УТВЕРЖДАЮ
Ректор БГТУ им. В.Г. Шухова,
д.т.н., профессор
А.М. Гридчин
«____» _____ 2005 г.

Правила пользования корпоративной компьютерной сетью БГТУ им. В.Г. Шухова

I. Общие положения

Корпоративной компьютерной сетью БГТУ им. В.Г. Шухова (в дальнейшем ККС) называется совокупность компьютеров, кабельной системы, сетевых адаптеров, активного сетевого оборудования, работающих под управлением сетевых операционных систем и прикладного программного обеспечения.

Настоящие правила содержат необходимые требования по обеспечению совместной работы в ККС, сохранности информации пользователей сети и соблюдения прав на ее распространение, в том числе и защиты личной информации пользователей.

Настоящие правила предназначены для регулирования распределения ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, установленных ее собственником, в том числе и соблюдения конфиденциальности личной информации. Правила служат интересам всех пользователей, поэтому в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а, в особенности, о фактах несанкционированного доступа к информации, размещенной на его компьютере или каком-либо другом, он должен немедленно сообщить администратору сети или лицу, ответственному в сети за компьютерную безопасность.

II. Права и обязанности администрации ККС

Администрацией сети являются сотрудники БелЦНИТ, наделенные административными правами.

Администрация сети в рамках настоящих правил несет ответственность за:

1. Функционирование ККС в целом;
2. Функционирование базовых сервисов сети;
3. Нарушение функционирования ККС вследствие некорректного управления маршрутизацией;
4. Нарушение функционирования ККС вследствие некорректного управления базовыми сетевыми сервисами (DNS, DHCP, AD).

Администрация ККС не несет ответственности за:

1. Информацию, находящуюся на компьютерах в сети подразделений, входящих в ККС, установленные права доступа к компьютерам в локальных сетях подразделений и за деятельность, ведущуюся на этих компьютерах;
2. Работоспособность компьютеров и оборудования сети подразделений, работоспособность и физическое состояние линий связи и других средств коммуникаций внутри сети подразделений;
3. Содержание проходящих по сети данных.

Администрация обязана:

1. Ограничивать доступ сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование ККС;
2. Обеспечивать контроль структуры сети и пресечение несанкционированного подключения к ККС;

Технические мероприятия включают в себя:

- § регулярную смену сетевых паролей;
- § отслеживание запуска и пресечение использования программного обеспечения затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней и нарушающего безопасность сети;
- § настройка доменных политик безопасности.

3. Принимать организационные и технические меры к пресечению попыток несанкционированного доступа на компьютеры из внешних сетей и с компьютеров ККС, а также к пресечению распространения информации, запрещенной действующим законодательством.

Администрация имеет право:

1. В случае злоупотребления сетью частично или полностью отстранять нарушителей от пользования ККС;
2. Удалять программное обеспечение, нарушающее работу ККС.

III. Права и обязанности пользователей ККС

Пользователями ККС БГТУ им. В.Г. Шухова являются участники Белгородского образовательно-научного пространства, ознакомленные с настоящими правилами и соблюдающие их требования в процессе работы.

Пользователь несет полную ответственность за все действия, связанные с использованием компьютерных сетей, от его имени или с закрепленного за ним рабочего места. За действия связанные с настройкой сетевых параметров несет ответственность администратор рабочего места. Лица, допустившие нарушения требований настоящих правил, несут дисциплинарную ответственность. В особо серьезных случаях, нарушители подвергаются судебному преследованию в установленном законом порядке, (см. Приложение 1).

Пользователи должны уважать права других пользователей на конфиденциальность и право на пользование общими ресурсами.

Пользователь имеет право:

1. На доступ ко всем ресурсам ККС университета в пределах требований настоящих правил;
2. Обращаться за справочной информацией и консультацией к соответствующему техническому персоналу, обслуживающему ККС.

Пользователь обязан:

1. Использовать ресурсы ККС исключительно в некоммерческих, образовательных и научных целях;
2. Выполнять все требования администрации сети, не противоречащие настоящим правилам;
3. Соблюдать правила техники безопасности при работе с техническими средствами;
4. Обеспечивать неразглашение идентификационной информации, используемой для доступа к ресурсам ККС (паролей и прочих кодов авторизованного доступа);
5. Препятствовать несанкционированному и недобросовестному использованию ресурсов ККС;
6. Содействовать сохранности и дальнейшему развитию ресурсов и технических средств ККС;
7. В случае замены сетевой карты пользователь должен известить администратора для изменения информации о новой сетевой карте во избежание блокировки пользователя;
8. Пользоваться антивирусными программами.

IV. Общие рекомендации и правила пользования ККС

Использование учетной записи:

Для надежной и безопасной работы в ККС администрация настоятельно рекомендует пользователям придерживаться следующих правил при работе с учетными записями:

1. Контролировать доступ к своей учетной записи, следить за содержимым своей домашней директории на сервере, за появлением файлов неизвестного происхождения (особенно скрытых).
2. Обеспечивать безопасность учетной записи, устанавливать пароль в соответствии с требованиями к нему:
   - § пароль должен содержать не менее 6 символов;
   - § пароль обязательно должен содержать цифры, строчные и заглавные символы;
   - § пароль не должен содержать имя для входа в систему, имя, фамилию, отчество, сочетание инициалов, дату рождения, телефон, другую личную информацию и английское слово;
   - § пользователь должен известить системного администратора об удалении ненужной учетной записи из системы;
   - § пароль должен меняться хотя бы раз в 3 месяца, для смены пароля пользователю необходимо обратиться к администратору, назвав при этом старый пароль и придумав новый.

Рекомендации к пользованию компьютерной корпоративной сетью:

1. Произвести заземление компьютерной техники;
2. Отключать компьютерную технику и сетевой кабель во время грозы;
3. Помнить свой сетевой адрес, сетевые настройки и пароли доступа в сеть;
4. Знать и соблюдать настоящие правила;
5. Пользоваться антивирусными программами;
6. Помнить, что покидающий сеть/общежитие пользователь должен сообщить об этом администраторам. Адрес, который не был оплачен в течение 1 месяца или не использовался в течение 6 месяцев (по данным сервера статистики), считается свободным и может быть передан другим пользователям;
7. Сообщать свои замечания и предложения о работе сети системному администратору.

Правила работы с персональным компьютером в ККС:

1. Пользователь компьютера, включенного в ККСуниверситета, должен быть ознакомлен с настоящими правилами.
2. Разрешение на подключение компьютера к сети дается администратором сети. Самовольное подключение является серьезнейшим нарушением правил пользования сетью. При подключении к сети пользователю выдается IP-адрес его компьютера. Так как передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу организации защиты информации других компьютеров, то передача таких данных категорически запрещена. В целях контроля за использованием ресурсов сети и обеспечения необходимых мер компьютерной безопасности на передачу данных в ККС с использованием протоколов, отличных от общепринятых, требуется разрешения администратора сети.
3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ККС и за ее пределами. В случае, если с данного компьютера производился несанкционированный доступ к информации на других компьютерах и в случаях других серьезных нарушений правил пользования сетью, по решению администратора сети компьютер отключается от сети, а к пользователю данного компьютера применяются меры, предусмотренные административным или уголовным законодательством.

V. Пользователям ККС категорически запрещается

1. Использовать вычислительную технику для несанкционированного доступа к другим компьютерам сети и нарушения системы безопасности в целом;
2. Подключать компьютеры к сети без специального разрешения системного администратора;
3. Категорически запрещается самовольно изменять IP-адреса компьютеров в сети, принадлежность компьютера к домену, сетевое имя компьютера, настройки шлюзов и основных серверов;
4. Распространять и использовать программное обеспечение и любые материалы, полностью или частично защищенные авторскими правами, без разрешения владельца.
5. Преднамеренно/непреднамеренно распространять компьютерные вирусы и зараженные ими файлы;
6. Перехватывать чужую информацию, передаваемую по сети;
7. Использовать программное обеспечение, ориентированное на нарушение системы безопасности сети ("троянские кони", бэкдоры и другое шпионское программное обеспечение).
8. Обмениваться информацией, запрещенной действующим законодательством РФ: пропаганда насилия, разжигание расовых, национальных и религиозных распрей, порнография, любая информация, несущая оскорбления и клевету, а также распространяемая с целью хищения чужих денежных средств или имущества путем обмана или злоупотребления доверием;
9. Несанкционированный доступ (или его попытки) к закрытым ресурсам в сети. Участвовать в проведении "сетевых атак" и "сетевого взлома";

Эти действия определяются как:

- использование против компьютеров или оборудования компьютерных сетей специальных средств, позволяющих получить нелегальный доступ к содержащейся информации;
- передача компьютерам или оборудованию компьютерных сетей бессмысленной или бесполезной информации, создающей паразитическую нагрузку на аппаратуру;
- уничтожение/модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами или администраторами этого программного обеспечения или данных;
- фальсификация своего сетевого адреса при передаче данных в сеть;
- фальсификация контактной информации, предъявленной владельцам или администраторам ресурсов или сетей;
- использование псевдонимов и анонимность, кроме случаев, когда право пользования соответствующими ресурсами или сетей разрешают анонимность при их использовании.

10. Сканировать порты на удаленных хостах. Это может быть расценено как попытка взлома, со всеми вытекающими последствиями;

Сканированием *считается выдача запросов, в том числе и единичных, на предмет наличия того или иного сервиса или опрос наличия работающих машин на группу адресов, либо опрос диапазона портов с целью определения работающих сервисов на одной машине или группе машин, а также выдача запросов, обработка которых не санкционирована принимающей стороной, не предусматривается сетевым сервисом или не разрешена администрацией ресурса.*

11. Сканировать диапазоны IP-адресов (всю легально предоставляемую информацию об удаленной сети можно получить средствами DNS, traceroute и т.п.);
12. Использовать сеть во вред другим пользователям, путем самостоятельного или с помощью третьих лиц вмешательства в действие аппаратуры и оборудования, а также иным способом;
13. Использовать доступ к компьютерным сетям для создания "сетевого шума" или "спама";
14. Рассылать не затребованную информацию по e-mail (спам), писем с указанием чужого адреса отправителя, писем угрожающего или оскорбляющего характера, "mailbombing", т.е.

отправку писем, переполняющих почтовый ящик получателя и препятствующих получению новой почты;
15. Распространять информацию, оскорбляющую честь и достоинство других пользователей и персонала компьютерных сетей;
16. Физически повреждать оборудование сети;
17. Устанавливать серверные операционные системы без специального разрешения системного администратора;
18. Пользователям, работающим с конфиденциальными документами (УБУиФК, ПФУ, УК, и т.п.) категорически запрещается пользоваться на рабочем месте различного рода мессенджерами (ICQ, MSN, Miranda, QIP, Mail.Ru агентами, Google messenger и т.д.);
19. Просмотр видео через сеть, за исключением случаев, связанных со служебной необходимостью;
20. Хранение на локальных и публичных сетевых дисках файлов, не относящихся к выполнению служебных обязанностей сотрудника (игры, видео, музыку, фотографии, виртуальные CD и т.п.);
21. Просмотр в рабочее время сайтов развлекательной направленности и сайтов, содержание которых не относится напрямую к служебным обязанностям работника;
22. Играть в рабочее и учебное время в онлайн игры;
23. Устанавливать нелицензионное программное обеспечение, а также свободно распространяемое (FreeWare) программное обеспечение, способное нарушить работу ККС;
24. Разрабатывать или распространять любые виды компьютерных вирусов, «троянских коней» или «логических бомб»;
25. Использовать ККС в деятельности, противоречащих законодательству Российской Федерации (см. Приложение 1).

Приложение 1.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно - вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Статья 274 УК РФ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.