АДМИНИСТРАЦИЯ ТРОИЦКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 22.09.2017 № 629р

Об утверждении регламента проведения резервного копирования и восстановления программ и данных, хранящихся на серверах и рабочих станциях в администрации Троицкого муниципального района

В целях исполнения Федерального закона от 27 июля 2006 года № 152 – ФЗ «О персональных данных», в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01 ноября 2012 года № 1119:

1. Утвердить прилагаемый регламент проведения резервного копирования и восстановления программ и данных, хранящихся на серверах и рабочих станциях в администрации Троицкого муниципального района.

2. Контроль за исполнением настоящего распоряжения возложить на управляющего делами администрации Троицкого муниципального района Валееву Э.Ш.

Глава администрации
Троицкого муниципального района Л.В. Шаталова

УТВЕРЖДЕН
Распоряжением администрации
Троицкого муниципального района
от «22.09.2017г.» № 629-р

РЕГЛАМЕНТ

проведения резервного копирования и восстановления программ и данных, хранящихся на серверах и рабочих станциях в администрации Троицкого муниципального района

1. Общие положения

1.1. Настоящий регламент проведения резервного копирования и восстановления программ и данных, хранящихся на серверах и рабочих станциях в администрации Троицкого муниципального района (далее – Регламент) разработан с целью:

1.1.1) определения порядка резервирования данных для последующего восстановления работоспособности информационных систем персональных данных (ИСПДн) администрации Троицкого муниципального района (далее - Администрация) при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

1.1.2) определения порядка восстановления информации в случае возникновения такой необходимости;

1.1.3) упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

1.2. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

1.2.1) резервное копирование;

1.2.2) контроль резервного копирования;

1.2.3) хранение резервных копий;

1.2.4) полное или частичное восстановление данных и приложений.

1.3. Ответственным за проведение процедуры резервного копирования является администратор безопасности ИСПДн Администрации.

2. Порядок резервного копирования

2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе. Резервному копированию подлежит информация следующих основных категорий:

- базы данных, содержащие персональные данные (согласно Перечню информационных систем персональных данных администрации Троицкого муниципального района) – не реже раза в неделю;

- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД) – не реже раза в месяц;

- групповая информация пользователей (общие каталоги отделов) – не реже раза в месяц;

- персональная информация пользователей (личные каталоги на файловых серверах) – не реже раза в месяц;

- персональные профили пользователей сети – не реже раза в месяц;

- регистрационная информация системы информационной безопасности автоматизированных систем – не реже раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.2. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в вечернее время.

2.3. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета (Приложение 1 к Регламенту).

2.4. Минимальный срок хранения резервных копий - 3 месяца.

2.5. Резервные копии хранятся на машинных носителях, отличных от носителей, содержащих исходную информацию.

2.6. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования. Машинные носители, содержащие резервные копии баз данных с персональными данными, маркируются и регистрируются в Журнале учета машинных носителей ПДн.

2.7. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

2.8. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения резервируемой информации в установленные сроки и с заданной периодичностью.

2.9. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено администратору безопасности ИСПДн Администрации.

2.10. Контроль результатов всех процедур резервного копирования осуществляется администратором безопасности ИСПДн.

3. Ротация носителей резервной копии

3.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются администратором безопасности ИСПДн. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

3.2. Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

4. Восстановление информации из резервной копии

4.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

4.2. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к используемой системе резервного копирования.

4.3. Вне зависимости от требований инструкций к используемому ПО, перед каждым процессом восстановления СУБД и файлов из резервных копий, должно проводиться внеплановое резервное копирование информации, подлежащей замене из резервной копии.

Управляющий делами администрации
Троицкого муниципального района Э.Ш. Валеева

Приложение №1
к регламенту проведения резервного копирования и восстановления программ и данных, хранящихся на серверах и рабочих станциях в администрации Троицкого муниципального района
от «22.09.2017г.» № 629-р

Журнал учета проведенного резервного копирования

№ п/п	Дата проведения процедуры	Резервируемая информация	Тип и регистрационный номер машинного носителя	Место хранения машинного носителя	Ответственный за резервное копирование	Подпись ответственного