Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

ПРИНЯТО	УТВЕРЖДЕНО
решением Ученого совета ФГБОУ ВО «ТГТУ» «29» 08 2016 г. (протокол № *10*)	приказом ректора ФГБОУ ВО «ТГТУ» «08» 09 2016 г. № *481-04*

Р Е Г Л А М Е Н Т

компьютерной сети Тамбовского государственного технического университета

(с изменениями согласно п.3 приказа ректора от 28.01.2019 г. № 11-04)

город Тамбов
2016 год

1. Общие положения

1.1. Настоящий Регламент конкретизирует документ «Положение о компьютерной сети федерального государственного бюджетного образовательного учреждения высшего образования «Тамбовский государственный технический университет» (далее по тексту – «Положение») в части правил работы в Сети, обязанностей администрации и подразделений и является внутренним нормативным документом ТГТУ.

В настоящем: документе без специального объяснения используются термины и сокращения, определенные в «Положении».

1.2. Абонент является конечным пользователем и не имеет права на предоставление услуг третьим лицам, если это не оформлено другими соглашениями с ТамбовЦНИТ.

1.3. Получение услуг Сети в полном объеме гарантируется Абоненту через 2 рабочих дня с момента согласования с Администрацией Сети сетевых реквизитов абонента.

1.4. Администрация Сети обеспечивает возможность круглосуточного получения услуг абонентом, если иное не оговорено другими нормативными актами и распоряжениями ТГТУ.

Услуги Абонентской группы Администрации Сети предоставляются только в рабочее время.

1.5. Администрация Сети не несет ответственности за качество работы линий связи, предоставляемых другими организациями.

1.6. Официальные сообщения Администрации Сети, связанные с обслуживанием Абонентов, отправляются абонентам по электронной почте. Электронные почтовые сообщения для Администрации Сети оформляются в соответствии с RFC 822 (русская кодировка KOI8-R).

1.7. Администрация Сети имеет право временно прекратить предоставление услуг Абоненту в следующих случаях:

– распространение информации, оскорбляющей честь и достоинство других абонентов и персонала компьютерных сетей;

– распространение в Сети материалов рекламного или коммерческого содержания, а равно и иная, не предусмотренная уставом ТГТУ деятельность в Сети;

– распространение в Сети информации, запрещенной законодательством Российской Федерации;

– рассылка почтовой корреспонденции, содержащей вложенные файлы, без согласования с получателем;

– нарушение авторских прав на информацию, представленную в сети;

– намеренное либо ненамеренное нанесение ущерба другим лицам;

– вмешательство в действия других абонентов или обслуживающего персонала (например, несанкционированный доступ к компьютерам и информационным источникам);

– неправомерное использование коммерческой информации;

– распространение, в том числе неумышленное, вредоносных программ.

1.8. Возобновление предоставления услуг (повторное включение) после прекращения предоставления услуг возможно только после устранения причины отключения в соответствии с п. 1.7.

1.9. Рекламации по услугам принимаются в течение 30 дней от даты возникновения спорной ситуации.

1.10. Администрация Сети не несет ответственность за компрометацию паролей по вине Абонента. Абонент обязан немедленно оповестить Администрацию Сети о компрометации паролей.

1.11. Изменение пароля по требованию Абонента производится только в случае его, либо его ответственного представителя, явки в Администрацию Сети и предъявления документов, удостоверяющих личность.

1.12. Абонент обязан в пятидневный срок заполнить и вернуть Администрации Сети представленные ему Администрацией Сети формы статистической отчетности (подаваемой ТГТУ в государственные органы Российской Федерации) и другие официальные документы, касающиеся состояния его сети.

1.13. Установка и настройка Администрацией Сети операционной системы или других программных продуктов на машине(ах) Абонента, изготовление линий связи, создание ЛВС, тестирование аппаратных средств, предназначенных для получения услуг Сети, настоящим Регламентом не предусматривается.

1.14. Для выполнения договорных обязательств Администрация Сети и Абонент каждый со своей стороны назначают ответственных представителей. Все взаимоотношения сторон, осуществляются через ответственных представителей кроме действий, отмеченных особо. Ответственный представитель Абонента, как правило, выполняет обязанности ответственного за информатизацию подразделениях ТГТУ. В случае назначения нового ответственного представителя абонент письменно информирует об этом Администрацию Сети.

1.15. С целью удобства обслуживания абонентов Администрацией Сети для своих ответственных представителей определены следующие зоны ответственности

(совпадающие с сетевыми зонами), охватывающие корпус или блок корпусов ТГТУ:

– корпус по ул. Советская, д. 106;

– блок корпусов по ул. Советская, д. 116/ ул. Коммунальная, д. 5;

– блок корпусов по ул. Мичуринская, д.112, включая корпуса общежитий и поликлиники ТГТУ;

– корпус по ул. Ленинградская, д.1.

1.16. Зона ответственности ответственного представителя со стороны Абонента – локальная вычислительная сеть (ЛВС) Абонента до точки подключения к техническим средствам Сети.

1.17. В особых случаях подключения абонентов Администрация Сети может потребовать выполнения технических условий на подключение, которые письменно выдаются Абоненту по его запросу.

1.18. Администрация Сети публикует на сайте ТГТУ тексты документов, необходимых для регламентации деятельности Сети.

2. Сетевые протоколы и ограничения в Сети

2.1. В Сети ТГТУ используются протоколы семейства TCP/IP.

2.2. В случае использования во внутренних сетях Абонента иных протоколов для доступа в Сеть абонент должен самостоятельно обеспечить их преобразование (шлюз).

2.3. Для обеспечения безопасности и надежности работы Сети, а равно и в целях повышения эффективности ее работы и использования ресурсов Администрация Сети может ограничивать использование отдельных сетевых сервисов, например, путем перекрытия IP- портов.

Внутри ЛВС Абонентов использование любых сервисов находится целиком в компетенции подразделения.

2.4. В соответствии с п. 7.1. «Положения» и в связи с ограниченной скоростью внешних каналов связи для Абонентов может лимитироваться месячный объем внешнего входящего трафика. Внешним считается трафик, приходящий из других сетей, кроме местных, с которыми имеются соглашения об обмене трафиком.

Месячные лимиты внешнего входящего трафика в календарный месяц на 1 компьютер, подключенный к Сети, устанавливаются распоряжением начальника управления информатизации. По достижении лимита подразделение отключается от внешних каналов до конца месяца.

2.5. В случае острой необходимости для отдельного подразделения лимиты могут

быть увеличены начальником управления информатизации. Основанием для рассмотрения увеличения лимитов является служебная записка руководителя подразделения с обоснованием необходимости увеличения.

3. Услуги Сети, предоставляемые Абонентам

3.1. Соединение с Сетью обеспечивает возможность получения Абонентом услуг передачи данных и телематических служб как в пределах Сети ТГТУ, так и в сети Интернет.

3.2. Администрация Сети обеспечивает АБОНЕНТАМ:

– выделение адресного пространства Сети;

– регистрацию в доменной системе имен, как правило, в сетевой зоне, в которой физически расположена локальная сеть абонента (имя*.зона.tstu.ru, имя*.зона.тгту.рф, имя*.зона.тамбовгту.рф), либо в центральной зоне доменной системы имен ТГТУ (имя *.tstu.ru, имя*.тгту.рф, имя*.тамбовгту.рф);

– электронный почтовый ящик и адрес электронной почты в определенном домене. Для получения почтового ящика абонент должен предоставить заявку с указанием необходимой регистрационной информации.

3.3. По письменному разрешению возможно размещение информации абонента на центральном WWW-портале ТГТУ или других серверах Сети.

3.4. Консультации по использованию услуг сети оказываются абоненту ответственным представителем Администрации Сети и персоналом соответствующих служб Сети (сетевых зон) без выхода к Абоненту.

3.5. Обслуживающий персонал Сети несет ответственность за поддержание работоспособности и исправности ОСПД в своей зоне ответственности. Обслуживающий персонал Сети производит работы по текущему ремонту, восстановлению программного обеспечения и т.п.

3.6. Абонент имеет возможность получить необходимые сведения о текущей работоспособности Сети.

3.7. Абонент имеет возможность получить необходимые сетевые реквизиты для доступа к информации о величине своего трафика, для чего по его письменному запросу Администрация Сети сообщает ему необходимые сетевые реквизиты.

3.8. По причинам, упомянутым в п. 2.3, а также в п. 6.1., 6.2. «Положения», могут вводиться иные ограничения на использование ресурсов Сети Абонентами. Текущий список ограничений утверждается начальником управления информатизации.

4. Сетевые сервисы

4.1. Сервис – это совокупность аппаратных и программных средств, в соответствии со стандартами, обеспечивающих функциональность, направленную на предоставление информационных услуг и ресурсов, или обеспечение работоспособности других сервисов.

4.2. Политика в области определения списка сервисов, поддерживаемого в Сети, выбора технических и программных средств их реализации и прочие вопросы, связанные с созданием, существованием, развитием и закрытием сервисов целиком определяется Администрацией Сети.

4.3. Новый сервис Сети может быть создан по инициативе Администрации Сети, пользователей или групп пользователей сети и должен быть согласован с Администрацией Сети.

4.4. Пользователям запрещается создавать на включенных в Сеть компьютерах сервис, доступный для внешних пользователей, без согласования с Администрацией Сети.

4.5. Каждый создаваемый сервис должен иметь администратора, ответственного за его поддержку и эксплуатацию. Администратор сервиса обязан выполнять все распоряжения и рекомендации администратора сети подразделения и Администрации Сети.

4.6. Администратор общедоступного сервиса определяет порядок его использования, разрабатывает и своевременно обновляет инструкции и другую необходимую документацию для пользователей данного сервиса.

4.7. Администрация Сети при обнаружении общедоступного сервиса, не имеющего данных об администраторе и не зарегистрированном Администрацией Сети, принимает меры по ликвидации такого сервиса.

4.8. Администрация Сети создает и поддерживает ряд базовых системных и общедоступных сервисов:

– транспортный сервис (коннективность, поддержка адресного пространства, маршрутизация);

– служба доменной системы имен (DNS);

– почтовый сервис;

– WWW-портал ТГТУ.

5. Поддержка и документирование Сети

5.1. Сеть работает круглосуточно 7 дней в неделю. Абонентам при их регистрации сообщаются месторасположение обслуживающего персонала сети, способы связи и режим работы персонала.

5.2. Поддержание работоспособности сети корпуса в целом возлагается на администратора сети корпуса (сетевой зоны). Для выполнения этой задачи и обеспечения работоспособности отдельных сегментов сети администратор сети корпуса привлекает необходимый персонал из сотрудников обслуживающего персонала сети корпуса.

5.3. Любые действия, связанные с поддержанием работоспособности Сети, ее модернизацией или иное изменение, создание новых и удаление старых сервисов вправе производить только обслуживающий персонал Сети.

5.4. Возникающие в процессе работы Сети неполадки, связанные как с аппаратной частью Сети, так и с её программным обеспечением, должны быть устранены обслуживающим персоналом Сети в максимально короткие сроки.

5.5. При необходимости проведения работ, связанных с модернизацией аппаратной части Сети или используемого программного обеспечения, администратор соответствующего участка Сети не позднее, чем за сутки обязан предупредить об этом Абонентов, нормальная работа которых может быть нарушена проведением таких работ.

5.6. Для обеспечения возможности восстановления Сети в кратчайшие сроки при поломке аппаратуры создается университетский резервный фонд оборудования, который используется при необходимости.

5.7. Подключение новых сетей и отдельных компьютеров внутри сетевой зоны осуществляется только обслуживающим персоналом сетевой зоны, который выдает рекомендации по настройке аппаратной части и, при необходимости, сетевого программного обеспечения. При этом по письменному запросу абонента ему сообщаются необходимые для работы в сети реквизиты.

5.8. Поддержка и сопровождение установленного сетевого программного обеспечения на маршрутизаторах или ином оборудовании сопряжения Сети с ЛВС Абонента осуществляется обслуживающим персоналом сети Абонента. При необходимости использования нового сетевого программного обеспечения (далее ПО) Абонент обязан согласовать его использование с администрацией сети корпуса (сетевой

зоны). Все остальное ПО, установленное в сети Абонента, поддерживается и эксплуатируется им самостоятельно.

5.9. При обнаружении распространения с компьютера или ЛВС Абонента компьютерных вирусов, источник вирусов должен быть немедленно отключен от Сети. Администратор сетевой зоны или Сети в целом вправе отключить любой сегмент Сети до локализации источника вирусов. Администратор ЛВС Абонента обязан предпринять немедленные меры антивирусной защиты. Повторное подключение компьютера или локальной сети может быть осуществлено только после устранения причины отключения.

5.10. Каждый компьютер, Абонента, включенный или вновь подключаемый к сети, снабжается "сетевым паспортом" (паспорт), в котором ответственным представителем Абонента указываются:

а) Тип компьютера и его назначение;

б) Используемая операционная система;

в) Используемая(ые) сетевая плата (платы) и MAC адрес (а); г) IP-номер компьютера и маска сети, IP-номер шлюза, IP-номер сервера DNS;

д) ФИО ответственного представителя Абонента;

е) ФИО ответственного представителя Администрации Сети; ж) Дата заполнения.

Документ заполняется ответственным представителем Абонента, при этом графа г) согласуется с администратором сетевой зоны (см. Приложение 1).

Паспорт составляется в двух экземплярах, один из которых хранится у Абонента, второй - у Администрации Сети. При внесении каких-либо изменений в указанные выше данные составляется новый паспорт. Самостоятельное внесение изменений в паспорт или конфигурацию сетевых средств не допускается, а самовольное изменение Абонентом конфигурации компьютера в части данных в) и г), зарегистрированных в паспорте, может расцениваться Администрацией Сети как несанкционированный доступ к компьютерам и информационным источникам и рассматривается в соответствии с законодательством Российской Федерации.

5.11. Администратор сети корпуса составляет и при необходимости корректирует схему сети корпуса с указанием физической топологии сети, параметров подсетей, специфики поддерживаемых протоколов и сервисов, и иных необходимых сведений.

5.12. В Сети осуществляется мониторинг событий. Конкретный перечень событий, подлежащих протоколированию, определяется Администрацией Сети.

Полученные при этом электронные журналы событий используются Администрацией Сети для анализа её работы, а также могут служить доказательством неправомерных действий пользователей в отношении Сети. Любые попытки сбора информации, передаваемой по Сети, неуполномоченными на то лицами (запуск tcpdump, satan и т.п.) считаются неавторизованным доступом к Сети и влекут соответствующую ответственность.

5.13. Любая информация, содержащая детальные сведения о конфигурации сетей и их функционировании, в частности, упомянутая в п. 5.10, 5.11, 5.12, считается конфиденциальной и должна быть доступна только уполномоченным лицам.

6. Безопасность в Сети

6.1. Организация защиты информации в Сети вуза возлагается на руководителей подразделений, эксплуатирующих средства вычислительной техники и активное (управляемое) телекоммуникационное оборудование (СВТ). Политика защиты информации строится и координируется на основании решений ТС и реализуется администраторами Сети в соответствии с иерархической схемой управления, и лицами, ответственными за СВТ, путем выполнения организационных и технических мероприятий.

6.2. Организационные мероприятия включают в себя:

– организацию постоянного контроля соблюдения всех документов, регламентирующих работу Сети;

– проведение антивирусной политики в Сети;

– ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и телекоммуникационное оборудование Сети;

– контроль структуры Сети и пресечение несанкционированного подключения СВТ к Сети.

6.3. Технические мероприятия включают в себя:

– регулярную смену паролей на доступ к конфигурированию СВТ;

– антивирусный контроль;

– регулярное резервное копирование информации;

– физическое выделение сегментов Сети, в которых передается конфиденциальная информация;

– отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность Сети, компьютеров в

ней и нарушающего безопасность локальных сегментов и Сети в целом;

– логическое выделение СВТ и/или групп пользователей, обладающих строгим разграничением доступа к ресурсам Сети;

– ограничение пропуска сетевых протоколов на маршрутизаторах в соответствии с определенными в утвержденной документации потребностями отдельных сегментов Сети;

– проведение скоординированных действий по возможно максимальному использованию на СВТ программного обеспечения, обеспечивающего авторизацию доступа к управлению СВТ и к сетевым сервисам, а также централизованную аутентификацию пользователей, получивших доступ в Сеть.