Приложение \_\_\_

к приказу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. №\_\_\_\_\_\_\_

УТВЕРЖДАЮ

Директор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование

образовательного учреждения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО)

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

**Инструкция**

**по антивирусной защите информационной системы персональных данных**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(название ИСПДн)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

(город)

1. **Общие положения**

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты информационной системы персональных данных\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(далее –

(название ИСПДн)

ИСПДн, используемой в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование образовательного учреждения)

(далее - ОУ), и устанавливает ответственность за их выполнение.

Действие настоящей инструкции распространяется в полном объеме на ОУ и обязательно для выполнения всеми сотрудниками.

1. **Инструкция по применению средств антивирусной защиты**
   1. Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.
   2. К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.
   3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за систему защиты информации (СЗИ) ИСПДн.
   4. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
   5. Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
   6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.
   7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ОУ.
   8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.
   9. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
   10. Контроль входящей информации необходимо проводить непосредственно после ее приема.
   11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
   12. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
   13. 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к ответственному за СЗИ ИСПДн.
   14. При получении информации о возникновении вирусной эпидемии вне ОУ должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
   15. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения вируса ответственного за СЗИ ИСПДн;
* провести лечение зараженных файлов;
* в случае невозможности лечения обратиться к сотруднику, ответственному за СЗИ ИСПДн;
  1. По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен составить служебную записку, 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.
  2. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
  3. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
  4. Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
  5. Пользователи должны быть ознакомлены с данной инструкцией под подпись.
  6. Проводить периодическое тестирование функций средств антивирусной защиты.
  7. Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

**Лист ознакомления**

**с Инструкцией** **по антивирусной защите информационной системы персональных данных\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(название ИСПДн)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, имя, отчество работника** | **Дата ознакомления с Инструкцией** | **Подпись работника** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |