УТВЕРЖДЕНО
приказом заведующего
МАДОУ «Конструктор успеха» г. Перми
от 11.12.2023 г. №01-08/325
Заведующий _____ М.В. Пынзарь

ПРАВИЛА
пользования средствами антивирусного ПО

Антивирусная защита в МАДОУ «Конструктор успеха» г. Перми применяется с целью защиты информационных ресурсов и ПО от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ) посредством использования специализированного ПО.

Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах), Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

1. Обязанность по своевременному получению и предоставлению МАДОУ «Конструктор успеха» г. Перми лицензионных ключей антивирусного ПО возлагается на ИП «Рубцов А.С.».
2. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ работников ДОУ возлагается на системного администратора.
3. При установке антивирусного ПО системным администратором должны выполняться следующие требования:

- актуализация антивирусных баз на АРМ, подключенных к локальной сети ДОУ, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;
- актуализация антивирусных баз на АРМ, не подключенных к локальной сети ДОУ, должна осуществляться с использованием съемных носителей информации не реже одного раза в неделю;
- проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

4. Некоторые признаки проявления вируса:

прекращение работы или неправильная работа ранее успешно функционировавшего ПО;
медленная работа АРМ;
невозможность загрузки операционной системы;
нетипичная работа ПО;
вывод на экран непредусмотренных сообщений или изображений; подача непредусмотренных звуковых сигналов;
частые зависания и сбои в работе АРМ;
частое появление сообщений о системных ошибках;
исчезновение файлов, каталогов или искажение их содержимого; изменение даты и времени модификации файлов;

изменение размеров файлов;

неожиданное значительное увеличение количества файлов на диске; существенное уменьшение размера свободной оперативной и дисковой памяти.

5. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде работники обязаны:

- убедиться, что на АРМ установлено и включено антивирусное ПО;

- незамедлительно сообщить заместителю заведующего о нарушениях работы антивирусного ПО;

- перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;

- при переносе на свой АРМ файлов в архивированном виде проверять их до и после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

- использовать антивирусное ПО для входного контроля всех файлов (исполняемых файлов, файлов данных, сообщений электронной почты и так далее), получаемых из компьютерных сетей, а также на съемных носителях информации;

- в случае установки или изменения ПО при возникновении подозрения на наличие вирусов проверять на наличие вирусов жесткие диски АРМ, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.

6. Работникам запрещается:

- открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;

- переходить по ссылкам в спам-письмах;

- загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла.

7. При возникновении подозрения на наличие вирусов работники обязаны:

- приостановить все операции, связанные с обработкой файлов на АРМ;

- запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;

- о факте обнаружения вирусов немедленно сообщить зам. заведующего, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе; - провести анализ необходимости дальнейшего использования зараженных вирусом файлов; провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компьютера.