Приложение 11
к приказу МАУДО «ДПШ»
от 31.08.2020 № 276/1-од

Инструкция
по организации антивирусной защиты
информационной системы МАУДО «ДПШ»

I. Общие положения

1. Данная Инструкция определяет требования к организации защиты информационной системы (далее – ИС) Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г.Челябинска» (далее – МАУДО «ДПШ») от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и других должностных лиц, за выполнение указанных требований.

II. Термины и определения

2. **Антивирусная база** – это база, которая содержит уникальные данные о каждом конкретном вирусе.

Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного программного обеспечения при помощи антивирусных программных продуктов.

Средство антивирусной защиты – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

Носитель информации – любой материальный объект или среда, используемые для хранения или передачи информации.

Программное обеспечение (ПО) – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

III. Обязанности ответственного за обеспечение безопасности персональных данных в информационных системах

3. К использованию в МАУДО «ДПШ» допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

4. Установка средств антивирусного контроля на АРМ и серверах ИС МАУДО «ДПШ» осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

5. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

6. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

7. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех АРМ ИС, работающих в сети, не реже 1 (одного) раза в неделю для всех АРМ ИС, работающих автономно.

8. Устанавливаемое (изменяемое) ПО должно быть предварительно проверено ответственным за обеспечение безопасности персональных данных в информационных системах на предмет отсутствия вредоносного ПО.

9. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

10. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС МАУДО «ДПШ»

осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС МАУДО «ДПШ».

IV. Обязанности пользователя ИС

11. При возникновении подозрения на наличие вредоносного ПО (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с ответственным за обеспечение безопасности персональных данных в информационных системах провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение безопасности персональных данных в информационных системах для определения им факта наличия или отсутствия вредоносного ПО.

12. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного ПО:

1) приостановить обработку данных;

2) немедленно поставить в известность о факте обнаружения вредоносного ПО ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3) совместно с владельцем файлов, заражённых вредоносным ПО, провести анализ необходимости дальнейшего их использования;

4) произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности персональных данных в информационных системах).

V. Ответственность

13. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

14. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

15. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.14 Кодекса об административных правонарушениях РФ.

16. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.