МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 5»

ПРИНЯТО
педагогическим советом
МКОУ «СОШ № 5»
Протокол № 1 от 26.08.2021г.

УТВЕРЖДЕНО
Директор МКОУ «СОШ № 5»
Т.Н. Мурадханова
Приказ № 165 от 26.08.2021г.

МКОУ «СОШ № 5»

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ПО БЕЗОПАСНОСТИ
ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

с. Эдиссия

2021 год

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью МКОУ «СОШ № 5» и предоставляются обучающимся и учителям.

ПК, серверы, ПО, оборудование локально – вычислительной сети и коммуникационное, пользователи образуют систему локальной сети МКОУ «СОШ № 5»

1. **Общие положения:**

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.

К работе в системе допускаются лица, администрацией школы и прошедшие инструктаж и регистрацию у ответственного за работу в сети Интернет.

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.

По уровню ответственности и правам доступа к СЕТИ пользователи СЕТИ разделяются на следующие категории: системные администраторы и пользователи.

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.

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.

Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.

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.

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.

В случае появления у пользователя компьютера сведений или подозрений о фактах нарушениянастоящих 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.

Системный администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ. Системный администратор дает разрешение на подключение компьютера к СЕТИ. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.

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.

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.

Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и начальнике отдела ИТО.

2. Пользователи СЕТИ обязаны:

Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

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

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.

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

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

Обеспечивать беспрепятственный доступ системному администратору к сетевому оборудованию и компьютерам пользователей.

Выполнять предписания системного администратора, направленные на обеспечение безопасности СЕТИ.

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

3. Пользователи СЕТИ имеют право:

Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с отделом ИТО. 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.

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.

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

Вносить предложения по улучшению работы с ресурсом.

4. Пользователям СЕТИ запрещено:

Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаевподключения/отключения ресурсов, выполняемого специалистами ИТО).

Использовать сетевые программы, не предназначенные для выполнения прямых служебныхобязанностей без согласования с системным администратором.

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.

Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

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 дисков или флэш-карт.

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 угрозубезопасности информации на других компьютерах.

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.

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.

Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

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

Осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить

илиучаствовать в сетевых атаках и сетевом взломе.

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.

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.

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

Закрывать доступ к информации паролями без согласования с системным администратором.

5. Работа с электронной почтой:

Электронная почта школы предоставляется сотрудникам только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

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

Необходимо организовать обучение пользователей правильной работе с электронной почтой

Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.

Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту школы.

Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение правил работы с электронной почтой.

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

В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

Конфиденциальная информация не может быть послана с помощью электронной почты.

Если будет установлено, что сотрудник неправильно использует электронную почту с

умыслом, он будет наказан.

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

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

Запрещено использовать несуществующие обратные адреса при отправке электронных писем.

6. При работе с веб-ресурсами:

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

Использование ресурсы сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать информационной системе школы.

По использованию Интернет ведется статистика.

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

Сотрудникам школы, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским.

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

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

Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet.

В школе должна быть организована фильтрация запрещенных ресурсов Internet. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

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

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.

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

7. Ответственность:

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

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

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

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

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.