Регламент предоставления телематических услуг компании ООО «Инфотех» (ТМ Лайнер).

(редакция от 22 января 2016 года.)

1. ОБЩИЕ ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЕТИ

1.1. В случае переустановки системы (Windows) настройки Интернет изменяются. В случае, если Заказчик самостоятельно не может восстановить настройки - повторная настройка параметров Интернет производится специалистами Исполнителя. Бесплатно оказывается поддержка по телефону. Вызов мастера - платный.

1.2. В случае установки другой сетевой карты (вне зависимости от причин такой перестановки) происходит автоматическое выключение с целью предотвращения несанкционированного доступа к сети или использования реквизитов Заказчика. Заказчик обязан заблаговременно уведомлять Исполнителя о возможных изменениях в сетевой конфигурации его компьютера, планируемого подключения дополнительных сетевых устройств.

1.3. Самостоятельное изменение IP-адреса Заказчиком недопустимо ввиду предотвращения несанкционированного доступа к сети или использования реквизитов других пользователей.

1.4. Недопустимо использование программного обеспечения, производящего сканирование сети, рассылку широковещательных (broadcast) сообщений, рассылку вирусов, а также программного обеспечения, нарушающего работу сети и/или нарушающего работу пользователей.

1.5. Заказчики, замеченные в подмене реквизитов, сканировании сети, нелегальных, с точки зрения сети, действиях - считаются отключенными с момента начала таких действий. Оплата за тарифный план при этом не возвращается. При нанесении материального убытка другим пользователям такими действиями, Исполнитель оставляет за собой право передать дело в суд в порядке, предусмотренном действующим законодательством Российской Федерации.

1.6. Исполнитель не несет ответственность за работу или услуги, оказанные третьими лицами посредством использования сети (в частности работа серверов ICQ, бесплатных почтовых серверов mail.ru, yandex.ru и др., компьютерные игры CS, Quake, AW и т.д.) размещенными за пределами физической сети Исполнителя.

1.7. Исполнитель не несет ответственности за содержание, точность и достоверность информации, передаваемой Заказчиком или третьими лицами по сети Интернет.

1.8. Заказчик самостоятельно отвечает за состояние своего компьютера, а также устанавливает антивирусные пакеты. В случае обнаружения вируса у Заказчика, Исполнитель производит немедленное программное выключение Заказчика с целью пресечения дальнейшего распространения вирусов.

1.9. Ответственность за использование нелицензионных программ остается за Заказчиком.

1.10. В случае, если система подает Заказчику сообщение о подмене реквизита или о совпадении реквизитов, необходимо немедленно уведомить об этом Исполнителя посредством телефонного звонка в службу технической поддержки.

1.11. Заказчик является конечным пользователем и не имеет права на предоставление услуг, предоставляемых Исполнителем, третьим лицам, если это не оформлено другими соглашениями с Исполнителем.

2. **ОГРАНИЧЕНИЯ НА ИНФОРМАЦИОННЫЙ ШУМ (СПАМ)**

2.1. 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). В частности, являются недопустимыми со стороны Заказчика следующие действия:

2.1.1. Массовая рассылка не согласованных предварительно электронных писем (mass mailing). 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 личного обмена информацией.)*

2.1.2. Несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения.

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

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

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

2.1.6. 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.

3. **ЗАПРЕТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И СЕТЕВЫХ АТАК**

3.1. Не допускается осуществление со стороны Заказчика попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса. В том числе запрещены:

3.1.1. действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих Заказчику;

3.1.2. действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих Заказчику, без согласования с владельцами этого программного обеспечения либо администраторами данного информационного ресурса;

3.1.3. 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 связности сетей и доступности отдельных ее элементов.

4. **СОБЛЮДЕНИЕ ПРАВИЛ, УСТАНОВЛЕННЫХ ВЛАДЕЛЬЦАМИ РЕСУРСОВ**

4.1. Помимо вышеперечисленного, владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования.

4.2. 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.

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

5. **НЕДОПУСТИМОСТЬ ФАЛЬСИФИКАЦИИ**

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

5.1.1. использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили Заказчика на такое использование. В то же время Заказчик должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);

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

5.1.3. Использование несуществующих обратных адресов при отправке электронных писем.

6. **НАСТРОЙКА СОБСТВЕННЫХ ВНУТРИСЕТЕВЫХ РЕСУРСОВ**

6.1. При работе в сети Интернет Заказчик становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих Заказчику, третьими лицами. В связи с этим Заказчик должен принять надлежащие меры по такой настройке своих ресурсов, которые препятствовали бы недобросовестному использованию этих ресурсов третьими лицами, а также оперативно реагировать при обнаружении случаев такого использования.

Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытый ретранслятор электронной почты (SMTP-relay);

- 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 авторизацией подписки или без возможности ее отмены.

7. **ИСПОЛЬЗОВАНИЕ ВНЕШНИХ IP АДРЕСОВ**

7.1. В случае, когда Заказчик заказывает услугу «Внешний IP адрес» *(выделенный IP адрес, фиксированный IP адрес)* он автоматически соглашается со следующими правилами (если не было дополнительного письменного соглашения с Исполнителем):

7.1.1. При использовании «Внешнего IP адреса» запрещается размещать на компьютере Заказчика публичные сервисы (dns/web/mail/ssh/proxy/ftp/p2p-сервера/irc-сервера/чаты/игровые-сервера) а также сервисы видео-аудио трансляции доступные извне сети Исполнителя.

7.1.2. Весь внешний трафик (заказанный и не заказанный абонентом) подлежит тарификации (в случае тарификации по трафику)

7.1.3. Доступ извне сети Исполнителя на компьютер Заказчика посредством программ ssh/vnc/radmin/vpn желателен, только с использованием для этой цели нестандартных портов(1022/5901/3355 и подобных), для предотвращения атак/сканирования компьютера Заказчика.

7.1.4. В случае обнаружения DDoS атак как со стороны Заказчика, так и извне сети на «Внешний IP адрес» Исполнитель вправе приостановить действие услуги, или заблокировать доступ по портам/сервисам которые участвуют в атаке.

7.2. Абонентская плата услуги «Внешний IP адрес» списывается за календарный месяц вне зависимости от даты подключения данной услуги, согласно тарифам Исполнителя.

7.3. Настройки услуги «Внешний IP адрес» заказываются посредством Электронного кабинета, раздела «техподдержка, IP адреса внешние и внутренние».

7.4. Заказчик самостоятельно устанавливает настройки услуги на свой компьютер, либо может заказать платный вызов мастера.