УТВЕРЖДЕНО
приказом директора МАУ ДО
«Детско-юношеский центр»
№ 23 от 14 января 2019 года

Инструкция
по организации антивирусной защиты в муниципальном автономном учреждении дополнительного образования «Детско-юношеский центр»

1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет требования к организации защиты информационной системы (далее – информационная система; ИС) Муниципального автономного учреждения дополнительного образования «Детско-юношеский центр» (далее – Организация) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности информации (далее – АБИ) и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИС, за выполнение указанных требований.

1.2. К использованию в Организации допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на автоматизированные рабочие места (далее – АРМ) и сервера ИС Организации осуществляется АБИ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК России в области защиты информации.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов АРМ.

2.2. 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 ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в 3 месяца.

2.4. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИС, работающих в сети, не реже одного раза в неделю для всех АРМ ИС, работающих автономно.

2.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБИ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверов и АРМ ИС.

2.6. 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 АБИ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля – уведомить о результатах АБИ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

2.7. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
– провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь АБИ).

3. Ответственность

3.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИС Организации в соответствии с требованиями настоящей Инструкции возлагается на АБИ и всех должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИС Организации.

3.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а так же проверка работоспособности средств антивирусной защиты) в ИС Организации, осуществляется АБИ и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС Организации.