

Инструкция
по проведению антивирусного контроля в информационной системе
персональных данных Муниципального учреждения дополнительного образования
«Центр развития творчества детей и юношества им. И.А.Панкова»

1. Общие положения

1.1 Настоящая инструкция определяет требования к организации обеспечения безопасности персональных данных в информационной системе персональных данных (далее – ИСПДн) МУДО «ЦРТДиЮ им.И.А.Панкова» (далее – Учреждение) от воздействия компьютерных вирусов и другого вредоносного программного обеспечения и устанавливает ответственность сотрудников Учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2 В целях обеспечения антивирусной защиты в ИСПДн производится антивирусный контроль.

1.3 Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации ИСПДн.

1.4 К применению в ИСПДн допускаются сертифицированные антивирусные средства.

1.5 В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

1.6 Пользователи ИСПДн при работе со съемными носителями информации (USB флеш-накопителями) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

1.7 Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

1.8 Установка и настройка средств антивирусного контроля осуществляется администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

1.9 Администратор безопасности информации ИСПДн осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

1.10 Администратор безопасности информации ИСПДн проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

1.11 При обнаружении компьютерного вируса пользователь ИСПДн обязан немедленно поставить в известность администратора безопасности информации ИСПДн и прекратить какие-либо действия в ИСПДн.

1.12 Администратор безопасности информации ИСПДн проводит, в случае необходимости, «лечение зараженных» файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

1.13 В случае обнаружения на съемных носителях информации нового вируса, «не поддающегося лечению», администратор безопасности информации ИСПДн обязан запретить использование данного съемного носителя информации.

1.14 В случае обнаружения вируса, «не поддающегося лечению», администратор безопасности информации ИСПДн обязан поставить в известность ответственного за обеспечение безопасности персональных данных в ИСПДн, запретить работу в ИСПДн и в возможно короткие сроки обновить пакет антивирусных программ.

1.15 Доведение Инструкции до сотрудников ГБОУ ДПО ТОИУУ в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией.

С.В. Попова