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

**Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта**

1. **Назначение и область действия**
   1. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и систем защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта (далее – Порядок) определяет действия, связанные с функционированием государственных информационных систем (далее – ГИС) Федерального агентства железнодорожного транспорта (Росжелдор), меры и средства поддержания непрерывности работы и восстановления работоспособности ГИС.
   2. Целью настоящего документа является превентивная защита элементов ГИС от предотвращения потери защищаемой информации, определение мер защиты от потери информации, определение действий восстановления в случае потери информации.
   3. Действие настоящего Порядка распространяется на всех пользователей, имеющих доступ к ресурсам ГИС, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

* системы жизнеобеспечения ГИС;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.
  1. Ответственными работниками за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначаются:
* работники, обрабатывающие персональные данные;
* руководители подразделений Росжелдора, в которых производится обработка персональных данных;
* работники ответственные за организацию обработки и обеспечение безопасности персональных данных, обрабатываемых в информационных системах Росжелдора.

1. **Порядок реагирования на инцидент**
   1. В настоящем Порядке под инцидентом понимается любое происшествие, связанное со сбоем в функционировании элементов ГИС, а также потерей защищаемой информации.
   2. Происшествие, вызывающее инцидент, может произойти:

* в результате непреднамеренных действий пользователей;
* в результате преднамеренных действий пользователей и третьих лиц;
* в результате нарушения правил эксплуатации технических и программных средств ГИС;
* в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.
  1. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с непосредственным руководителем. По необходимости, иерархия согласования может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

1. **Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов**
   1. Техническими мерами для обеспечения непрерывной работы и восстановления является использование систем для предотвращения потери информации (включающих программные и технические средства), таких как:

* системы жизнеобеспечения ГИС;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.
  1. Системы жизнеобеспечения ГИС включают:
* пожарные сигнализации и системы пожаротушения;
* системы резервного питания.
  1. Все помещения, в которых размещаются элементы ГИС и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.
  2. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ГИС: ПЭВМ, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания.
  3. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.
  4. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердых носителях (жесткий магнитный диск, лазерный диск, флэшку).
  5. Резервное копирование и хранение данных должно осуществляться на периодической основе:
* для обрабатываемых персональных данных – не реже 1 раза в неделю;
* для технологической информации – не реже 1 раза в месяц;
* эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты) – каждый раз при внесении изменений в эталонные копии (выход новых версий).
  1. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.