УТВЕРЖДЕНО  
приказом Росжелдора  
от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_

**Инструкция  
по организации антивирусной защиты  
в государственных информационных системах  
Федерального агентства железнодорожного транспорта**

1. **Общие положения**
   1. Инструкция по организации антивирусной защиты (далее – Инструкция) определяет требования к организации защиты государственных информационных систем в центральном аппарате Федерального агентства железнодорожного транспорта (Росжелдор) от разрушающего воздействия компьютерных вирусов.
   2. К использованию в Росжелдоре допускаются только сертифицированные лицензионные антивирусные средства.
   3. Установка и настройка средств антивирусного контроля и защиты на серверах и автоматизированных рабочих местах (далее – АРМ) государственных информационных систем осуществляется администратором информационной безопасности.
2. **Применение средств антивирусного контроля**
   1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться 1 раз в сутки в автоматическом режиме.
   2. 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 (магнитных дисках, лентах, CD - ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее получения. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
   3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
   4. Установка (изменение) системного и прикладного программного обеспечения осуществляется в соответствии с Перечнем разрешенного к использованию программного обеспечения.
   5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на защищаемых серверах и АРМах государственных информационных систем персональных данных администратором информационной безопасности.
3. **Действия при обнаружении вирусов**
   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.) государственный гражданский служащий Росжелдора вместе с администратором информационной безопасности должен провести внеочередной антивирусный контроль своего АРМа.
   2. В случае обнаружения при проведении антивирусной проверки файлов, зараженных компьютерными вирусами, необходимо:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов, владельца зараженных файлов, а также смежные отделы/управления, использующие эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* провести лечение или уничтожение зараженных файлов вместе администратором информационной безопасности.

1. **Ответственность**
   1. Ответственность за организацию антивирусного контроля и защиты в Росжелдоре, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.
   2. Ответственность за проведение мероприятий антивирусного контроля и защиты в Росжелдоре, и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех пользователей государственных информационных систем персональных данных Росжелдора.
   3. Периодический контроль состояния антивирусной защиты, а также соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей Инструкции осуществляется администратором информационной безопасности.