

Данные правила являются общепринятыми нормами использования сети Интернет, их выполнение будет способствовать комфортной и безопасной работе пользователей.

1 . Ограничения на информационный шум.

Развитие Интернет привело к тому , что одной из основных проблем пользователей стал избыток информации. Поэтому сетевое сообщество выработало определённые правила , направленные на ограждение пользователя от ненужной информации. В частности , являются недопустимыми :

1.1 . Массовая рассылка сообщений посредством электронной почты и других средств персонального обмена информацией (включая службы немедленной доставки сообщений , такие как SMS , IRC и т.п.) , не иначе как по явно и недвусмысленно выраженной инициативе получателей .

1.2 . Отправка электронных писем и других сообщений , содержащих вложенные файлы и / или имеющих значительный объем , без предварительно полученного разрешения адресата .

1.3 . Рассылка не иначе как по прямой инициативе получателя :

электронных писем и других сообщений рекламного , коммерческого или агитационного характера ;

писем и сообщений , содержащих грубые и оскорбительные выражения и предложения ;

сообщений , содержащих просьбу переслать данное сообщение другим доступным пользователям .

1.4 . Рассылка информации получателям , ранее в явном виде выразившим нежелание получать информацию данной категории или от данного отправителя.

1.5 . 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 , с какой точки сети были совершены эти действия .

1.6 . Осуществление деятельности по техническому обеспечению рассылки спама , такой как: 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 или других служб доставки сообщений (за исключением случая , когда владельцы всех адресов , включенных в такую базу данных , в явном виде выразили свое 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 следующие действия :

2.1 . Направленные на нарушение нормального функционирования элементов сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.

2.2 . 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 владельцем этого программного обеспечения или данных либо администраторами данного информационного ресурса. Под

несанкционированным доступом понимается любой доступ способом, отличным от предусмотренного владельцем.

2.3 . Передача компьютерам или оборудованию сети ненужной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

2.4 . 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 2.1 и 2.2 настоящих правил.

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 учетом 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 настоящего документа, 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 данном документе.

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 используется им как средство доступа к сети. При этом пользователь не должен:

4.1 . Использовать идентификационные данные (имена , адреса , телефоны и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование.

4.2 . Фальсифицировать свой IP - адрес, а также адреса, используемые в других сетевых протоколах, при передаче данных в сеть.

4.3 . Использовать несуществующие обратные адреса при отправке электронных писем и других сообщений.

4.4 . 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 .

5 . Настройка собственных ресурсов.

При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять определенные меры по настройке своих ресурсов препятствующих 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;
Общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
Средства, позволяющие третьим лицам авторизованы скрыть источник соединения (открытые прокси - серверы и т.п.);
Электронные списки рассылки с недостаточной надежностью механизма подтверждения подписки или без возможности ее отмены;
Сайты и другие подобные ресурсы, осуществляющие отправку корреспонденции третьим лицам по анонимному или недостаточно аутентифицированному запросу .