

УТВЕРЖДАЮ

Директор муниципального  
учреждения дополнительного  
образования Детская школа искусств

им. Г.Ф. Пономаренко  
муниципального образования  
город Краснодар

В.А. Ковалева



« 25 октября 2018 г.

### Инструкция по антивирусной защите

1. Инструкция по антивирусной защите (далее – Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимой в работе ДШИ им. Г.Ф. Пономаренко (далее – Школа).

2. Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

3. Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных электронных носителей и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов.

4. К использованию допускаются только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств, а их установка и техническая поддержка производятся уполномоченным сотрудником Школы.

5. Периодически, не реже 1 раза в неделю, работник Школы, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

6. Пользователь (в случае необходимости совместно с уполномоченным сотрудником Школы) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на

съемных носителях (магнитных дисках, оптических носителях, Flash — память и т.п.).

7. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения. Полная проверка информации хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.

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.) работник Школы самостоятельно или вместе с уполномоченным сотрудником Школы должен провести внеочередной антивирусный контроль своей рабочей станции.

9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники Школы обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту Организации, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

10. Ответственность за организацию антивирусного контроля Школы, в соответствии с требованиями настоящей Инструкции возлагается на заместителя директора по информационным технологиям.

11. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту Школы и всех сотрудников, являющихся пользователями ПК Школы.