Муниципальное бюджетное общеобразовательное учреждение
«Сосновская средняя общеобразовательная школа»

Школьный пер.., д. 7, с. Сосновка, район Шарканский, УР, 427077, тел. (34136) 3-12-32, ssosh2008@yandex.ru

СОГЛАСОВАНО
Решение Педагогического собрания
Протокол № 12 от 25.06.2024

УТВЕРЖДАЮ
Директор МБОУ «Сосновская СОШ»
_____ Е.С. Корепанова
Приказ от 27.06.2024 № 38/1-ОД.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ МЕР АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В МБОУ «СОСНОВСКАЯ СОШ»

I.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2. Настоящая инструкция определяет требования к организации защиты информационных систем ПДн от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИС, за их выполнение.

1.3. К использованию в МБОУ «Сосновская СОШ» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств или свободно-распространяемое программное обеспечение.

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

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, flashнакопителях и т.п.).

1.6. 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.

II.МЕРОПРИЯТИЯ, НАПРАВЛЕННЫЕ НА РЕШЕНИЕ ЗАДАЧ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

2. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль системных файлов.

2.2. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы.

2.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера.

2.4. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании заявки. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за организацию антивирусной защиты на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера на автоматизированном рабочем месте (АРМ) ответственным за организацию антивирусной защиты должна быть выполнена антивирусная проверка.

2.7. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в электронном журнале антивирусного средства (операционной системы).

2.8. 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.) сотрудник самостоятельно или вместе с ответственным за организацию антивирусной защиты должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

III.ДЕЙСТВИЯ СОТРУДНИКОВ ПРИ ОБНАРУЖЕНИИ КОМПЬЮТЕРНОГО ВИРУСА

3.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

3.2. Приостановить работу; немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в МБОУ «Сосновская СОШ»;

3.1.2. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

3.1.3. провести лечение или уничтожение зараженных файлов.

3.1.4. при возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

3.1.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отдельном съемном носители Администратору безопасности ИС;

3.1.6. по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИС, в которой необходимо указать предположительный источник (отправителя, владельца и т. д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

IV.ОТВЕСТВЕННОСТЬ

4.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором МБОУ «Сосновская СОШ».

4.2. Ответственность за проведение мероприятий антивирусного контроля в МБОУ «Сосновская СОШ» возлагается на ответственного за организацию антивирусной защиты.

4.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

4.4. Периодический контроль за состоянием антивирусной защиты в МБОУ «Сосновская СОШ» осуществляется директором школы и фиксируется Актом проверки (не реже 1 раз в квартал).

Лист ознакомления

с инструкцией по организации антивирусной защиты в информационных системах персональных данных

в МБОУ «Сосновская СОШ»

N п/п	Фамилия, имя, отчество	Дата	Занимаемая должность	Подпись
1	2	3	4	5