Государственное бюджетное дошкольное образовательное учреждение детский сад № 19 комбинированного вида Центрального района Санкт-Петербурга

УТВЕРЖДАЮ
Заведующий ГБДОУ
детский сад №19
Центрального района СПб.
_____Е.Е. Суханова
Приказ № 59/1 от 30.08.2019 г.

ИНСТРУКЦИЯ
пользователям автоматизированных систем Государственного бюджетного дошкольного образовательного учреждения детский сад № 19 комбинированного вида Центрального Санкт-Петербурга по организации антивирусной защиты

Санкт-Петербург
2019 год

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты автоматизированных систем (АС) Государственного бюджетного дошкольного учреждения детский сад №19 комбинированного вида Центрального района Санкт-Петербурга (далее ГБДОУ) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС Предприятия, за их выполнение.

К использованию в ГБДОУ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и рекомендованные к применению специалистами отдела защиты информации.

Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на рабочих станциях (ПЭВМ), серверах ЛВС ГБДОУ осуществляется *ответственным за работу сети Интернет ограничения доступа к интернет-ресурсам* или системным администратором в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

Ежедневно в начале работы при загрузке средств вычислительной техники (ПЭВМ) (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенной автономной ПЭВМ, или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться **не реже одного раза в месяц**.

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.) сотрудник подразделения самостоятельно или совместно с *ответственным за работу сети Интернет ограничения доступа к интернет-ресурсам* или системного администратора должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Организации обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, специалистов отдела защиты информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести «лечение» или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела защиты информации);

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл в специальную карантинную зону, на специально выделенном для этого каталоге (при необходимости для выполнения требований данного пункта привлечь специалистов отдела защиты информации);
- все факты обнаружения зараженных вирусом файлов записываются в служебный журнал, где отображается тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за организацию антивирусного контроля в центральном аппарате Организации, возлагается на *ответственным за работу сети Интернет ограничения доступа к интернет-ресурсам.*

Ответственность за проведение мероприятий антивирусного контроля непосредственно в подразделении и соблюдение требований настоящей Инструкции возлагается на руководителя подразделения и всех сотрудников подразделения, являющихся пользователями автоматизированных систем.

Периодический контроль за состоянием антивирусной защиты в автоматизированной системе Организации, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений ГБДОУ осуществляется *ответственным за работу сети Интернет ограничения доступа к интернет-ресурсам.*