

Принято
решением педагогического совета
протокол от "29" 08 2019
№ 1

Утверждаю
Директор школы
Г.Р. Ахмерова
Приказ от "29" 08 2019
№ 34/11



ПОЛОЖЕНИЕ
по организации антивирусной защиты компьютеров в Государственном
казенном общеобразовательном учреждении «Вечерняя (сменная)
общеобразовательная школа № 36»

I. Общие положения

1.1. Настоящее Положение определяет порядок организации антивирусной защиты компьютеров Государственном казенном общеобразовательном учреждении «Вечерняя (сменная) общеобразовательная школа № 36» (далее - школа) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и персональные данные, обрабатываемые и хранимые школой, возникновения фактов заражения программного обеспечения компьютерными вирусами.

1.2. Положение разработано в соответствии с действующими редакциями нормативных документов:

- ФЗ "Об образовании в Российской Федерации" от 29.12.2012 №273-ФЗ;
- ФЗ "О персональных данных" от 27.07.2006 №152-ФЗ;
- "Уголовного кодекса Российской Федерации" от 13.06.1996 №63-ФЗ (глава 28. "Преступления в сфере компьютерной информации");
- Постановления Главного государственного санитарного врача РФ от 29.12.2010 №189 "Об утверждении СанПиН 2.4.2.2821-10 "Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях";
- Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 05.12.2016 №646;
- Устава школы.

II. Ответственность при организации антивирусной защиты

2.1. Ответственность за организацию антивирусной защиты в школе возлагается на специалиста ЭВТ и персонально на каждого педагога за антивирусную защиту закрепленного компьютера (НОУТБУКА).

2.2. Специалист ЭВТ обеспечивает:

- функционирование, поддерживает работоспособность систем защиты информации;
- периодический контроль состояния антивирусной защиты в школе.

III. Порядок организации антивирусной защиты

3.1. В школе средства антивирусного контроля устанавливаются и настраиваются специалистом ЭВТ на все компьютеры (ноутбуки) и автоматизированные рабочие места пользователей для обеспечения защиты от внедрения вредоносного программного обеспечения (далее - ВПО) в них со съемных носителей.

3.2. Все устанавливаемые программы антивирусного контроля должны быть лицензионными (либо свободно-распространяемыми (СГ10)).

3.3. При осуществлении антивирусной защиты выполняются следующие обязательные мероприятия:

- контроль съемных носителей информации на предмет наличия на них ВПО до начала работы с ними;

- периодическая проверка на предмет наличия ВПО жестких дисков не реже одного раза в месяц;
- внеплановая проверка жестких дисков и съемных носителей информации в случае подозрения на наличие ВПО;
- восстановление работоспособности программных средств и информационных систем, поврежденных программными вирусами.

IV. Порядок действий при обнаружении ВПО

4.1. При обнаружении ВПО на съемных носителях пользователь персонального компьютера обязан;

- приостановить работу с источником угрозы (съемным носителем);
- принять меры по локализации и удалению ВПО, рекомендованные специалистом ЭВТ.
- в случае невозможности удаления ВПО вновь обратиться к специалисту ЭВТ

4.2. В случае невозможности удаления пользователем ВПО, специалист ЭВТ обязан:

- лично принять меры по локализации и удалению ВПС на рабочем месте пользователя;

- при не устранении проблемы по мере необходимости обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты.

- при передаче образцов зараженных файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации, специалистом ЭВТ должны быть соблюдены требования конфиденциальности обрабатываемой в школе информации.