**ПРАВИЛА ПОЛЬЗОВАНИЯ ВЫЧЕСЛИТЕЛЬНОЙ СЕТЬЮ ТПУ**

1. Общие положения.
   1. Данные правила определяют права и обязанности пользователей корпоративных сетевых ресурсов вычислительной сети (ВС) ТПУ в целом и правила получения доступа к ресурсам сети Internet. Выполнение этих правил позволит пользователям избежать различных проблем и осложнений, а также повысить эффективность своей работы.
   2. Данные правила являются общими для ВС ТПУ и вместе с правилами принятыми в подразделениях определяют поведение пользователей в пределах всей ВС ТПУ.
   3. Пользователь работает в сети в соответствии с настоящими правилами.
   4. Все вопросы и проблемы конечного пользователя должны решаться в первую очередь в пределах ЛВС подразделения с её сетевым администратором и только затем с администрацией управления информатизации (УИ) ТПУ. При обращении в УИ следует предоставить администратору вывод следующих команд ОС Microsoft Windows: ipconfig, ping , tracert, route print (Инструкция по запуску команд в приложении 1).
   5. Пользователи сети несут полную персональную административную и финансовую ответственность за свои действия в ВС ТПУ, российских и международных сетях.

## Ограничения на информационный шум (спам).

Развитие cети привело к тому, что одной из основных проблем пользователей стал избыток информации. Поэтому сетевое сообщество выработало специальные правила, направленные на ограждение пользователя от ненужной/не запрошенной информации (спама). В частности, являются недопустимыми:

* 1. Массовая рассылка сообщений посредством электронной почты и других средств персонального обмена информацией, иначе как по явно и недвусмысленно выраженной инициативе получателей.
  2. Обязательно наличие возможности для любого подписчика немедленно покинуть список рассылки без каких-либо затруднений при возникновении у него такого желания. При этом наличие возможности покинуть список само по себе не может служить оправданием внесения адресов в список не по воле владельцев адресов.
  3. Рассылка (иначе как по прямой инициативе получателя)
* электронных писем и других сообщений (в том числе единичных) рекламного, коммерческого или агитационного характера;
* писем и сообщений, содержащих грубые и оскорбительные выражения и предложения.
* Рассылка сообщений, содержащих просьбу переслать данное сообщение другим доступным пользователям (chain letters).
  1. 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.
  2. Рассылка информации получателям, ранее в явном виде выразившим нежелание получать эту информацию, информацию данной категории или информацию от данного отправителя.
  3. 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 ВС были совершены эти действия.
  4. 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, 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).

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

Не допускается осуществление попыток несанкционированного доступа к ресурсам ВС, 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:

* 1. Действия, направленные на нарушение нормального функционирования элементов ВС (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.
  2. Действия, направленные на получение несанкционированного доступа к ресурсу ВС (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.
  3. Передача компьютерам или оборудованию ВС 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. 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 3.1 и 3.2 настоящего документа.

1. ***Соблюдение правил, установленных владельцами ресурсов***
   1. Владелец любого информационного или технического ресурса ВС 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.
   2. Правила использования ресурса, установленные владельцем, не должны нарушать права владельцев других ресурсов или приводить к злоупотреблениям в отношении других ресурсов.
   3. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.
2. 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.
3. ***Недопустимость фальсификации***

Значительная часть ресурсов ВС 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 ВС. При этом пользователю запрещается:

* 1. Использовать идентификационные данные (имена, адреса, телефоны и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование.
  2. Фальсифицировать свой IP-адрес, а также адреса, используемые в других сетевых протоколах, при передаче данных в ВС.
  3. Использовать несуществующие обратные адреса при отправке электронных писем и других сообщений.
  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 пользователя (с сокрытием, таким образом, истинного источника действий).
  5. Установка, настройка собственного сетевого оборудования.
  6. Разрешается настройка собственного активного оборудования с условием соблюдения ниже следующих требований:
  7. Устанавливаемое оборудование **не должно** оказывать влияния на работу ВС ТПУ.
  8. В случае установки Wi-Fi точек доступа следует ограничить радиус их действия таким образом, что бы они не были доступны за пределами того помещения в котором установлены.
  9. Использование проводных и Wi-Fi маршрутизаторов допускается только в режимах мост (bridge) или точка доступа access point.

**7.Ответственность.**

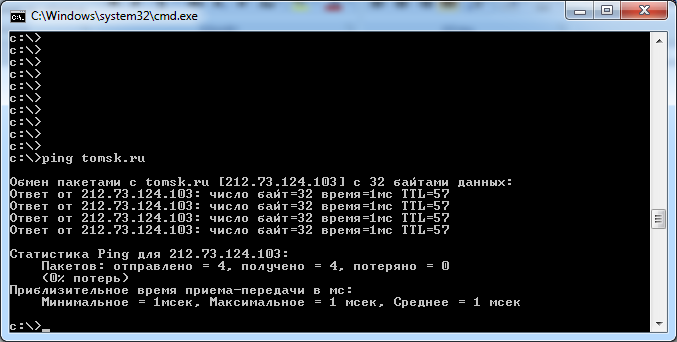
* 1. Пользователь несет полную ответственность за все действия, совершенные от его имени, с использованием его учетной записи.
  2. Действия любого пользователя, подозреваемого в нарушении правил пользования ВС, могут быть запротоколированы, и использоваться для принятия решения о применении к нему санкций административного характера.
  3. При несоблюдении пользователями условий настоящих правил к ним применяются административные меры наказания, вплоть до отчисления из ТПУ, в соответствии со степенью вины, установленной служебным расследованием.

Приложение 1.

* Использование команды ping.

Меню «Пуск» -> Выполнить ->cmd

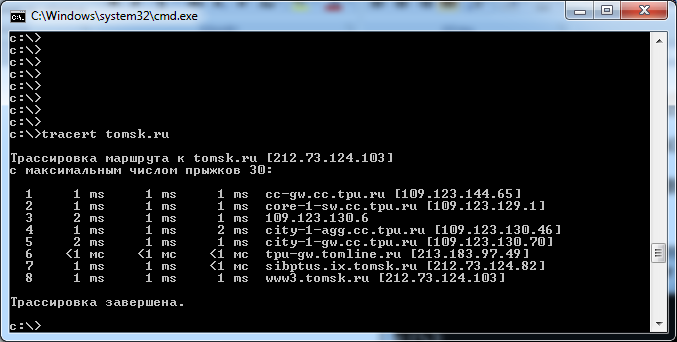
В появившимся окне вводим команду ping tomsk.ru



* Использование команды tracert.

Меню «Пуск» -> Выполнить ->cmd

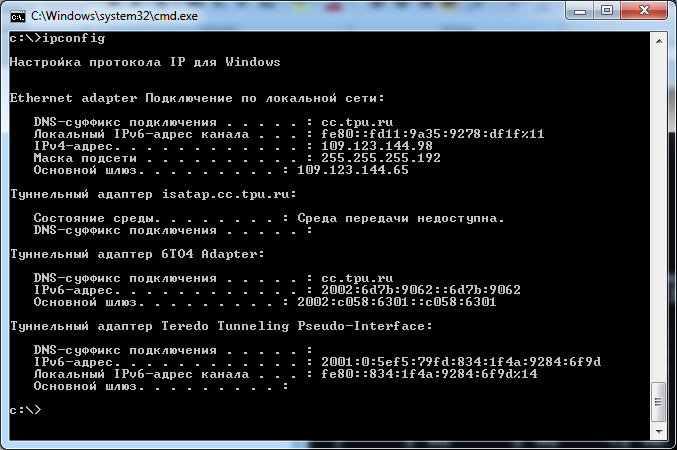
В появившимся окне вводим команду tracert tomsk.ru



* Использование команды ipconfig.

Меню «Пуск» -> Выполнить ->cmd

В появившимся окне вводим команду ipconfig



* Использование команды route print.

Меню «Пуск» -> Выполнить ->cmd

В появившимся окне вводим команду route print

