Приложение №7

к Приказу № 35-од

от 21.08.2020 года

**Регламент антивирусной защиты**

**в МКДОУ «Детский сад комбинированного вида «Рябинушка»**

**I. Общие положения**

1. Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей МКДОУ «Детский сад комбинированного вида «Рябинушка» (далее МКДОУ) к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

2. Основополагающими требованиями к системе антивирусной защиты МКДОУ являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие только конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего неизвестно;

- решение задачи антивирусной защиты должно осуществляться в реальном времени.

3. Мероприятия, направленные на решение задач по антивирусной защите:

- установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения;

- регулярное обновление и еженедельные профилактические проверки;

- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;

- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;

- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;

- проведение регулярных проверок целостности критически важных программ и данных.

- наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано: внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

**II. Технологические инструкции**

1.Заведующий МКДОУ назначает лицо, ответственное за антивирусную защиту.

2. В МКДОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (CDROM, DVD, flash-накопителях и т.п.).

4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

**III. Требования к проведению мероприятий по антивирусной защите**

1.В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей - ежедневно, в ночное время по расписанию.

3.Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

4.Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах.

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.).

6.При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

**7.** В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

- Приостановить работу.

- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия - заведующего) МКДОУ.

- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

- Провести лечение или уничтожение зараженных файлов.

**IV.** **Ответственность**

1. Ответственность за организацию антивирусной защиты возлагается на заведующего МКДОУ или лицо, им назначенное.

2. Ответственность за проведение мероприятий антивирусного контроля в МКДОУ возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на педагога, владеющего необходимыми знаниями и умениями.

3. Периодический контроль состояния антивирусной защиты в МКДОУ по вопросам регламентации доступа к информации в сети Интернет два раза в год (ноябрь, апрель) и фиксируется в Журнале проверок антивирусной защиты в МКДОУ.