Приложение №8

к приказу \_№26/1 от 01.09.2018г.

**Инструкция**

**по проведению антивирусного контроля в информационной системе персональных данных Муниципального дошкольного образовательного учреждения детский сад №1п.Рамешки**

1. **Общие положения**
2. Настоящая инструкция определяет требования к организации обеспечения безопасности персональных данных в информационной системе персональных данных (далее – ИСПДн) Муниципального дошкольного образовательного учреждения детский сад №1 (далее – Учреждение) от воздействия компьютерных вирусов и другого вредоносного программного обеспечения и устанавливает ответственность сотрудников Учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.
3. В целях обеспечения антивирусной защиты в ИСПДн производится антивирусный контроль.
4. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации ИСПДн.
5. К применению в ИСПДн допускаются сертифицированные антивирусные средства.
6. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.
7. Пользователи ИСПДн при работе со съемными носителями информации (USB флеш-накопителями) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
8. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.
9. Установка и настройка средств антивирусного контроля осуществляется администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.
10. Администратор безопасности информации ИСПДн осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.
11. Администратор безопасности информации ИСПДн проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.
12. При обнаружении компьютерного вируса пользователь ИСПДн обязан немедленно поставить в известность администратора безопасности информации ИСПДн и прекратить какие-либо действия в ИСПДн.
13. 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.
14. В случае обнаружения на съемных носителях информации нового вируса, «не поддающегося лечению», администратор безопасности информации ИСПДн обязан запретить использование данного съемного носителя информации.
15. 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.
16. Доведение Инструкции до сотрудников Учреждения в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией.