СОГЛАСОВАНО
Педагогическим советом
МБОУ «СШ № 33»
«31» августа 2016г.

СОГЛАСОВАНО
Председатель Управляющего совета
МБОУ «СШ № 33»
Т.Ш. Бологова
«01» сентября 2016г.

УТВЕРЖДАЮ
Директор МБОУ «СШ № 33»
(Должность руководителя, наименование ОО)
_____ /Ковалева Е.Н. /
(Подпись) (И.О. Фамилия)
«01» сентября 2016г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ТЕХНИКИ МБОУ «СШ № 33»

I. Общие положения

1.1. Положение об организации антивирусной защиты компьютерной техники МБОУ «СШ № 33»(далее – положение, школа) разработано в соответствиис:

- Федеральным Законом РФ от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральным Законом РФ от 28.07.2012 г. М139-ФЗ «О внесении изменений в ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»;
- Федеральным Законом от 0.07.2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»;
- Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Письмом заместителя Министра образования и науки Российской Федерации от 28.09.2011 г. №АП-1057/07 «О правилах подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет»;
- Методическими рекомендациями по ограничению образовательных в организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет от 01 июля 2015 г. № 280-245;
- Уставом МБОУ «СШ № 33».

1.2. Настоящее положениепредназначено для определенияпорядка проведения антивирусной защиты и предотвращения возникновения фактов заражения программного обеспечения школы компьютерными вирусами.

1.3.Ответственным за организацию антивирусной защиты вШколе является специалист школы, имеющий доступ к головному компьютеру сервера и локальной сети школы.

1.4. На компьютерном оборудовании школыможет использоваться только лицензионное антивирусное программное обеспечение, либо свободно-распространяемое программное обеспечение.

1.5. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты школы.

1.6.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.).
1.7. Контроль информации на съёмных носителях производится непосредственно перед её использованием.
1.8. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.
1.9. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
1.10. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2.Мероприятия, выполняемые для осуществления антивирусной защиты
2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.
2.2. Регулярное обновление программного обеспечения (далее – ПО) и систематические профилактические проверкиПО.
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)школы.
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 о того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.
2.5.Внешние носители информации неизвестного происхождения должны проверяться 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 работыкомпьютерного оборудования школыдля случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по организации антивирусной защиты
3.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и сервера 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:

- непосредственно после установки (изменения) ПОкомпьютера (локальной сети) должна быть выполнена антивирусная проверка на сервере и персональных компьютерахшколы;

- 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.

4. Порядок действий по организации антивирусной защиты при обнаружении вредоносного ПО

4.1.В случае обнаружения вредоносного ПОпользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты школы;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- 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 работников школы

5.1.Ответственность за организацию антивирусной защиты и мероприятия антивирусного контроля возлагается на лицо, назначенное приказом директорашколы.

5.2.Ответственность за соблюдение требований настоящегоположения при работе с ПК возлагается на ответственных, назначенных приказом директора Школы.

5.3.Периодический контроль состояния антивирусной защиты ПК вшколеосуществляется ответственным за информатизацию лицом и фиксируется актом проверки (не реже 1 раз в квартал).