

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 20 МУНИЦИПАЛЬНОГО  
ОБРАЗОВАНИЯ ТЕММРЮКСКИЙ РАЙОН**



**ИНСТРУКЦИЯ  
Пользователя по компьютерной безопасности при работе в сети  
интернет МБДОУ ДС № 20 МОТР**

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети (ЛВС), коммуникационное оборудование являются собственностью МБДОУ ДС № 20 МОТР и предоставляются работникам для осуществления ими их должностных обязанностей.

Целью настоящей инструкции является регулирование работы пользователей, распределение сетевых ресурсов коллективного пользователя 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.

Персональные компьютеры, сервер, программное оборудование, оборудование ЛВС и коммуникационное, пользователи образуют систему корпоративной сети (далее СЕТЬ).

Работа в системе каждому работнику разрешена только на определенных компьютерах, в рабочее время и только с разрешенными программами и сетевыми ресурсами.

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 к ней.

Пользователю запрещается:

- загружать, самостоятельно устанавливать прикладное, оперативное сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- использовать ресурсы Интернет в не служебных целях;
- допускать к работе посторонних лиц;
- строго запрещается подключаться к ресурсам Интернет, используя персональный компьютер учреждения через не служебный канал доступа, сотовый телефон, модем, и др. устройства;
- 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;
- повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;
- использовать электронную почту в личных целях;
- осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам);

- открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем;
- использовать несуществующие обратные адреса при отправке электронных писем;
- вскрывать компьютеры, сетевое и периферийное оборудование;
- подключать к компьютеру дополнительное оборудование;
- использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей;
- самовольно подключать компьютер к СЕТИ, а также изменять IP – адрес компьютера;
- 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;
- осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить или участвовать 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 право пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

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

Использование ресурсов сети Интернет разрешается только в рабочих целях, использование ее ресурсов не должно потенциально угрожать учреждению.

Сотрудникам учреждения. Пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или расистским и не относящимся к деятельности учреждения.

С целью обеспечения компьютерной безопасности пользователь обязан:

1. Знать и уметь пользоваться антивирусным программным обеспечением, установленным на каждый компьютер.
2. Включить режим автоматического сканирования файловой системы.
3. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера.
4. Активировать функцию ежедневного автоматического обновления антивирусных баз.
5. Ежедневно проверять состояние антивирусного программного обеспечения, а именно:
  - режим автоматической защиты должен быть включен постоянно;
  - дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;
  - просматривать журналы ежедневных антивирусных проверок;
 Контролировать удаление вирусов при их появлении.
6. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
7. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.
8. Запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
9. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.

10. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Интернет сети и сообщить об этом в обслуживающую организацию.  
Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках.  
Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.  
Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами а СЕТИ и за ее пределами.