ПРИНЯТО
на заседании педагогического совета
МАОУ «СШ «Успех»
протокол от «___» _____ 201__г.
секретарь Педагогического совета
_____ /_____

УТВЕРЖДЕНО
приказом директора
МАОУ «СШ «Успех»
_____ Т.В. Худякова
приказ № _____
от «___» _____201__г.

ПОЛОЖЕНИЕ
по организации антивирусной защиты в МАОУ «СШ «Успех»

1. Общие положения

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы МАОУ «СШ «Успех» 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 МАОУ «СШ «Успех» к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты МАОУ «СШ «Успех» являются:

1.1. Решение задачи антивирусной защиты должно осуществляться в общем виде.

1.2. 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.

1.3. Решение задачи антивирусной защиты должно осуществляться в реальном времени.

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

- установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение;
- регулярное обновление и ежедневные профилактические проверки;
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы;
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными;

- внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

1.5. 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. В учреждении руководителем должно быть назначено лицо, ответственное за антивирусную защиту.

2.2. В Учреждении 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 (CD-ROM, DVD, flash-накопителях и т.п.).

2.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

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.).

3.4. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

3.5. 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;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

4. Ответственность

4.1. Ответственность за организацию антивирусной защиты возлагается на руководителя МАОУ «СШ «Успех» или лицо, им назначенное.

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