Принята
на заседании педагогического совета МБДОУ детского сада «Радуга»
протокол от 28.09.2019 г. № 2

Утверждена
приказом заведующего МБДОУ детского сада «Радуга»
от 30.09.19 г. № 102
_____ С.Ю. Румянцева

ИНСТРУКЦИЯ
по организации антивирусной защиты в Муниципальном бюджетном дошкольном образовательном учреждения детский сад «Радуга» Уренского муниципального района Нижегородской области.

1. Общие положения

1.1.Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в МБДОУ детский сад «Радуга» Уренского муниципального района Нижегородской области (далее - ДОУ) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей ДОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2.В ДОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3.Установка, настройка и регулярное обновление антивирусных средств осуществляется персональными пользователями, закреплёнными за компьютерной техникой.

1.4. 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 (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.).

1.5.Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.6.Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.7.Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

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

2.1. Установка только лицензированного программного обеспечения либо бесплатного
антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы (далее ИКС) ДОУ.

2.4. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

5.6. Обеспечение бесперебойной работы ДОУ для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

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

3.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на персональных компьютерах ДОУ;

3.3.2. 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.);

3.3.3. При отправке и получении электронной почты необходимо проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ДОУ;

4.1.3. провести анализ необходимости дальнейшего их использования;

4.1.4. провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное заведующим ДОУ.

5.2. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных компьютерах возлагается на педагога, отвечающего за работу компьютера.

5.3. Периодический контроль за состоянием антивирусной защиты в ДОУ осуществляется заведующим ДОУ (не реже 1 раза в квартал).