

Принято

на заседании педагогического
совета МБДОУ детского сада
«Радуга»
протокол от 27.09.2019 г. № 2

Утверждено

приказом заведующего
МБДОУ детского сада «Радуга»
от 30.09.19 г. № 101

С.Ю. Румянцева



Положение

об антивирусном контроле Муниципального бюджетного дошкольного
образовательного учреждения детский сад «Радуга»
Уренского муниципального района Нижегородской области.

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности МБДОУ детский сад «Радуга» Уренского муниципального района Нижегородской области в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами и устанавливает порядок проведения антивирусного контроля в МБДОУ детский сад «Радуга» Уренского муниципального района Нижегородской области (далее Организация).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Организации.

1.3. Требования настоящего Положения распространяются на всех работников организации и должны применяться для всех средств компьютерной техники, эксплуатируемой в Организации.

1.4. Организационное обеспечение мероприятий антивирусного контроля и контроль за действиями пользователей возлагается на ответственного за антивирусный контроль заведующего МБДОУ детский сад «Радуга» Уренского муниципального района Нижегородской области.

2. Основные термины, сокращения и определения

АС – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

Компьютерный вирус программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без

Компьютерный вирус программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Зараженная программа - это программа, содержащая внедренную в нее программу-вирус.

3. Организация системы антивирусного контроля

3.1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС Организации.

3.2. Задачами антивирусной защиты являются:

- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС Организации.

3.3. Ответственный за антивирусный контроль Организации в своей работе руководствуется настоящим Положением, нормативными актами по защите информации, и другими документами.

3.4. К использованию в Организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению.

3.5. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных средств на компьютерах в Организации осуществляется ответственным за антивирусный контроль.

3.6. Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

3.7. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.

3.8. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические

проверки электронных архивов должны проводиться не реже одного раза в месяц.

3.9. Мероприятия по антивирусной защите на компьютерах в Организации включают в себя:

- профилактика вирусного заражения;
- применение средств антивирусной защиты;
- анализ ситуаций;
- проведение расследований инцидентов связанных с вирусами.

1. Профилактика вирусного заражения

4.1. В целях исключения появления и распространения вирусов на рабочих станциях АС Организации должны регулярно проводится профилактические мероприятия. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов по расписанию;
- регулярная (не реже одного раза в квартал) выборочная проверка рабочих станций и серверов на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- создание резервной копии программного продукта сразу же после приобретения;
- проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

1.2. Создание резервной копии программного продукта выполняется ответственным за антивирусный контроль, остальные профилактические работы и мероприятия выполняются ответственными за компьютерную технику в Организации.

2. Анализ ситуаций

5.1. При сообщении антивирусных программы о подозрении на наличие вирусов на рабочей станции, необходимо приостановить работу и немедленно известить об этом ответственного за антивирусный контроль Организации, а также других пользователей, если зараженные файлы являются совместно используемыми.

5.2. В ходе анализа ситуации обязательно требуется определить источник заражения. Если источником заражения является съемный носитель либо другая рабочая станция Организации, то необходимо проверить на наличие вирусов рабочую станцию - источник заражения. В случае заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.

3. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется ответственным за антивирусный контроль в Организации.

3.2. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.

3.3. В случае обнаружения, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусный контроль должен направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.

4. Ответственность

7.1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах техники на рабочем месте возлагается на пользователя компьютерной техники.

Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в АС Организации, а также уничтожение выявленных вирусов возлагается на пользователя компьютерной техники.

4.2. Периодический контроль за состоянием антивирусной защиты в АС Организации, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками Организации осуществляется заведующим МБДОУ.

4.3. Сотрудники Организации, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

