

Согласовано  
Председатель ПК  
\_\_\_\_\_ Р.Н.Чмыкова

Утверждаю:  
Директор МАОУ «Покчинская  
ООШ имени И.И.Широкшина»  
\_\_\_\_\_ О.В.Белина

### **Инструкция пользователя по безопасной работе в сети Интернет**

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью школы и предоставляются учащимся и учителям.

ПК, серверы, ПО, оборудование ЛВС и коммуникационное, пользователи образуют систему локальной сети школы (далее СЕТЬ)

Общие положения:

- 1.1. Настоящая инструкция является руководством по целевому использованию СЕТИ.
- 1.2. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации. Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования.
- 1.3. К работе в системе допускаются лица, назначенные начальником соответствующего отдела и прошедшие инструктаж и регистрацию у ответственного за работу в сети Интернет.
- 1.4. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение системного администратора.
- 1.5. По уровню ответственности и правам доступа к СЕТИ пользователи СЕТИ разделяются на следующие категории: системные администраторы и пользователи.
- 1.6. Пользователь подключенного к СЕТИ компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.
- 1.7. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором.
- 1.8. Каждый сотрудник САМ создает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 8 символов и состоять из букв и цифр.
- 1.9. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.
- 1.10. Для работы на компьютере кроме пользователя необходимо разрешение системного администратора. Никто не может давать разрешение на даже временную работу на компьютере, без разрешения системного администратора.
- 1.11. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь

данного компьютера, администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.12. 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 СЕТИ.

1.13. Системный администратор и 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 серьезнейшим нарушением правил пользования СЕТЬЮ.

1.14. Системный администратор информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.

1.15. 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.

1.16. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе.

2. Пользователи СЕТИ обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

2.2. При доступе к внешним ресурсам СЕТИ, соблюдать правила, установленные системными администраторами для используемых ресурсов.

2.3. Немедленно сообщать системному администратору СЕТИ или начальнику отдела ИТО 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.

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

2.5. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к СЕТИ до тех пор, пока системные администраторы не удостоверятся в удалении вируса.

2.6. Обеспечивать беспрепятственный доступ специалистам отдела ИТО к сетевому оборудованию и компьютерам пользователей.

2.7. Выполнять предписания специалистов отдела ИТО, направленные на обеспечение безопасности СЕТИ.

2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.

3. Пользователи СЕТИ имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с системным администратором или руководством школы. 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. 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 системным администратором СЕТИ.

3.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов СЕТИ.

3.4. Вносить предложения по улучшению работы с ресурсом.

4. Пользователям СЕТИ запрещено:

4.1. Разрешать посторонним лицам пользоваться вверенным им компьютером.

4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с администратором.

4.3. 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.

4.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет.

4.6. 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.

4.7. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с системным администратором СЕТИ. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен.

4.8. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

4.9. Обходнение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

4.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить установленный администратором межсетевой экран при соединении с сетью Интернет.

4.11. Осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить или участвовать в сетевых атаках и сетевом взломе.

4.12. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4.13. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

4.14. Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера Сети, равно как и любых других компьютеров в Интернет.

4.15. Закрывать доступ к информации паролями без согласования с системным администратором.

5. Работа с электронной почтой:

- 5.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.
- 5.2. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными.
- 5.3. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.
- 5.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными.
- 5.5. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.
- 5.6. Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.
- 5.7. Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками организации, и о таких случаях должно докладываться.
- 5.8. Почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось с помощью цифровой подписи отправителя.
- 5.9. Необходимо организовать обучение пользователей правильной работе с электронной почтой.
- 5.10. Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.
- 5.11. Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.
- 5.12. Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту организации.
- 5.13. Вся информация, классифицированная как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Интернет, Должна быть предварительно зашифрована.
- 5.14. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности фирмы.
- 5.15. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других сослуживцев.
- 5.16. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.
- 5.17. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.
- 5.18. Конфиденциальная информация не может быть послана с помощью электронной почты.
- 5.19. Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, он будет наказан.
- 5.20. Нельзя сообщать сторонним лицам электронные адреса фирмы.
- 5.21. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.
- 5.22. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5.23. Использовать несуществующие обратные адреса при отправке электронных писем.

6. При работе с веб-ресурсами:

6.1. Пользователи используют программы для поиска информации в WWW только в случае, если это необходимо для выполнения своих должностных обязанностей.

6.2. Использование ресурсы сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать Фирме.

6.3. По использованию Интернет ведется статистика и поступает в архив фирмы.

6.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему в санкций.

6.5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности Фирмы.

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

6.7. Все файлы, загружаемые с помощью сети Internet, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.

6.8. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet. Доступ к сети Internet предоставляется по служебной записке.

6.9. В организации должен вестись список запрещенных сайтов. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

6.10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

6.11. 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.

6.12. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.

7. Ответственность:

7.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

7.2. Системный администратор отвечает за бесперебойное функционирование вверенной ему СЕТИ, качество предоставляемых пользователям сервисов.

7.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.

7.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы с СЕТЬЮ.

7.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или СЕТИ компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.