

## УТВЕРЖДАЮ

Заведующий МБДОУ д/с №11  
«Радость»  
*САНКТ-ПЕТЕРБУРГСКИЙ КРАЙ, Г.Санкт-Петербург*

В.чернецова  
2016 года

2016 года

16

~~401107~~

## ных систем

## СТЬ»

## **ИНСТРУКЦИЯ**

по организации антивирусной защиты информационных систем  
персональных МБДОУ детский сад №11 «Радость»

## **1 Общие положения**

1.1 Настоящая Инструкция определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих информационные системы персональных данных, за их выполнение.

1.2 К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению администратором информационной безопасности (далее – ИБ).

1.3 В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с ответственным за информационную безопасность.

1.4 Установка средств антивирусного контроля на АРМ и сервера ИСПДн осуществляется уполномоченными сотрудниками. Настройка параметров средств антивирусного контроля осуществляется администратором ИБ в соответствии с руководствами по применению конкретных антивирусных средств.

## **2 Применение средств антивирусного контроля**

2.1 Антивирусный контроль всех дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2 Периодически, не реже одного раза в месяц, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДН (сканирование).

2.3 Обязательному антивирусному контролю подлежит любая

информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2.5 В случае установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ИСПДн лицом, установившим (изменившим) программное обеспечение, под контролем администратора ИБ.

2.6 Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подпись лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

### **3 Действия сотрудников при подозрении наличия компьютерного вируса**

3.1 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 вместе с администратором ИБ должен провести внеочередной антивирусный контроль АРМ или серверов ИСПДн. При необходимости он должен привлечь администратора информационной безопасности для определения ими факта наличия или отсутствия компьютерного вируса.

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

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и администратора ИБ, 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 администратора информационной безопасности);

- в случае обнаружения нового вируса, не поддающегося лечению

применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске ответственному за информационную безопасность для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости для выполнения требований данного пункта привлечь администратора информационной безопасности);

- по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за информационную безопасность, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

#### **4 Порядок обновления антивирусных баз**

4.1 Обновление антивирусных баз должно проводиться регулярно с периодичностью определенной технологией работы в ИСПДн.

4.2 После согласования с ответственным за информационную безопасность ответственные за установку, модификацию и техническое обслуживание программного обеспечения обновляют антивирусные средства, проводят внеочередной антивирусный контроль и делают отметку в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ и серверов, выполнения профилактических работ, установки и модификации аппаратных и программных средств защищенных АРМ и серверов» о проделанных действиях.

#### **5 Ответственность**

5.1 Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем ИСПДн, в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения.

5.2 Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за ИСПДн и всех сотрудников подразделения, являющихся пользователями ИСПДн.

5.3 Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений осуществляется администратором ИБ.