компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

**2. Работа за компьютером**

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо сообщить зам. заведующего по АХР.

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 к завхозу для устранения проблем. Запрещается включать мощные электроприборы (электрочайники, нагреватели, электроинструмент) в розетки, предназначенные для компьютерных устройств.

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.

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"). 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 нужно выключить.

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;

Выйти из системы.

2.12. При отключении электроэнергии источник бесперебойного питания (ИБП) позволяет компьютеру оставаться в рабочем состоянии от 5 до 20 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке сохранить документы и выключить компьютер в соответствии с данной инструкцией (пунтк 2.5).

2.13. Закрыть все открытые программы и документы, сохранив нужные изменения.

 2.14. С помощью меню “Пуск -> Завершение работы” выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь).

2.15. 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.

**3. 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 (имена пользователей, пароли), 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 (кроме случаев подключения/отключения ресурсов).

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.

**4. Работа с электронной почтой**

4.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено.

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. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

4.5. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается, как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

4.6. Размер вложений у отправляемых писем обычно не должен превышать 10Мб. Для пересылки фотографий или больших файлов их нужно предварительно подготовить к отправке.

**5. 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.

5.3. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство.

5.4. Все программы, используемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.

5.5. 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.

5.6. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.

**6. Работа со съемными носителями информации (флешки, 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 флэшках (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 флэшки на посторонний ПК, перед подключением включайте блокировку записи (если она предусмотрена конструкцией Вашей флэшки).

6.3 Не извлекайте флэшку из ПК в момент обращения к ней, это может привести к потере данных и повреждению устройства. Если же в момент отключения флэшки от ПК выполнялась операция записи, в файловой системе флэшки 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 флэшки. 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.

**7. 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.