



ИНСТРУКЦИЯ по организации антивирусной защиты

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция определяет требования к организации защиты информационной системы (далее – ИС) Муниципального бюджетного образовательного учреждения дополнительного образования «Образовательный технический центр» (далее – МБОУДО «ОТЦ») от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности информации и других должностных лиц, за выполнение указанных требований.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

2.4. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, multifunctional devices, scanners and etc.

2.5. **Информация** – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

2.6. **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.

2.7. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации

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

2.9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. К использованию в МБОУДО «ОТЦ» допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

3.2. Установка средств антивирусного контроля на автоматизированных рабочих местах (далее – АРМ) и серверах ИС МБОУДО «ОТЦ» осуществляется ответственным за обеспечение безопасности информации 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.

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

3.4. 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.

3.5. 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.

3.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за обеспечение безопасности информации на предмет отсутствия вредоносного программного обеспечения (далее – ПО).

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

3.8. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС МБОУДО «ОТЦ», осуществляется ответственным за обеспечение безопасности информации, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС МБОУДО «ОТЦ».

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. При возникновении подозрения на наличие вредоносного программного обеспечения (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 информации провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение

безопасности информации для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

4.2.1. приостановить обработку данных;

4.2.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

4.2.3. совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

4.2.4. произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности информации).

V. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС И ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Администратор и пользователи ИС 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.

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

5.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), 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) МБОУДО «ОТЦ», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник МБОУДО «ОТЦ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МБОУДО «ОТЦ» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

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

5.4. 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.