Приложение 6
к приказу заведующего
от «01» 09 2016 г. № 130/10

Утверждаю
Заведующий МБДОУ
«ЦРР – д/с №34 «Рябинушка»
_____ А.В. Почернина
«__» _____ 2016г.

Инструкция

по антивирусной защите информационной системы

персональных данных

г-к. Геленджик, 2016

1 Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты информационной системы персональных данных (далее – ИСПДн), используемых в МБДОУ «ЦРР – д/с №34 «Рябинушка» (далее - ДОУ), и устанавливает ответственность за их выполнение.

Действие настоящей инструкции распространяется в полном объеме на ДОУ и обязательно для выполнения всеми сотрудниками.

2 Инструкция по применению средств антивирусной защиты

1.1 Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

1.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.

1.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за систему защиты информации (СЗИ) ИСПДн.

1.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

1.5 Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты.

1.6

1.7 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.

1.8 Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.

1.9 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ДОУ.

1.10 Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

1.11 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы) хранящаяся на АРМ, получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

1.12 Процедура обновления баз средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже 1 (Одного) раза в неделю для всех АРМ ИСПДн, работающих автономно;

1.13 Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.14 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

1.15 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором безопасности ИСПДн на предмет отсутствия вредоносного программного обеспечения;

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

1.17 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к ответственному за СЗИ ИСПДн.

1.18 При получении информации о возникновении вирусной эпидемии вне ДОУ должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

1.19 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса ответственного за СЗИ ИСПДн;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к сотруднику, ответственному за СЗИ ИСПДн;

1.20 По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен составить служебную записку, 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.

1.21 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

1.22 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

1.23 Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

1.24 Пользователи должны быть ознакомлены с данной инструкцией под подпись.

1.25 Проводить периодическое тестирование функций средств антивирусной защиты.

1.26 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Лист ознакомления
с Инструкцией по антивирусной защите информационной системы персональных данных

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника