационных технологий, формирование глобальной культуры кибербезопасности на основе расширяющегося международного сотрудничества.

Если процессы глобализации были стимулированы изначально защитой окружающей среды (Рамочная конвенция ООН 1992 года, Декларация ООН 1997 года, Киотский протокол 1997 года), то развитие Интернета явилось, как мне представляется, катализатором этого процесса. Действительно, невозможно ограничить государственными границами движение воздушных масс и так же невозможно ограничить распространение информации с

использованием современной инфо-коммуникационной инфраструктуры.

Таким образом, отличительным признаком Интернета является его экстерриториальность. Это и основное достоинство, и основная проблема — проблема правовая, поскольку национальное законодательство распространяется только на субъектов, находящихся под его юрисдикцией.

Вместе с тем, технологические особенности Интернета позволяют игнорировать привычные юридические конструкции (территориальную юрисдикцию, административные границы и т.п.). Такие возможности используют, прежде всего, киберпреступники. Количество преступлений с использованием Интернета динамично растет. В прошлом году в России прирост составил 30%, при этом более 70% преступлений – совершено с использованием Сети и они, преимущественно, носят трансграничный характер.

О чем это свидетельствует? О том, что роль национального законодательства в защите прав и законных интересов пользователей Сети снижается. На первый план выходят инструменты межгосударственного (международного) регулирования, объединения усилий мирового сообщества для борьбы с киберпреступностью, кибертерроризмом и иными правонарушениями в Сети. Эти усилия пока носят региональный характер. Примером может быть Европейская конвенция по киберпреступности 2001 года.

Ряд важнейших международных документов был принят по инициативе России в рамках Содружества Независимых Государств, Организации Договора о коллективной безопасности (ОДКБ) и Шанхайской организации сотрудничества. В частности, в 2008 году

утверждены Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности и Комплексный план мероприятий по ее реализации на период с 2008 по 2010 год. Решением Совета коллективной безопасности ОДКБ утверждена также в 2008 году Программа совместных действий по формированию системы информационной безопасности государств-членов ОДКБ. 16 июня 2009 года на саммите ШОС было подписано Соглашение о сотрудничестве в области обеспечения международной информационной безопасности.

Россия является также инициатором Резолюции ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятой Генассамблеей ООН в декабре 2008 года, за которую проголосовало 178 государств, за исключением США.

Россия поддерживает лидирующую роль Международного союза электросвязи (МСЭ) в разработке международных актов, посвященных укреплению доверия и безопасности при использовании ИКТ.

Принятая МСЭ Глобальная программа кибербезопасности содержит стратегические цели и принципы кибербезопасности, предоставляет основу для установления диалога, направленного на максимально эффективную реализацию существующих инициатив и развитие сотрудничества в целях разработки глобальных стратегий для укрепления доверия и безопасности в информационном обществе.

Вместе с тем, при формировании глобальной системы кибербезопасности необходимо однозначно определиться с

терминологией, а также с видами угроз, на устранение которых она будет направлена. Помимо киберпреступности и кибертерроризма сама жизнь в глобальном информационном пространстве заставляет нас думать об угрозах военно-политического характера, таких как разработка и применение информационного оружия, подготовка и ведение информационных войн. Такие угрозы нельзя сбрасывать со счетов, тем более, что попытки использования информационного оружия уже имеют место.

Острой проблемой, с которой столкнулось мировое сообщество, стала проблема распространения в Сети материалов противоправного содержания. Это и детская порнография, и материалы экстремистского характера, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, информация, нарушающая неприкосновенность частной жизни.

Оказалось, что российское законодательство, несмотря на наличие соответствующих запретов в ряде федеральных законов и норм юридической ответственности, недостаточно эффективно работает в случаях, когда подобные материалы распространяются с использованием сети Интернет. Причин, возможно, несколько, но мне важной представляется отсутствие должного субъекта ответственности.

Законодательство о связи выделяет пару субъектов: пользователь услугами связи и оператор связи, то есть лицо, оказывающие услуги связи на основании соответствующей лицензии. В Интернете эти услуги ограничены деятельностью по приему, обработке, хранению, передаче, доставке сообщений электросвязи.

При этом, во-первых, субъекты, предоставляющие бесплатные сервисы, не обязаны получать лицензию и не подпадают под действие законодательства о связи. Во-вторых, очевидно, что оператор связи не может отвечать за содержание передаваемой информации. И в-третьих, в Интернете действуют субъекты (так называемые хостинг-провайдеры, контент-провайдеры, сервис-провайдеры), которых нельзя отнести к операторам связи. Таким образом закрепление в законодательстве правового статуса этих субъектов, так или иначе связанных с размещением информации, доступной неограниченному числу пользователей Интернета, позволит определить субъекта ответственности за распространение материалов противоправного содержания.

Наряду с этим, необходимо иметь в виду, что реализация существующих ограничений не всегда эффективна как раз «благодаря» технологии распространения. Ведь можно заблокировать экстремистский ресурс (сайт в Интернете), можно даже добиться его закрытия, однако информация не уничтожима в силу легкости копирования – она может возникнуть на другом сайте, зарегистрированном в иной стране, где оценка содержания информации может быть противоположной. Именно с этой проблемой столкнулись правоохранительные органы, когда пытались закрыть сайт чеченских экстремистов, располагавшийся за пределами территории России. Согласование подходов к оценке содержания противоправной информации это также одно из направлений международного сотрудничества.

Необходимо отметить, что выявление противоправного контента – задача для органов власти дорогостоящая и трудоемкая.

Здесь большое поле деятельности для организаций гражданского общества. Подобные организации созданы и в России. В феврале мы подводили итоги Года безопасного Интернета в России, где были представлены и результаты деятельности таких организаций. Эти результаты очень обнадеживают.

Представители правоохранительных органов давно сталкиваются с проблемой идентификации владельца сайта (владельца информационного ресурса) в процессе расследований и привлечения к ответственности нарушителей закона. Существующая система выделения доменных имен предусматривает представление документов удостоверяющих личность и проверку представленной информации. Однако учитывая, что заявки на регистрацию доменного имени подаются в электронном виде и не отлажена система проверки достоверности представляемой информации, эти данные могут быть недостоверными. Система регистрации доменных имен во всем мире регулируется некоммерческими организациями, действующими согласованно.

Не меняя принципиально сложившийся порядок, представляется все же целесообразным законодательно закрепить требования к идентификации субъектов, представляющих свои ресурсы для распространения информации или распространяющих информацию в Интернете. Более того, в Сети достаточно давно обсуждаются вопросы идентификации пользователя, а в ряде стран она существует. Анонимность пользователя уже сейчас весьма относительна: ваши действия фиксирует провайдер, владельцы бесплатных почтовых серверов, Интернет-магазинов, да и других сайтов. В то же время, анонимность позволяет развиваться компьютерной преступности в

виде: распространения вирусов, нарушения авторских и смежных прав, экстремизма, терроризма, спама, D-Dos атак и т.п. Сложно ограничить доступ несовершеннолетних к развращающей их информации. Таким образом, анонимность выгодна, прежде всего, нарушителям законов.

У этой проблемы есть обратная сторона. Усиление идентификации пользователя увеличит объемы персональных данных, накапливаемых различными субъектами правоотношений с использованием Интернета. В этой связи на первый план выходит задача совершенствования законодательства о персональных данных и эффективной его реализации, которая, в свою очередь, также зависит от закрепления правового статуса субъектов, осуществляющих свою деятельности исключительно через Интернет. Необходимо добиться, чтобы любой субъект экономической деятельности подчинялся закону независимо от того, каким способом эта деятельность осуществляется (традиционно или с использованием Сети).

И последнее, обсуждая проблемы развития Интернета и управления его развитием, всегда надо помнить, что право это не единственный регулятор общественных отношений. Немаловажную роль в этом играют корпоративные и профессиональные этические нормы, знания пользователей Сети об опасностях, которые несут глобальные коммуникации и умение от них защищаться и их предотвращать, то есть то, что в документах WSIS названо культурой кибербезопасности.

Подводя итог сказанному, считаю необходимым отметить, что одним из направлений деятельности по управлению Интернетом

должно быть формирование глобальной системы кибербезопасности, включающей разработку правовых, технических и процедурных мер, создание организационных структур, развитие культуры кибербезопасности и механизмов международного сотрудничества.

Хочу пожелать участникам форума успешной работы!