

свано, прошнуровано и скреплено
1 (Пр) листов
ГБОУ «Самарское художественное
училище им. К.С. Петрова-Водкина»
Мисюк Г.М.



художественное училище
им. К.С. Петрова-Водкина»
Протокол № 5

от «07» декабря 2017 г.

Утверждаю:

Директор ГБОУ «Самарское
художественное училище
им. К.С. Петрова-Водкина»

Мисюк Г.М.

Приказ № 485 от «07» декабря 2017 г.



ПОЛОЖЕНИЕ О ПОЛЬЗОВАНИИ КОМПЬЮТЕРНЫМ И ПЕРИФЕРИЙНЫМ ОБОРУДОВАНИЕМ

1. Общие положения

- 1.1. Целью настоящего положения является регулирование работы 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, а так же бесперебойной работы персональных компьютеров, ноутбуков и периферийной техники.
- 1.2. К работе с компьютерной техникой допускаются лица, ознакомленные с данным положением, что должно быть отмечено в специальном журнале ознакомления.
- 1.3. По уровню ответственности и правам доступа к сети пользователи разделяются на следующие категории: сотрудники ГБОУ «Самарское художественное училище им. К.С. Петрова-Водкина» (далее – ОО), инженер-электроник (далее – администратор), пользователи и временные пользователи.
- 1.4. Временный пользователь — лицо, за которым не закреплена материальная ответственность, но которому необходимо временно использовать компьютер в образовательных целях (обучающийся, слушатель курсов и т.п.).
- 1.5. Временный пользователь несет оговоренную в данном положении ответственность при использовании компьютера в образовательных целях на уровне пользователя.
- 1.6. Контроль за соблюдением пунктов настоящего положения временным пользователем осуществляется сотрудником ОО, за которым закреплена материальная ответственность на компьютеры и оборудование, предоставляемые временному пользователю (например, в учебных кабинетах, оснащенных ПК и УПМ).
- 1.7. Пользователь компьютера – сотрудник ОО, за которым закреплена материальная ответственность за данный компьютер.
- 1.8. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к ней.
- 1.9. Пользователь так же должен принимать все меры по недопущению физического повреждения компьютера и установке программного обеспечения лицами, не входящими в состав коллектива ОО, за исключением случаев, когда происходит обслуживание специализированными фирмами программного обеспечения. В случае обнаружения нарушений данного пункта, администратор имеет право изъять компьютер пользователя и передать его другим работникам ОО.
- 1.10. Пользователю запрещается вынос компьютера (ноутбука) и периферийной техники за пределы ОО, за исключением случаев, согласованных с администратором с соответствующей записью в журнале учета оборота оргтехники.
- 1.11. Каждый пользователь пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым администратором. Сотрудники должны знать точное написание своего индивидуального имени.

1.12. Каждый сотрудник может создать и изменять свой пароль для входа в компьютерную сеть; регистр и язык имеют значение. Не все системы поддерживают пароли на русском языке, поэтому необходимо использовать английский. Пользователи должны помнить свои пароли.

1.13. Каждый пользователь должен пользоваться только своим именем пользователя и паролем для входа в компьютер, локальную сеть и сеть Интернет, передача их кому-либо запрещена. Ответственность за утерю данных, произошедших в результате утери пароля или передачи его третьим лицам, лежит на пользователе.

1.14. В случае нарушения правил пользования сетью, связанных с используемым им компьютером, пользователь сообщает администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений.

1.15. 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 администратору.

1.16. Пользователи обязаны выполнять предписания администратора по работе с компьютером, локальной сетью и сетевыми ресурсами.

1.17. Администратор дает разрешение на подключение компьютера к сети сам или выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является нарушением правил пользования сетью.

1.18. 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.

1.19. Администратор имеет право отключить (самостоятельно) 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 настоящего положения.

2. Инструкция по работе за компьютером

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться к Администратору, сделав запись в соответствующем журнале заявок.

2.2. Все кабели, соединяющие системный блок с другими устройствами (особенно клавиатуры и мыши PS/2), следует вставлять и вынимать только при экстренной необходимости 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 случае подозрения на повреждение розетки или заземления до начала работы пользователь должен обратиться в хозяйственную часть 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, или через третьих лиц, не входящих в состав сотрудников ОО, за исключением случаев, согласованных с администратором (например, в случае обслуживания программного обеспечения специализированными фирмами), устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. В случае обнаружения нарушений данного пункта, администратор имеет право изъять компьютер пользователя и передать его другим работникам ОО.

2.5. Запрещено аварийно завершать работу компьютера кнопкой "Reset" или отключением от

электросети. Необходимо правильно завершать работу компьютера: с помощью меню «Пуск - Завершение работы».

2.6. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, загоразивать (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 в папке «Мои документы», на специально отведенные диски или в сети в месте, определенные администрацией ОО. Запрещено хранить нужные документы и другие данные в корневом каталоге системного диска С или на рабочем столе операционной системы.

2.8. Если есть подозрения на то, что какие-либо нужные документы уничтожены или повреждены, необходимо полностью прекратить работу с компьютером или сетевым ресурсом и незамедлительно обратиться к администратору.

2.9. По завершению рабочего дня компьютер можно выключить. По требованию администратора, ответственного за точку доступа в Интернет, компьютер может быть оставлен включенным для проведения профилактических работ в нерабочее время.

2.10. Перед началом работы пользователь должен:

2.10.1 Включить выключатель сетевого фильтра. При включении кнопка должна начать светиться. Если включается ноутбук — при необходимости включить блок питания.

2.10.2 Включить источник бесперебойного питания (при его наличии) и выждать 2-4 секунды.

2.10.3 Включить монитор (если выключен).

2.10.4 Включить компьютер (ноутбук) кнопкой “Power”. Дождаться загрузки операционной системы (ОС).

2.10.5 Войти в систему, используя свои личные имя пользователя и пароль.

2.11. По завершению работы пользователь должен:

2.11.1 Закрывать все открытые программы и документы, сохранив нужные изменения.

2.11.2 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.

2.12.1 Закрывать все открытые программы и документы, сохранив нужные изменения.

2.12.2 С помощью меню “Пуск - Завершение работы” выключить компьютер и дождаться завершения работы.

2.13. При возникновении ошибок во время работы с компьютером необходимо записать текст ошибки и код ошибки, после этого, если проблему не удастся решить самостоятельно, обратиться к администратору.

3. Инструкция по работе в локальной сети

3.1. Пользователи сети обязаны:

3.1.1 Соблюдать правила работы в сети, оговоренные настоящим положением.

3.1.2 При доступе к внешним ресурсам сети, соблюдать правила, установленные администрацией ОО для используемых ресурсов.

3.1.3 Немедленно сообщать администратору об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо.

3.1.4 Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети.

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

3.1.6 Выполнять инструкции, 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 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 настоящем положении рамках. Администратор 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 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.

3.2.3 Обращаться за помощью к 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 ОО.

3.3.3 Самостоятельно устанавливать или удалять установленные 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 администратором, изменять настройки BIOS, а также производить загрузку рабочих станций (компьютеров, ноутбуков) с внешних носителей.

3.3.6 Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный 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 каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с администратором. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя, вызвавшего перегрузку, к локальной сети, может быть прекращен без предупреждения.

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 Обходжение (попытка обходжения) учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

3.3.10 Использовать иные формы доступа к сети Интернет, за исключением разрешенных администрацией ОО.

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.

4. Инструкция по работе с электронной почтой

4.1. Электронная почта предоставляется сотрудникам ОО только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или изменение параметров почтового ящика проводится администратором по просьбе администрации ОО.

4.2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные администрацией ОО. Прямой доступ к другим почтовым системам может быть заблокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью администратора.

4.3. Все электронные письма, создаваемые и хранимые на компьютерах ОО, являются собственностью ОО и не считаются персональными.

4.4. Администрация ОО 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 всех сотрудников ОО.

4.6. В качестве клиентов электронной почты могут использоваться только программы, входящие в список разрешенных для использования в ОО.

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 не должен превышать 10Мб. Для пересылки фотографий или больших файлов их нужно предварительно подготовить к отправке (обработать в графическом редакторе для уменьшения размера, упаковать в архив и т.п.).

5. Инструкция по работе 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 и эти программы внесены в список разрешенных для использования в ОО.

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 об отключении компьютера пользователя от сети Интернет или передаче его другому сотруднику ОО.

5.4. Сотрудникам ОО, 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 администрацией ОО и входить в список разрешенных для использования. 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 ответственным за точку доступа к Интернет-ресурсам администратором.

6. 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 необходимо скопировать информацию с флэш-карты на ПК, перед подключением нужно включить блокировку записи (если она предусмотрена конструкцией флэш-карты).
- 6.3. Не извлекайте флэш-карту из ПК в момент записи или копирования информации, 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.
- 6.4. Если при попытке извлечь флэш-карту через значок "Безопасное извлечение устройства" появляется диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство 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.
- 6.5. По возможности, рекомендуется совершать обмен файлами данных через электронную почту или сетевые ресурсы, включая электронную систему обучения. 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 администрацией ОО.
- 6.6. Категорически не рекомендуется хранить на переносных съемных носителях важную информацию в единственном экземпляре без наличия копий на компьютере или сетевом ресурсе. Нередки случаи безвозвратной утери важной информации из-за повреждения или сбоя в работе съемного носителя.

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 использование картриджей, не совместимых с используемой моделью принтера. Не разрешается вынимать картриджи из принтеров за исключением их замены. Замена картриджей выполняется сотрудниками ОО после предварительной заявки в журнале учета замены картриджей.
- 7.3. Запрещается устанавливать периферийную технику рядом с обогревательными приборами или на подоконнике, а также подвергать воздействию прямых солнечных лучей, влаги или пыли.