

Рассмотрено
на педагогическом собрании
от 09.01.2019 г. № 3

Дир. шк. *Кравченко О.А.*
Кравченко О.А.

ИНСТРУКЦИЯ
по организации антивирусной защиты в муниципальном бюджетном
общеобразовательном учреждении средней общеобразовательной школе пгт.
Приисковский

1. Общие положения

- 1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в МБОУ СОШ пгт. Приисковский (далее - ОУ) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей ОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.
- 1.2. Директором школы назначается лицо, ответственное за организацию антивирусной защиты в ОУ.
- 1.3. В ОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.
- 1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в ОУ.
- 1.5. 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 (магнитных дисках, лентах, CD- ROM, DVD, flash-накопителях и т.п.).
- 1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.
- 1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.
- 1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
- 1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. Мероприятия, направленные на решение задач по антивирусной защите:

- 2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.
- 2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю в понедельник с 14.00).
- 2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы (далее ИКС) ОУ.
- 2.4. 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.
- 2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.
- 2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.
- 2.7. Обеспечение бесперебойной работы ОУ для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите.

- 3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.
- 3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.
- 3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:
 - 3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ОУ;
 - 3.3.2. 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.);
 - 3.3.3. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса.

- 4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:
 - 4.1.1. приостановить работу;
 - 4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ОУ;
 - 4.1.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
 - 4.1.4. провести лечение или уничтожение зараженных файлов.
- 4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность.

- 5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором ОУ.
- 5.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ возлагается на ответственного за организацию антивирусной защиты.
- 5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.
- 5.4. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором ОУ и фиксируется Актом проверки (не реже 1 раза в квартал).