



«СОГЛАСОВАНО»  
Председатель Совета Учреждения  
МАДОУ «ДС №13 «Родничок»  
 /А.Р.Трегубова/

«УТВЕРЖДАЮ»  
Заведующий МАДОУ «ДС №13 «Родничок»  
 /О.В.Любченко/  
Приказ от «03» февраля 2020 №32-О



«СОГЛАСОВАНО»  
Председатель Профсоюзного комитета  
МАДОУ «ДС №13 «Родничок»  
 /Я.А.Каширина/

## Инструкция о применении средств антивирусной защиты в Муниципальном автономном дошкольном образовательном учреждении детский сад № 13 «Родничок»

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 Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

**Основными требованиями к системе антивирусной защиты Учреждения являются:**

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие 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 не известно;

- решение задачи антивирусной защиты должно осуществляться в реальном времени.

**Мероприятия, направленные на решение задач по антивирусной защите:**

- установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой (типа Microsoft Security Essentials (сеть до 10 рабочих станций) или Microsoft Forefront Endpoint Protection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями.

- регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);

- 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;
- следует иметь планы обеспечения бесперебойной работы Учреждения для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

### **1. Технологические инструкции:**

1.1. В учреждении руководителем должно быть назначено лицо, ответственное за антивирусную защиту, в должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя Учреждения.

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

1.3. 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 (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

### **2. Требования к проведению мероприятий по антивирусной защите**

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

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

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

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

2.3.2. 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.).

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

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

2.4.1. Приостановить работу.

2.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты ( в случае его отсутствия – директора) Учреждения.

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

2.4.4. Провести лечение или уничтожение зараженных файлов.

### **3. Ответственность**

3.1. Ответственность за организацию антивирусной защиты возлагается на руководителя Учреждения или лицо, им назначенное.

3.2. Ответственность за проведение мероприятий антивирусного контроля в Учреждении возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.