ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в информационных системах персональных данных муниципального автономного общеобразовательного учреждения «Гимназия №1 Октябрьского района г. Саратова»

1. 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 МАОУ «Гимназия №1» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИС, за их выполнение.

1.3 К использованию в муниципальном автономном общеобразовательном учреждении «Гимназия №1 Октябрьского района г. Саратова» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.4 Установка средств антивирусного контроля на компьютерах осуществляется системным Администратором МАОУ «Гимназия №1». Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля.

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

2.2 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (DVD (CD)-ROM, flash-накопители и т. п.).

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 педагогического работника. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором безопасности ИС на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера на автоматизированном рабочем месте (АРМ) Администратором безопасности ИС 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 Администратором безопасности ИС должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

2.9 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Администратора безопасности ИС, владельца зараженных файлов, а также других сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отдельном съемном носители Администратору безопасности ИС;
- 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.

3. Ответственность.

3.1 Ответственность за организацию антивирусного контроля в муниципальном автономном общеобразовательном учреждении «Гимназия №1 Октябрьского района г. Саратова» и соблюдение требований настоящей инструкции возлагается на Администратора безопасности ИС.

3.2 Периодический контроль над состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции сотрудниками МАОУ «Гимназия №1» осуществляется Администратором безопасности ИС.