


Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад №22 «Журавлик» города Сафоново Смоленской области
(МБДОУ д/с №22)

**УТВЕРЖДАЮ:**
Заведующий МБДОУ д/с №22
С.В. Зыбина
Приказ № 109
от « 26 » сентября 2023 г.

ИНСТРУКЦИЯ
по организации антивирусной защиты
информационных систем персональных данных
в муниципальном бюджетном дошкольном
образовательном учреждении
«Детский сад №22 «Журавлик»
города Сафоново Смоленской области
(МБДОУ д/с №22)

1. Общие положения

1.1. Настоящая Инструкция разработана 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 Российской Федерации 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 персональных данных (ИСПД) муниципального бюджетного дошкольного образовательного учреждения «Детский сад №22 «Журавлик» города Сафоново Смоленской области (далее - МБДОУ) 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 ИСПД, за выполнение указанных требований.

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

1.3. Установка средств антивирусного контроля на компьютеры и сервера ИСПД МБДОУ осуществляется АБИ, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

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 иницироваться антивирусная проверка этих архивов.

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

2.4. 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 серверах и АРМ ИСПД.

2.5. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажение 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.

2.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС ДОУ обязаны:

- ✚ приостановить работу;
- ✚ немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора информационной безопасности, 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;
- ✚ в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору информационной безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);
- ✚ по факту обнаружения зараженных вирусом файлов составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

3.1. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя организации.

3.2. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПД МБДОУ в соответствии с требованиями настоящей Инструкции возлагается на ответственного за антивирусную защиту и всех должностных лиц, сопровождающих средства антивирусной защиты в ИСПД МБДОУ.

3.3. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПД МБДОУ, осуществляется ответственным за антивирусную защиту организации.

