

Согласовано
на педагогическом совете
протокол № 2
от "15" 09 2014 г.

Утверждено
Директор школы
О.А. Явственная
приказ № 48
от "16" 09 2014 г.



Регламент организации антивирусной защиты в МКОУ "Большедворская ООШ"

1. Общие положения

- 1.1. Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей образовательной организации к непродуктивным Интернет-ресурсам и контроля их электронной переписки.
- 1.2. основополагающими требованиями к системе антивирусной защиты ОУ являются:
 - решение задачи антивирусной защиты должно осуществляться в общем виде;
 - средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;
 - решение задачи антивирусной защиты должно осуществляться в реальном времени.
- 1.3. Мероприятия, направленные на решение задач по антивирусной защите:
 - установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение;
 - регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);
 - непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
 - анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;
 - проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;
 - проведение регулярных проверок целостности критически важных программ и данных;
 - внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;
 - необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2. Технологические инструкции

- 2.1. Руководителем образовательной организации назначается лицо, ответственное за

антивирусную защиту. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя образовательной организации.

- 2.2. В МКОУ "Большедворская ООШ" может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.
- 2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
- 2.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
- 2.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

3. Требования к проведению мероприятий по антивирусной защите

- 3.1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.
- 3.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию.
- 3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:
 - Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.
 - При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).
 - При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.
- 3.4. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:
 - приостановить работу;
 - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия – директора) ОУ;
 - совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
 - провести лечение или уничтожение зараженных файлов;
 - в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на внешнем носителе в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

4. Ответственность

4.1. Ответственность за организацию антивирусной защиты возлагается на руководителя ОУ или лицо, им назначенное.

4.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

4.3. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется руководителем или специалистом, им назначенным.