Республика Ингушетия
Администрация муниципального образования «Городской округ город Магас»

Проспект Идриса Зязикова, 2,
город Магас, 386001,
тел.: +7 (8734) 55-12-33, факс: 55-12-33
e-mail: magas@ingushetia.ru

ГIалгIай Республика
«Магас пхье пхьен округ» яхача муниципальни округа Администраци

Заьзикнаькъан Идриса цIерагIа
проспект, 2, Магас пхье
тел.: +7 (8734) 55-12-33, факс: 55-12-33
e-mail: magas@ingushetia.ru

П О С Т А Н О В Л Е Н И Е

«17» марта 2017 г. № 25

г. Магас

Об утверждении регламента проведения резервного копирования данных

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»:

1. Утвердить:

1.1. Регламент проведения резервного копирования данных (Приложение № 1);

1.2. Журнал учета отчуждаемых носителей информации резервного копирования (Приложение № 2).

2. Контроль за исполнением настоящего распоряжения оставляю за собой.

И.о. Главы города Магас **И.Б. Ганиев**

Приложение № 1
к Постановлению Администрации
муниципального образования
«Городской округ город Магас»
от « 14 » марта 2017 г. № 95

Регламент
проведения резервного копирования данных

1. Общие положения

1.1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на автоматизированных рабочих местах и серверах Администрации муниципального образования «Городской округ город Магас» (далее – Организация) разработан с целью:

1.1.1. определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее – ИСПДн) Организации 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. Резервному копированию подлежит информация следующих основных категорий:

1.3.1. персональные данные субъектов;

1.3.2. персональная информация пользователей (личные каталоги на файловых серверах);

1.3.3. групповая информация пользователей (общие каталоги отделов);

1.3.4. информация, необходимая для восстановления серверов и систем управления базами данных;

1.3.5. персональные профили пользователей сети;

1.3.6. информация автоматизированных систем, в т.ч. базы данных;

1.3.7. рабочие копии установочных компонент программного обеспечения рабочих станций;

1.3.8. регистрационная информация системы информационной безопасности.

1.4. Машинным носителям информации, содержащим резервную копию, присваивается маркировка в соответствии с «Инструкцией по учету машинных носителей и регистрации их выдачи».

2. Порядок резервного копирования

2.1. Состав и объем копируемых данных, периодичность проведения резервного копирования определяется «Перечнем резервируемых данных» (Приложение №1). Максимальный срок хранения резервных копий 3 (три) месяца.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне (Приложение №1), в установленные сроки и с заданной периодичностью. «Методика проведения резервного копирования» описана в Приложении №2.

2.3. 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, либо ответственному за обеспечение безопасности персональных данных Организации.

3. Контроль результатов резервного копирования

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

3.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

4. Ротация носителей резервной копии

4.1. 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.

4.2. Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения.

5. Восстановление информации из резервной копии

5.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн. Процедура восстановления информации из резервной копии осуществляется в соответствии с Методикой восстановления информации (Приложение №3).

5.2. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Приложение 1
к Регламенту резервного
копирования данных

Перечень информации для резервного копирования

Копируемый ресурс	Метод копирования	Тип копирования	Место размещения		Расписание копирования	Временные характеристики		Примечание
			Тип носителя	Периодичность смены		Срок хранения	Периодичность тестирования копий	
Операционная система, настройки, конфигурация основных системных служб и приложений	Бэкап данных с помощью стандартных системных служб	Локальное копирование	Внешний HDD	По выработке ресурса указанного в технической документации установленного заводом изготовителем, либо после диагностики HDD показавшей сильную изношенность оборудования	По ходу установки нового программного обеспечения или изменения настроек и конфигурации используемого программного обеспечения на действительном АРМ	Три месяца с даты резервирования данных		
Базы данных ИС, в том числе с ПД	Архивация специальным внешним программным ПО, либо внутренним	Локальное копирование	Внешний HDD	По выработке ресурса указанного в технической документации установленног	Каждые 7 дней	Три месяца с даты резервирования данных		

	и средствами ИС (если есть)			о заводом изготовителем, либо после диагностики HDD показавшей сильную изношенность оборудования				
Общие и личные локальные каталоги служащих АМО содержащие производственную документацию	Архивация специальным внешним программным ПО	Локальное копирование	Внешний HDD	По выработке ресурса указанного в технической документации установленного заводом изготовителем, либо после диагностики HDD показавшей сильную изношенность оборудования	Каждые 7 дней	Три месяца с даты резервирования данных		

Приложение 2
к Регламенту резервного
копирования данных

Методика резервного копирования

1. Для организации системы резервного копирования используются стандартные средства операционной системы.
2. Существует еженедельная копия. Срок хранения: три месяца.

Копии хранятся на внешнем НЖМД.

3. Различаются два принципиально разных источника информации, подлежащей резервированию:

– Информация, хранимая непосредственно в файловой системе - MS Windows.
– Базы данных ИСПДн.

4. Для резервирования информации, хранимой в базах данных ИСПДн Организации, в качестве промежуточного звена автоматизации используются средства конфигурирования ИСПДн и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИСПДн.

Приложение 3
к Регламенту резервного
копирования данных

Методика восстановления резервируемых данных

Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн или в случае необходимости восстановления утерянной или поврежденной информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования ПО.

Приложение № 2
к Постановлению Администрации
муниципального образования
«Городской округ город Магас»
от « 17 » августа 2017 г. № 25

Журнал учета отчуждаемых носителей информации резервного копирования

Носитель копии	Передача на хранение			Выдача с хранения		
	Дата и время	Ответственное лицо, передавшее носитель		Дата и время	Ответственное лицо	
		ФИО	Подпись		ФИО	Подпись