«УТВЕРЖДАЮ»
Заведующий МАДОУ детский сад №9 «Сказка»
Коровкина Наталья Геннадьевна Н.Г.Коровкина
Приказ от 25.09.2017г. № 244

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных МАДОУ детский сад №9 «Сказка»

Топки 2017

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных систем персональных данных (далее – информационные системы) МАДОУ детский сад №9 «Сказка» (далее – Учреждение) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих указанные информационные системы, за их выполнение.

1.2. В информационных системах используется средство антивирусной защиты «ESET Endpoint Security».

1.3. Установка и настройка параметров антивирусной защиты осуществляется администратором безопасности информационных систем (далее – администратор безопасности) в соответствии с руководствами по применению соответствующего антивирусного средства.

1.4. Администратору безопасности необходимо иметь в наличии резервные копии операционных систем для возможности быстрого восстановления работоспособности информационных систем в случае воздействия опасного вируса.

2. Применение средств антивирусного контроля

2.1. Обновления антивирусной базы антивирусных средств осуществляются в автоматическом режиме через информационно-телекоммуникационную сеть «Интернет». Для информационных систем, не подключенных к сети «Интернет», обновления антивирусной базы осуществляет администратор безопасности с периодичностью в одну неделю.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивированная информация) на съемных носителях информации: гибких магнитных дисках, оптических компакт-дисках и других носителях информации.

2.3. Контроль входящей и исходящей информации должен производиться в автоматическом режиме антивирусным средством, как в процессе работы пользователя, так и во время начальной загрузки операционной системы. Дополнительно, пользователь обязан проводить проверку (антивирусное сканирование) всех подключаемых съемных носителей.

2.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться в автоматическом режиме антивирусным средством не реже одного раза в месяц. Проведение проверок должно фиксироваться в журнале регистрации событий антивирусного средства.

2.5. Пакеты обновлений инсталлированного программного обеспечения должны быть предварительно проверены антивирусным средством на отсутствие вредоносного кода.

2.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь информационной системы самостоятельно или вместе с администратором безопасности должен провести полную антивирусную проверку.

2.7. 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 начальника отдела и/или администратора безопасности, владельца зараженных файлов (в случае использования съемного носителя информации);
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести «лечение» или «удаление» зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности);
- в случае обнаружения нового вируса, при невозможности «лечения», сохранить зараженный вирусом файл на съемный носитель информации и передать его администратору безопасности;
- в случае определения факта повреждения операционной системы после воздействия вредоносного кода, администратор безопасности должен восстановить операционную систему из резервной копии.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты информационных систем, в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на администратора безопасности и пользователей информационных систем.

Лист ознакомления работников с инструкцией по организации антивирусной защиты информационных систем персональных данных

№ п/п	Ф.И.О. работника	Должность работника	Дата ознакомления с инструкцией и получения копии инструкции	Личная подпись