ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ТУЛЬСКОЙ ОБЛАСТИ «ТУЛЬСКАЯ ШКОЛА» (ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»)

Приложение № 2 к приказу
от 30.08.2024 № 79-осн

ПРИНЯТО на заседании
общего собрания работников
ГОУ ТО «Тульская школа»
протокол от 26.08.2024 № 1

УТВЕРЖДЕНО
приказом ГОУ ТО «Тульская школа»
от 30.08.2024 № 79-осн

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ СРЕДСТВ ИНФОРМАТИЗАЦИИ В ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»

г. Тула

1. Общие положения

1.1. Настоящее положение об организации антивирусной защиты средств информатизации государственного общеобразовательного учреждения Тульской области «Тульская школа» (далее – Положение и Учреждение соответственно) определяет требования к организации защиты средств информатизации от деструктивного воздействия вредоносного программного обеспечения, включая компьютерные вирусы, порядок организации работ по антивирусной защите средств информатизации в Учреждении, устанавливает ответственность руководителей и работников структурных подразделений.

1.2. Положение разработаю с учетом следующих документов:

- Федерального закона от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической

информационной инфраструктуры Российской Федерации»;

- Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»;
- Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении

перечня сведений конфиденциального характера»;

- приказа Федеральной службы по техническому и экспортному контролю от 11.02.2017 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказа Федеральной службы по техническому и экспортному контролю от 25.12.2017 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- Государственного стандарта Российской Федерации ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 14.07.1998 № 295);
- Методического документа Федеральной службы по техническому и экспортному контролю от 11.02.2014 «Меры защиты информации в государственных информационных системах»;

- Методического документа Федеральной службы по техническому и экспортному контролю от 05.02.2021 «Методика оценки угроз безопасности информации».

- Типовой инструкции по организации антивирусной защиты средств информатизации в образовательных учреждениях, утвержденной приказом Министерства образования Тульской области от 01.08.2008 № 1333.

1.3. 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.).

1.4. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, используемых в Учреждении.

1.5. К использованию в Учреждении допускается только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства Российской Федерации.

1.6. Директором Учреждения назначается лицо ответственное за антивирусную защиту средств информатизации.

1.7. Ответственный за антивирусную защиту средств информатизации Учреждения имеет право на стимулирующие выплаты из фонда стимулирования педагогических и руководящих работников Учреждения за выполнение функций, определенных настоящим Положением.

2. Используемые в положении термины и определения

2.1. Вредоносное программное обеспечение (ВПО) - любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа или нейтрализации средств защиты информации.

Компьютерный вирус - вид вредоносного программного обеспечения, способного создавать свои копии и внедрять их в загрузочные секторы носителей, системные области памяти, код других программ и распространяться с использованием различных каналов связи. Сопутствующей функцией вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей.

Средства вычислительной техники (СВТ) - автоматизированные рабочие места, серверы, периметральные средства защиты информации (средства межсетевого экранирования, прокси-серверы, почтовые шлюзы и другие средства, используемые для защиты информации), мобильные технические средства и иные точки доступа в информационные системы,

подверженные заражению вредоносным программным обеспечением со съемных машинных носителей информации или через сетевые подключения.

3. Порядок установки настройки антивирусного программного обеспечения

3.1. Антивирусная защита средств информатизации Учреждения осуществляется посредством специального антивирусного программного обеспечения.

3.2. Установка и настройка средств антивирусного программного обеспечения осуществляются в соответствии с эксплуатационной документацией, поставляемой в комплекте с ним.

3.3. Установка, настройка и регулярное обновление антивирусного программного обеспечения осуществляется только ответственным за антивирусную защиту средств информатизации Учреждения.

3.4. Антивирусное программное обеспечение настраивается таким образом, чтобы обеспечить следующие условия:

- обязательный входной контроль на наличие программных вирусов во всех поступающих электронных носителях информации в автоматическом режиме;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов в автоматическом режиме;

- блокирование сетевых атак из сети Интернет в автоматическом режиме.

4. Требования к проведению мероприятий по антивирусной защите средств информатизации Учреждения

4.1. Ответственный за антивирусную защиту средств информатизации Учреждения раз в год проводит инструктаж по работе с антивирусными программным обеспечением.

4.2. Ответственный за антивирусную защиту средств информатизации Учреждения ведет журнал инструктажа по работе с антивирусными программным обеспечением.

4.3. Пользователям, работающим со средствами информатизации Учреждения, запрещается отключать средства антивирусной защиты информации во время работы;

4.4. Устанавливаемое (изменяемое) программное обеспечение на персональные компьютеры Учреждения должно быть предварительно проверено на отсутствие вирусов.

4.5. Проведение мероприятий по антивирусной защите средств информатизации Учреждения должно включать следующее:

- ежедневно в начале работы при загрузке компьютера в автоматическом режиме выполнять обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера;

- периодическая проверка в автоматическом режиме на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц);

- обязательная проверка съемных носителей информации перед началом работы с ними;

- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

4.6. Плановые проверки средств информатизации Учреждения должны проводиться не реже одного раза в месяц.

4.7. 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), необходимо провести внеплановую проверку средств информатизации Учреждения (жестких магнитных дисков и съемных носителей информации) на наличие программных вирусов.

4.8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- провести лечение или уничтожение зараженных файлов и поставить в известность ответственного за антивирусную защиту средств информатизации Учреждения;

- в случае, ели не удается удалить вирус, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за антивирусную защиту средств информатизации Учреждения;

- ответственный за антивирусную защиту средств информатизации Учреждения совместно с пользователем зараженных вирусом файлов должен определить необходимость дальнейшего их использования и провести лечение или уничтожение заражённых файлов.

5. Ответственность при организации антивирусной защиты

5.1. Ответственный за антивирусную защиту средств информатизации Учреждения несет персональную ответственность за невыполнение Положения.

5.2. Ответственность за организацию мероприятий по антивирусной защите в структурных подразделениях Учреждения в соответствии с требованиями настоящей Положения возлагается на руководителей структурных подразделений.

5.3. Контроль за соблюдением Положения ответственным за антивирусную защиту средств информатизации Учреждения, осуществляет директор Учреждения.