Приложение №1
к приказу от 31.12.2019 г. № 104/07-од
«Об утверждении локальных актов»

УТВЕРЖДЕНО
приказом ГБОУ гимназии №1
г. Новокуйбышевска
от 31.12.2019 г. № 104/07-од

Директор
_____ **Л.Г. Слепцова**

Инструкция
по организации антивирусной защиты

1. Общие положения

1.1. Настоящая Инструкция по организации антивирусной защиты (далее - Инструкция) определяет требования к организации защиты АС в государственном бюджетном общеобразовательном учреждении Самарской области гимназии № 1 им. Н.И. Ферапонтова города Новокуйбышевска городского округа Новокуйбышевск Самарской области (далее – образовательная организация) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих АС, за их выполнение.

1.2. К использованию в образовательной организации допускаются лицензионные антивирусные средства, а также используются антивирусные средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, централизованно закупленные у разработчиков (поставщиков) указанных средств, и (или) рекомендованные к применению отделами автоматизации и безопасности информации.

1.3. В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо

согласовать с администратором ИС или ответственным за организацию обработки персональных данных.

1.4. Установка средств антивирусного контроля на компьютерах, сервере и рабочих станциях АС администратором ИС или ответственным за организацию обработки персональных данных, либо через привлечение на договорной основе сторонних организаций для таких работ.

1.5. Настройка параметров средств антивирусного контроля осуществляется администратором ИС или ответственным за организацию обработки персональных данных, либо сотрудниками, привлеченными на договорной основе сторонних организаций для таких работ.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для сервера - при перезапуске) в автоматическом режиме.

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 (магнитных дисках, лентах, CD - ROM 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 с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере.

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. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

2.7. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

3. Действия при обнаружении вирусов

3.1. 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 обработки персональных данных должен провести внеочередной антивирусный контроль своей рабочей станции.

При необходимости для таких работ на договорной основе привлечь специалистов сторонних организаций для определения ими факта наличия или отсутствия компьютерного вируса.

3.2. 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 (директора) и ответственного за организацию обработки персональных данных образовательной организации, а также других сотрудников, использующих эти файлы в работе;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске ответственному за организацию обработки персональных данных для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку руководителю (директору) образовательной организации, 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.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в образовательной организации в соответствии с требованиями настоящей Инструкции возлагается на руководителя (директора) образовательной организации.

4.2. Ответственность за проведение мероприятий антивирусного контроля в образовательной организации и соблюдение требований настоящей Инструкции возлагается на ответственного за организацию обработки персональных данных и всех сотрудников образовательной организации, являющихся пользователями АС.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками образовательной организации осуществляется администратором ИС или ответственным за организацию обработки персональных данных.