



Утверждены Приказом директора ЗАО "Ориент-Телеком"  
№1112-1-ДО от 12 декабря 2011 года

## Нормы пользования Сетью

Сеть Интернет (далее "Сеть") представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования Сетью не установлено. Существуют, однако, общепринятые нормы работы в Сети (далее "Нормы"), направленные на то, чтобы деятельность каждого пользователя Сети не мешала работе других пользователей.

Фундаментальное положение этих Норм таково: правила использования любых ресурсов сети Интернет определяют владельцы этих ресурсов и только они (здесь и далее словом "ресурс" обозначается любая совокупность программных и аппаратных средств, составляющих в том или ином смысле единое целое). Ресурсом сети Интернет могут считаться, например, сайт или портал, почтовый ящик, персональный компьютер, виртуальный или физический сервер, локальная вычислительная сеть, канал связи и т.д.

Настоящий документ представляет собой формальное описание Норм сетевого взаимодействия, считающихся в большинстве сетей (как входящих в сеть Интернет непосредственно, так и доступных из сети Интернет тем или иным опосредованным образом) обязательными к исполнению всеми пользователями. Такие или аналогичные Нормы применяются в отношении всех доступных сетевых ресурсов, когда заранее не известны правила, установленные владельцами этих ресурсов самостоятельно.

### 1. Ограничения на информационный шум (спам)

Развитие Сети привело к тому, что одной из основных проблем пользователей стал избыток информации. Поэтому сетевое сообщество выработало специальные правила, направленные на ограждение пользователя от ненужной/незапрошенной информации (спама). Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств персонального обмена информацией. В частности, являются недопустимыми:

- Массовая рассылка несогласованных предварительно с получателями электронных писем (mass mailing), при условии, что такая несогласованная рассылка порождает жалобы получателей. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю.
- Несогласованная с получателем рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения.
- Рассылка сообщений, содержащих просьбу переслать данное сообщение другим доступным пользователям (chain letters).
- Использование безличных ("ролевых") адресов иначе, как по их прямому назначению, установленному владельцем адресов и/или стандартами.
- Размещение в любой электронной конференции сообщений, которые не соответствуют тематике данной конференции (off-topic), при условии, что эти факты порождают жалобы модератора конференции, если он есть. Здесь и далее под конференцией понимаются телеконференции (группы новостей) Usenet и другие конференции, форумы и списки рассылки.
- Размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами данной конференции либо их размещение было согласовано с владельцами или администраторами данной конференции предварительно.
- Размещение в любой конференции статьи, содержащей приложенные файлы, кроме случаев, когда вложения явно разрешены правилами данной конференции либо такое размещение было



согласовано с владельцами или администраторами конференции предварительно.

- Рассылка информации получателям, ранее в явном виде выразившим нежелание получать эту информацию, информацию данной категории или информацию от данного отправителя.
- Использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из вышеописанных действий, вне зависимости от того, из какой точки Сети были совершены эти действия.
- Осуществление деятельности по техническому обеспечению рассылки спама (spam support service), как то:
  - целенаправленное сканирование содержимого информационных ресурсов с целью сбора адресов электронной почты и других служб доставки сообщений;
  - распространение программного обеспечения для рассылки спама;
  - создание, верификация, поддержание или распространение баз данных адресов электронной почты или других служб доставки сообщений (за исключением случая, когда владельцы всех адресов, включённых в такую базу данных, в явном виде выразили своё согласие на включение адресов в данную конкретную базу данных; открытая публикация адреса таковым согласием считаться не может).

## **2. Запрет несанкционированного доступа и сетевых атак**

Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса. В том числе запрещены:

- Действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.
- Действия, направленные на получение несанкционированного доступа к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами данного информационного ресурса. Под несанкционированным доступом понимается любой доступ способом, отличным от предполагавшегося владельцем ресурса.
- Передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объёмах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных элементов Сети.
- Целенаправленные действия по сканированию узлов сетей с целью выявления внутренней структуры сетей, списков открытых портов и т.п. иначе как в пределах, минимально необходимых для проведения штатных технических мероприятий, не ставящих своей целью нарушение пунктов 1 и 2 настоящих Норм.

## **3. Соблюдение правил, установленных владельцами ресурсов**

Владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Правила должны быть легко доступными, написанными с учётом разного уровня подготовки пользователей.

Правила использования ресурса, установленные владельцем, не должны нарушать права владельцев других ресурсов или приводить к злоупотреблениям в отношении других ресурсов.

Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

В случае, если правила, установленные владельцем ресурса, противоречат тем или иным пунктам настоящих Норм, в отношении данного ресурса применяются правила, установленные



владельцем, если это не ведет к нарушениям в отношении других ресурсов. В случае, если владельцем группы ресурсов явно установлены правила только для части ресурсов, для остальных применяются правила, сформулированные в данных Нормах.

#### **4. Недопустимость фальсификации**

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его и используемые им средства доступа к Сети. При этом пользователь не должен:

- Использовать идентификационные данные (имена, адреса, телефоны и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование;
- Фальсифицировать свой IP-адрес, а также адреса, используемые в других сетевых протоколах, при передаче данных в Сеть;
- Использовать несуществующие обратные адреса при отправке электронных писем и других сообщений;
- Небрежно относиться к конфиденциальности собственных идентификационных реквизитов (в частности, паролей и прочих кодов авторизованного доступа), что может привести к использованию тех или иных ресурсов третьими лицами от имени данного пользователя (с сокрытием, таким образом, истинного источника действий).

#### **5. Настройка собственных ресурсов**

При работе в сети Интернет пользователь становится её полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а при обнаружении случаев такого использования принимать оперативные меры по их прекращению.

Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытые ретрансляторы электронной почты (open SMTP-relays);
- общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
- средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);
- общедоступные широковещательные адреса локальных сетей;
- электронные списки рассылки с недостаточной надёжностью механизма подтверждения подписки или без возможности её отмены;
- веб-сайты и другие подобные ресурсы, осуществляющие отправку корреспонденции третьим лицам по анонимному или недостаточно аутентифицированному запросу.