

УТВЕРЖДАЮ

Приказ № 205 от «15» 06 2018 г.

Директор школы-интерната № 1 им. К.К. Грота



А.В. Мухин

**Инструктаж по антивирусной защите информационной
системы персональных данных
Государственного бюджетного общеобразовательного учреждения
школы-интерната № 1 имени К. К. Грота Красногвардейского района
Санкт-Петербурга**

Санкт-Петербург
2018г.

1 Общие положения

- 1.1 Настоящая инструкция определяет правила и основные требования к организации защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов в ГБОУ Школы-интерната №1 им. К. К. Грота Красногвардейского района Санкт-Петербурга (далее – Школы-интерната) и устанавливает ответственность за их выполнение.
- 1.2 Компьютерный вирус – это вид вредоносного программного обеспечения (далее – ПО), способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов (удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п.).
- 1.3 Действие настоящей инструкции распространяется в полном объеме на Школу-интернат и обязательна для выполнения всеми сотрудниками.

2 Инструкция по применению средств антивирусной защиты

- 2.1 Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.
- 2.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.
- 2.3 Установка и настройка средств антивирусной защиты на автоматизированных рабочих местах (далее – АРМ) и серверах осуществляется сотрудниками школьной информационной сети.
- 2.4 Частота обновления баз данных средств антивирусной защиты, автоматическая проверка и лечения всех файлов должна проходить не реже 1 раза в неделю.
- 2.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
- 2.6 Средства антивирусной защиты устанавливаются на всех АРМ и серверах Школы-интерната.
- 2.7 Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.
- 2.8 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
- 2.9 Разархивирование и контроль входящей информации, поступающей по каналам электронной почты, осуществляется до передачи поступившей информации исполнителю. До проведения антивирусного контроля файлы запрещается копировать на сетевые диски и в архивы электронной почты. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой.
- 2.10 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль АРМ либо обратиться к сотрудникам, осуществляющим сетевое администрирование ИСПДн.
- 2.11 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
 - немедленно поставить в известность о факте обнаружения вируса сотрудников сетевого администрирования ИСПДн;
 - провести лечение зараженных файлов;
 - в случае невозможности лечения обратиться к сотрудникам, осуществляющие сетевое администрирование ИСПДн;
 - не начинать работу до устранения причины заражения вирусом и выполнения антивирусных мероприятий;
- 2.12 По факту обнаружения зараженных вирусом файлов сотрудник сетевого администрирования ИСПДн должен установить причины заражения вирусом и принять соответствующие меры по предотвращению подобных ситуаций.
- 2.13 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
- 2.14 Пользователи должны быть ознакомлены с данной инструкцией под роспись.
- 2.15 Проводить периодическое тестирование функций средств антивирусной защиты.
- 2.16 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

3. Пользователю запрещается:

- вмешиваться в работу системы антивирусной защиты;
- отключать, выгружать или деинсталлировать средства антивирусной защиты на АРМ;
- установка ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;

4. Ответственность

- 4.1 Ответственность за организацию антивирусного контроля в Школе-интернате возлагается на сотрудников сетевого администрирования.
- 4.3 За невыполнение требований настоящей инструкции несут ответственность пользователи ИСПДн.