

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 МОБУ СОШ №20 имени Ф.К.Попова.

1. Общие положения.

1.1. Настоящая инструкция является дополнением к Правилами использования сети Интернет.

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, прошедшие инструктаж 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.

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. 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.

1.8. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает 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.

1.9. 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 Администратору СЕТИ.

1.10. Администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ. 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.

1.11. 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.

1.12. 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.

1.13. 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 Администраторами для используемых ресурсов.

2.3. Немедленно сообщать 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.

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 администраторы не удостоверятся в удалении вируса.

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

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

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

3. Пользователи СЕТИ имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. 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 за помощью к Администратору при решении задач использования ресурсов СЕТИ.

3.3. Вносить предложения по улучшению работы с ресурсом.

4. Пользователям СЕТИ запрещено:

4.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами).

4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами.

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. Обходление 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 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. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

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

5.3. Нельзя сообщать сторонним лицам электронные адреса сотрудников.

5.4. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

5.5. 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 ресурсов сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать школе.

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

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

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

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

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

6.8. 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.

6.9. 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. 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.