Утверждено:
Директор
МБОУ СОШ № 8 им.А.Демина
_____ И.П.Лысенко
приказ от «30» 03 2017 г.
№ 59

Положение
муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы № 8 им. Александра Демина ст.Чепигинской муниципального образования Брюховецкий район об антивирусном контроле

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности МБОУ СОШ №8 им.А.Демина в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами и устанавливает порядок проведения антивирусного контроля в МБОУ СОШ № 8 им.А.Демина (далее Организация).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Организации.

1.3. Требования настоящего Положения распространяются на всех работников, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети Организации) и должны применяться для всех средств вычислительной техники, эксплуатируемой в Организации.

1.4. Организационное обеспечение мероприятий антивирусного контроля и контроль за действиями пользователей возлагается на ответственное лицо по защите информации.

2. Основные термины, сокращения и определения

АС – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

Компьютерный вирус программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Зараженная программа - это программа, содержащая внедренную в нее программу-вирус.

3. Организация системы антивирусного контроля

3.1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС Организации.

3.2. Задачами антивирусной защиты являются:

- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС Организации.

3.3. Для проведения мероприятий по предотвращению вирусного заражения приказом по Организации назначается ответственный за антивирусный контроль. Ответственный за антивирусный контроль в своей работе руководствуются настоящим Положением, нормативными актами по защите информации, и другими документами.

3.4. К использованию в Организации допускаются только лицензионные антивирусные средства, централизованно закупленные отделом информационных технологий у разработчиков (поставщиков) указанных средств.

3.5. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных средств на компьютерах в Организации осуществляется электроником.

3.6. Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

3.7. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.

3.8. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

3.9. Мероприятия по антивирусной защите на компьютерах в Организации включают в себя:

- профилактика вирусного заражения;
- анализ ситуаций;
- применение средств антивирусной защиты;
- проведение расследований инцидентов связанных с вирусами.

4. Профилактика вирусного заражения

4.1. В целях исключения появления и распространения вирусов на рабочих станциях АС Организации должны регулярно проводиться

профилактические мероприятия. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов по расписанию;
- регулярная (не реже одного раза в квартал) выборочная проверка рабочих станций и серверов на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- проверка наличия вирусов на рабочих станциях, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- создание резервной копии программного продукта сразу же после приобретения;
- установка защиты от записи на съемные носители информации, где это возможно;
- тщательная проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

4.2. Создание резервной копии программного продукта выполняется отделом информационных технологий, остальные профилактические работы и мероприятия выполняются ответственным за антивирусный контроль в Организации.

4.3. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

5. Анализ ситуаций

5.1. При сообщении антивирусных программы о подозрении на наличие вирусов на рабочей станции, необходимо приостановить работу и немедленно известить об этом ответственного за антивирусный контроль Организации, начальника отдела по защите информации Организации, а также других пользователей и подразделения, использующие эти файлы в работе, если зараженные файлы являются совместно используемыми.

5.2. Анализ ситуации наличия вирусов выполняется ответственным за антивирусный контроль в Организации. При анализе могут дополнительно использоваться специальное программное обеспечение для обнаружения вирусов.

5.3. В ходе анализа ситуации обязательно требуется определить источник заражения. Если источником заражения является съемный носитель либо другая рабочая станция Организации, то необходимо проверить на наличие вирусов рабочую станцию - источник заражения. В случае заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.

5.4. В случае обнаружения вирусного заражения расследование допущенных нарушений производится отделом по защите информации на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Организации.

6. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется ответственным за антивирусный контроль в Организации.

6.2. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.

6.3. В случае обнаружения, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусный контроль должен направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.

7. Ответственность

7.1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых сотрудниками в соответствии с требованиями настоящего Положения, возлагается на ответственного за антивирусный контроль.

7.2. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники на рабочем месте в соответствии с требованиями настоящего Положения, возлагается на пользователя средств вычислительной техники.

7.3. Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в АС Организации, а также уничтожение выявленных вирусов возлагается на ответственного за антивирусный контроль Организации.

7.4. Периодический контроль за состоянием антивирусной защиты в АС Организации, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками Организации осуществляется ответственным по защите информации.

7.5. Сотрудники Организации, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.