Приложение № 2
к приказу № 78/2-ОД от 16.08.2021г

Инструкция
по организации антивирусной защиты в информационной системе МБДОУ «Ерёминский детский сад»

1. Общие требования

1.1. Настоящая Инструкция по организации антивирусной защиты в информационной системе МБДОУ «Ерёминский детский сад» (далее – Инструкция) определяет требования к организации защиты в информационной системе МБДОУ «Ерёминский детский сад» (далее – ИС) от разрушающего воздействия вредоносных компьютерных программ (компьютерных вирусов) и устанавливает ответственность сотрудников МБДОУ «Ерёминский детский сад», эксплуатирующих и сопровождающих ИС, за нарушение требований.

1.2. К использованию в ИС допускаются только средства антивирусной защиты, прошедшие в установленном порядке процедуру оценки соответствия.

1.3. Установка и настройка средств антивирусной защиты осуществляется специально назначенным лицом (администратором безопасности ИС), в соответствии с руководствами по применению конкретных средств антивирусной защиты.

2. Применение средств антивирусной защиты

2.1. Порядок применения средств антивирусной защиты устанавливается с учетом соблюдения следующих требований:

– проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке;

– обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;

– обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;

– периодическая проверка на предмет отсутствия программных вирусов машинных носителей информации, встроенных в корпус средств вычислительной техники (не реже одного раза в неделю), и обязательная проверка съемных носителей информации перед началом работы с ними;

– внеплановая проверка машинных носителей информации, встроенных в корпус средств вычислительной техники, и съемных носителей информации в случае подозрения на наличие программных вирусов;

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

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка на всех компьютерах, на которых произошло изменение состава программного обеспечения.

2.5. 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 и т.п.)

сотрудник подразделения самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

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

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИС;

– провести анализ необходимости дальнейшего использования зараженных файлов;

– провести лечение или уничтожение зараженных файлов.

2.6. Обновление баз данных, необходимых для реализации функций безопасности средства защиты информации (обновление баз сигнатур вирусов средств антивирусной защиты) выполняется ежедневно в автоматическом режиме со специальных серверов обновления производителей средств защиты информации.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС, на период его отсутствия – на системного администратора ИС.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на администратора безопасности ИС и всех сотрудников, являющихся пользователями ИС.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором безопасности ИС.

3.4. Ответственность за своевременное обновление антивирусных баз возлагается на администратора безопасности ИС.

Разработчик инструкции: заведующий
МБДОУ «Ерёминский детский сад» Лукошенко Л.В. _____

Лист ознакомления с инструкцией
по организации антивирусной защиты в информационной системе
МБДОУ «Ерёминский детский сад»

№ п/п	Ф.И.О. работника	Дата ознакомления	Личная подпись