

## ПРАВИЛА ПОЛЬЗОВАНИЯ СЕТЬЮ (ППС)

ППС RETN являются обязательными для всех пользователей услугами RETN. Все клиенты должны соблюдать условия ППС и отвечают за то, чтобы их собственные клиенты не заставляли их нарушать условия данных Правил.

Неприемлемое использование сети можно разделить на 3 основных категории:

- незаконное использование;
- злоумышленное использование;
- использование, угрожающее целостности сети.

RETN оставляет за собой право в любое время вносить изменения в данные ППС. Изменения вступают в силу с момента их публикации на сайте RETN по следующему адресу <https://retn.net/>.

Последствия нарушения ППС подробно разъяснены в рамках Генерального соглашения на оказание услуг.

Запрещенное использование:

Незаконное использование

- Любая деятельность, которая считается незаконной на территории, на которой клиенту предоставляются услуги;
- Хранение или передача материала, который нарушает авторское право или право на торговый знак;
- Хранение или передача детской порнографии;
- Использование услуг в мошеннических целях, для хищения персональных данных или иной вредоносной или мошеннической деятельности, включая предложение или распространение мошеннических товаров, услуг, схем, продвижений;
- Использование услуг для распространения, контроля или иного взаимодействия с вредоносными компьютерными программами (вирусами, троянскими программами, «червями», шпионскими программами и иными хакерскими программами);
- Пиратство программного обеспечения или иное медийное пиратство;
- Нарушение местного импортно-экспортного законодательства.

Злоумышленное использование

- Притеснение человека или организации, будь то посредством прямой угрозы, словесного запугивания или простого отказа прекратить указанные действия;
- Тестирование на проникновение / уязвимость или несанкционированный доступ к сети RETN и какой-либо операционной или административной системе RETN;
- Тестирование на несанкционированное проникновение / уязвимость или доступ к сети или системам любой иной компании;
- Электронная выдача себя за другого человека или организацию, или другие приемы обмана;
- Рассылка спама; нежелательная электронная рассылка; нежелательная реклама; сообщения, предназначенные для дестабилизации других услуг; сообщения содержащие вредоносный контент;
- Фарминг адресов электронной почты или иных индивидуальных онлайн-идентификаторов;
- Фишинг;
- Несанкционированный перехват сообщений или иных данных;
- Операционные сетевые услуги, как, например, открытые прокси-серверы, открытые почтовые трансляторы или открытые рекурсивные серверы доменных имён.

Использование, угрожающее целостности сети

Общее вмешательство в сеть RETN или её системы мониторинга.

- Действия, которые нарушают ППС поставщиков RETN;
- Действия, которые превращают сеть RETN в цель DDoS-атак или прочих нацеленных атак;
- Всё, что ведёт к тому, что IP пространство RETN заносится в черный список базами данных по злоумышленному использованию (Spamhaus и т.д.);
- Действия, которые приводят к прерыванию функционирования сети RETN по постановлению правительства;
- Любые действия, которые приводят к прерыванию предоставления услуг другим клиентам RETN.