ПРИНЯТО:
Совет по вопросам регламентации доступа к Интернет

от 16.02.2021

УТВЕРЖДЕНО:
Директор МБОУ «Сиверская СОШ №3»

О.А.Воропаева

Приказ от 17.02.2021 № 5

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 муниципального бюджетного общеобразовательного учреждения «Сиверская средняя общеобразовательная школа № 3» (структурное подразделение- дошкольные группы) (далее - ОУ) и предоставляются работникам.

ПК, серверы, ПО, пользователи образуют систему локальной Сети МБОУ «Сиверская СОШ №3».

1.Общие положения

1.1. Настоящая инструкция является дополнением к Регламенту по работе работников в Сети Интернет (далее- Сети).
1.2. Целью настоящей инструкции является регулирование работы пользователями Сетью, 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. По уровню ответственности и правам доступа к Сети пользователи Сети разделяются на следующие категории: ответственный за работу «точки доступа к Интернет» и пользователи.
1.4. К работе в системе допускаются лица, прошедшие инструктаж и регистрацию у ответственного за работу в Сети Интернет.
1.5. 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.
1.6. Работа в системе каждому работнику разрешена только на прикрепленных к нему компьютере, в рабочее время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать с другими программами, необходимо получить разрешение ответственного за работу «точки доступа к Интернет».
1.7. Каждый работник ОУ создает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 8 символов и состоять из букв и цифр.
1.8. Для работы на компьютере кроме пользователя необходимо разрешение ответственного за работу «точки доступа к Интернет». Никто не может давать разрешение на даже временную работу на компьютере, без разрешения ответственного за работу «точки доступа к Интернету в ОУ».

1.9. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает ответственному за работу «точки доступа к Интернет», который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, ответственный за работу «точки доступа к Интернет» имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.10 . 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 ответственному за работу «точки доступа к Интернет».

1.11 . Ответственный за работу «точки доступа к Интернет» 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.

1.12 . Ответственный за работу «точки доступа к Интернет в ОУ» 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.

1.13 . Ответственный за работу «точки доступа к Интернет» 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.

1.14. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на ответственном за работу «точки доступа к Интернет».

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 ответственным за работу «точки доступа к Интернет» для используемых ресурсов.

2.3. Немедленно сообщать ответственному за работу «точки доступа к Интернет» об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Ответственный за работу «точки доступа к Интернет» в ОУ должен 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 ответственный за работу «точки доступа к Интернет» в ОУ не удостоверится в удалении вируса.

2.6. Обеспечивать беспрепятственный доступ ответственного за работу «точки доступа к Интернет» в ОУ к сетевому оборудованию и компьютерам пользователей.

2.7. Выполнять предписания ответственного за работу «точки доступа к Интернет», направленные на обеспечение безопасности Сети.

2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к ответственному за работу «точки доступа к Интернет».

3. Пользователи Сети имеют право:

3.1. 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. Обращаться к ответственному за работу «точки доступа к Интернет» 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 ответственным за работу «точки доступа к Интернет» в ОУ.

3.3. Обращаться за помощью к ответственному за работу «точки доступа к Интернет» 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 (кроме случаев подключения/отключения ресурсов, выполняемого специалистами ЦИТ).

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

4.3. Самостоятельно устанавливать или удалять установленные ответственным за работу «точки доступа к Интернет» 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 ответственного за работу «точки доступа к Интернет», изменять настройки BIOS, а также производить загрузку рабочих станций с посторонних носителей.

4.6. Самовольно подключать компьютер к Сети, а также изменять IP-адрес компьютера, выданный ответственным за работу «точки доступа к Интернет». 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. 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.

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

4.9. Использовать иные формы доступа к Сети Интернет, за исключением разрешенных ответственным за работу «точки доступа к Интернет».

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

4.11. 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.

4.12. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (ответственный за работу «точки доступа к Интернету в ОУ») 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.

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

4.14. Закрывать доступ к информации паролями без согласования с ответственным за работу «точки доступа к Интернет».

5. Работа с электронной почтой:

5.1. Электронная почта предоставляется работникам 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 работников, 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 работниками организации, и о таких случаях должно докладываться.

5.8. Необходимо организовать обучение пользователей правильной работе с электронной почтой.

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

5.10. 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.

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

5.12. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других работников.

5.13. ОУ оставляет за собой право осуществлять наблюдение за почтовыми отправлениями работников. Электронные письма могут быть прочитаны ОУ, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.

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

5.15. Конфиденциальная информация не может быть послана с помощью электронной почты.

5.16. Если будет установлено, что работник неправильно использует электронную почту с умыслом, он будет наказан.

5.17. Нельзя сообщать сторонним лицам электронные адреса фирмы.

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

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

5.20. 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 ОУ.

6.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему в санкции.
6.4. Работникам ОУ, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности ОУ.
6.5. Все программы, используемые для доступа к Сети Интернет, должны быть утверждены ответственным за работу «точки доступа к Интернет» и на них должны быть настроены необходимые уровни безопасности.
6.7. Все файлы, загружаемые с помощью Сети Интернет, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.
6.8. Работники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Интернет. Доступ к Сети Интернет предоставляется по служебной записке.
6.9. В ОУ должен вестись список запрещенных сайтов. Программы для работы с Интернет должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.
6.10. Запрещено размещать на 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. Ответственный за работу «точки доступа к Интернет» 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.