**Нормы пользования сетью Интернет.**

Сеть Интернет 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 Интернет не установлено. Существуют, однако, общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей.

Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов и только они.

Настоящий документ описывает общепринятые нормы работы в сети Интернет, соблюдение которых является обязательным для всех пользователей. Действие этих норм распространяется на порядок использования ресурсов Сети. Здесь и далее словом Сеть обозначены сеть Интернет и доступные из нее иные сети.

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 и (или) незапрошенной информации (спама). В частности, являются недопустимыми:

1.1. Не согласованная предварительно с получателем массовая рассылка электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю.

Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств обмена информацией.

1.2. Не согласованная предварительно с получателем рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения.

1.3. Размещение в любой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списка рассылки (т.н. off-topic). Здесь и далее под конференцией понимаются телеконференции (группы новостей) и другие электронные конференции, форумы и списки рассылки.

1.4. Размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами такой конференции либо их размещение было предварительно согласовано с владельцами или администраторами такой конференции.

1.5. Размещение в любой конференции статьи или статей, содержащих приложенные файлы, кроме случаев, когда подобные вложения явно разрешены правилами такой конференции либо такое размещение было предварительно согласовано с владельцами или администраторами такой конференции.

1.6. Рассылка информации получателям, высказавшим ранее явное нежелание получать эту информацию.

1.7. 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.

1. **Запрет несанкционированного доступа и сетевых атак.**

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

2.1. Действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.

2.2. Действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, локальной вычислительной сети, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение, модификация и (или) блокирование программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами данного информационного ресурса.

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

2.4. Умышленное создание, использование и распространение вредоносных программ для ЭВМ.

1. **Соблюдение правил, установленных владельцами ресурсов.**

Помимо вышеперечисленного, 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 для исполнения всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

1. **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 пользователю запрещается:

4.1. Использование чужих идентификационных данных (имен, адресов, телефонов и т.п.), кроме случаев, когда какие-либо лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети посторонними лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа).

4.2. Фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах при передаче данных в Сеть.

4.3. Использование чужих и (или) несуществующих обратных адресов при отправке электронных писем.

1. **Настройка собственных ресурсов.**

При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность посторонним лицам для использования сетевых ресурсов, принадлежащих пользователю. В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов посторонними лицами, а также оперативно реагировать при обнаружении случаев такого использования.

Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытый ретранслятор электронной почты (SMTP-relay);

- общедоступные серверы новостей (конференций, групп);

- средства, позволяющие посторонним лицам скрывать источник соединения (использование открытых прокси-серверов и т.п.);

- общедоступные адреса локальных вычислительных сетей;

- электронные списки рассылки с недостаточной авторизацией подписки или без возможности ее отмены.

1. **Обязательства по аутентификации и идентификации пользователей**

**беспроводных сетей.**

При самостоятельной организации пользователем сети беспроводного доступа (WiFi) с использованием Сети Интернет провайдера, пользователь в обязательном порядке обязан обеспечить аутентификацию и идентификацию пользователей, подключаемых к сети. Под идентификацией доступа пользователей в сети Wi-Fi понимается процедура идентификации пользователя беспроводной сети посредством отправки-получения SMS-сообщения, предоставлением персональных данных пользователя, посредством голосового сообщения. Также клиент несет полную ответственность по предоставлению полного объема запрашиваемых данных по запросу от контролирующих органов.