Положение
О пользовании персональным компьютером и ресурсами сети в Частном учреждении профессионального образования "Белевский кооперативный техникум"

СОГЛАСОВАНО:

Решением педагогического совета

от « 05 » августа 2019г
Протокол № 01

г. Белёв
2019г

«УТВЕРЖДАЮ»
Директор ЧУ ПО Белевский
кооперативный техникум
_____Е.А.Овсянникова
Приказ №_____
«05» _____ 20___ г.

ИНСТРУКЦИЯ
О пользовании персональным компьютером и ресурсами сети

I. Общие положения

Данная инструкция по пользованию персональным компьютером обязательна к применению во всех подразделениях колледжа, так как это существенно уменьшает вероятность отказа компьютерного оборудования и сети.

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью колледжа и предоставляются работникам для осуществления ими их должностных обязанностей. Персональные компьютеры, серверы, программное обеспечение, оборудование ЛВС и коммуникационное, пользователи образуют систему корпоративной сети техникума.

1.1. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, для эффективного использования и распределения сетевых ресурсов коллективного пользования, поддержания необходимого уровня защиты информации, ее сохранности, соблюдения прав доступа к информации, уменьшение риска умышленного или неумышленного неправильного использования сетевых ресурсов.
1.2. К работе в системе допускаются лица, назначенные директором техникума и ознакомившиеся с данной инструкцией;
1.3. По уровню ответственности и правам доступа к сети пользователи сети разделяются на следующие категории: системные администраторы и пользователи;
1.4. Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к ней;
1.5. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором.

В общем случае имя это фамилия и инициалы сотрудника, написанные английскими буквами (регистр букв не имеет значения). Сотрудники должны знать точное написание своего индивидуального имени.
1.6. Каждый сотрудник может создать и изменять свой пароль для входа в компьютерную сеть; Пароль изменяется из пункта меню «Сменить пароль», в которое можно попасть, нажав после входа в систему одновременно клавиши Ctrl Alt Del. Регистр и язык имеют значение. Пользователи должны помнить свои пароли.
1.7. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем (в соответствии с пунктами 1.5-1.6 настоящей инструкции по пользованию компьютером и сетевыми ресурсами) для входа в компьютер, локальную сеть и сеть Интернет, передача их кому-либо запрещена;
1.8. В случае нарушения правил пользования сетью, связанных с используемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений;
1.9. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору;
1.10. Пользователи обязаны выполнять предписания системного администратора по работе с компьютером и сетью.
1.11. Системный администратор - лицо, обслуживающее сервер и следящее за правильным функционированием сети. Системный администратор дает разрешение на подключение компьютера к сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является нарушением правил пользования сетью;
1.12. Системный администратор информирует пользователей
обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;
1.13. Системный администратор имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

II. Работа за компьютером

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо

обратиться к системному администратору;
2.2. Все кабели, соединяющие системный блок с другими устройствами (особенно клавиатуры и мыши PS/2), следует вставлять и вынимать только при полностью обесточенном компьютере и выключенными дополнительными устройствами. Исключение составляют автономные USB-устройства: они могут быть подключены к включенному компьютеру; Полностью обесточенным считается компьютер с отключенным силовым проводом питания электросети. В помещении все электрические розетки должны соответствовать ГОСТ и иметь заземление. В случае подозрения на повреждение розетки или заземления до начала работы пользователь должен обратиться в обслуживающую данную электросеть организацию для устранения проблем. Запрещается включать мощные электроприборы (электрочайники, нагреватели, электроинструмент) в розетки, предназначенные для компьютерных устройств без письменного согласования с соответствующей организацией.
2.3. Запрещено подвергать механическим воздействиям компьютерные провода (например, ставить на них мебель, сильно перегибать прикреплять скрепками, завязывать узлом).
2.4. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. Этим занимается системный администратор;
2.5. Запрещено аварийно завершать работу компьютера кнопкой “Reset” или отключением от электросети. Завершайте работу компьютера правильно, через кнопку (Пуск) и Завершение работы;
2.6. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, загораживать (например, бумагами или мебелью) вентиляционные отверстия, проливать на него жидкости, просыпать семечки, скрепки, ставить у батареи и других нагревательных приборов);
2.7. Документы необходимо сохранять на специально отведенные диски, (обычно D:\"Мои документы") или в сети в месте определенным системным администратором. Запрещено хранить нужные документы и другие данные на системном диске С;
2.8. Если есть подозрения что, какие либо нужные документы уничтожены или повреждены, необходимо полностью прекратить работу с компьютером или сетевым ресурсом и незамедлительно обратиться к системному администратору.
2.9. По завершению рабочего дня компьютер можно выключить, по требованию системного администратора компьютер может быть оставлен включенным для проведения профилактических работ в нерабочее время;
2.10. Перед началом работы пользователь должен:

- ✓ Включить выключатель сетевого фильтра.
- ✓ При включении кнопка должна начать светиться;
- ✓ Включить монитор (если выключен);
- ✓ Включить компьютер кнопкой “Power”.

- ✓ Дождаться загрузки операционной системы (ОС);
- ✓ Войти в систему, используя свои личные имя пользователя и пароль (Имя пользователя обычно состоит из латинских букв в формате "Фамилия-ИО");

2.11.По завершению работы пользователь должен:

- ✓ Закрыть все открытые программы и документы, сохранив нужные изменения;
- ✓ С помощью меню “Пуск - Завершение работы” выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь);
- ✓ При возникновении ошибок во время работы с компьютером необходимо записать текст ошибки и код ошибки, после этого, если проблему не удается решить самостоятельно, обратится к системному администратору.

III. Работа в локальной сети

3.1 Пользователи сети обязаны:

3.1.1. Соблюдать правила работы в сети, оговоренные настоящей инструкцией;

3.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов;

3.1.3. Немедленно сообщать системному администратору сети об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администраторы, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры;

3.1.4. Не разглашать известную им конфиденциальную информацию, необходимую для безопасной работы в сети;

3.1.5. Обеспечивать беспрепятственный доступ системным администраторам к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

3.1.6. Выполнять предписания системных администраторов, направленные на обеспечение безопасности сети;

3.1.7. В случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.

3.1.8. Удалять с сетевых ресурсов устаревшие или не используемые файлы.

3.2 Пользователи сети имеют право:

3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Системные администраторы вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;
3.2.2. Обращаться к администратору сети по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться администратором сети;
3.2.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов сети;
3.2.4. Вносить предложения по улучшению работы с ресурсом.
3.3 Пользователям сети запрещено:
3.3.1. Разрешать посторонним лицам пользоваться вверенным им компьютером;
3.3.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с администрацией и системным администратором;
3.3.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;
3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;
3.3.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с системным администратором, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;
3.3.6. Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;
3.3.7. Работать с каналоёмкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с системным администратором сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя вызвавшего перегрузку, может быть прекращен;
3.3.8. Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;

3.3.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;
3.3.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором.
3.3.11. Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;
3.3.12. Использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

IV. Работа с электронной почтой

4.1. Электронная почта предоставляется сотрудникам колледжа только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или изменение параметров почтового ящика проводится системным администратором по просьбе администрации;
4.2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные администрацией. Прямой доступ к другим почтовым системам может быть блокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью системного администратора.
4.3. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными;
4.4. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.
4.5. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других сослуживцев;
4.6. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы (MS Outlook);
4.7. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).
4.8. Размер вложений у отправляемых писем обычно не должен превышать 10Мб. Для пересылки фотографий или больших файлов их нужно предварительно подготовить к отправке.

V. Работа в сети Интернет

5.1. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;
5.2. По использованию ресурсов Интернет необходимо ведение статистики.
5.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций;
5.4. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;
5.5. Все программы, используемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности;
5.6. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;
5.7. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.
5.8. Запрещается скачивать и запускать с любых ресурсов любые исполняемые файлы без согласования с системным администратором.

VI. Работа со съемными носителями информации (флеш - карты, переносные жесткие диски, цифровые фотоаппараты, телефоны и т.д)

6.1 Подключение съемных носителей следует производить при включенном компьютере и загруженной операционной системой.
6.2 Существует большое количество вирусов предназначенных для повреждения информации на флэш-картах (эти вирусы на зараженном ПК постоянно загружены в оперативную память и отслеживают порты на предмет подключения съемных устройств), если Вам нужно скопировать информацию с Вашей флэш-карты на посторонний ПК, перед подключением включайте блокировку записи (если она предусмотрена конструкцией Вашей флэшки).
6.3 Не извлекайте флэш-карту из ПК в момент обращения к ней, это может привести к потере данных и повреждению устройства. Если же в момент отключения флэш-карты от ПК выполнялась операция записи, в файловой системе флэш-карты неизбежно появятся ошибки. Если при попытке извлечь флэшку через значок "Безопасное извлечение устройства" появляется

диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство Универсальный том не может быть остановлено прямо сейчас. Попробуйте остановить его позже", значит, открыты какие-то файлы с флэш-карты. Закройте их и повторите попытку. Для сохранности данных не рекомендуется открывать файлы данных со сменных носителей.

6.4 Рекомендуется совершать обмен файлами данных через электронную почту. Перед копированием файлов данных с внешних носителей настоятельно рекомендуется проверить носитель с помощью антивируса. Запрещается запускать или переписывать с любых внешних носителей любые исполняемые файлы (приложения или командные файлы с расширениями exe, bat, com, cmd, inf, dll, scr) без согласования с системным администратором.

VII. Работа с периферийными устройствами (принтеры, ксероксы, сканеры, копиры)

7.1 Запрещается использовать для печати дешевую бумагу не соответствующего типа, а также использовать для печати бумагу со скрепками, наклейками или мятую бумагу.

7.2 Запрещается использовать не оригинальные картриджи. Не разрешается вынимать картриджи из принтеров за исключением их замены.

7.3 Не рекомендуется установка периферийной техники рядом с обогревательными приборами или на подоконнике, а также подвергать воздействию прямых солнечных лучей, влаги или пыли.