АДМИНИСТРАЦИЯ
МАРЁВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

П О С Т А Н О В Л Е Н И Е

29.11.2024 № 410

с. Марёво

Об утверждении Регламента проведения резервного копирования информации, обрабатываемой в информационных (автоматизированных) системах Администрации Марёвского муниципального округа

В соответствии с подпунктом «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с целью предотвращения реализации угроз безопасности информации Администрация муниципального округа **ПОСТАНОВЛЯЕТ:**

1. Утвердить Регламент проведения резервного копирования информации, обрабатываемой в информационных (автоматизированных) системах Администрации Марёвского муниципального округа (далее – Регламент).

2. Опубликовать настоящее постановление на официальном сайте Администрации Марёвского муниципального округа в информационно-телекоммуникационной сети «Интернет».

Глава муниципального округа **С.И. Горкин**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Серийный номер сертификата:
59C3121DFFCAC46612F60E9667D9E687
Владелец: Горкин Сергей Иванович
Дата подписания: 29.11.2024 15:34
Срок действия: с 10.09.2024 по 04.12.2025

УТВЕРЖДЁН
постановлением Администрации
Марёвского муниципального округа
от 29.11.2024 №410

Регламент проведения резервного копирования информации, обрабатываемой в информационных (автоматизированных) системах Администрации Марёвского муниципального округа

1. Общие положения

Настоящий Регламент проведения резервного копирования информации, обрабатываемой в информационных (автоматизированных) системах Администрации Марёвского муниципального округа, разработан с целью:

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

определения порядка восстановления информации в случае возникновения такой необходимости;

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

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

резервное копирование;

хранение резервных копий;

полное или частичное восстановление данных.

Резервному копированию подлежит информация следующих основных категорий:

персональные данные субъектов;

персональная информация пользователей (личные каталоги на файловых серверах);

групповая информация пользователей (общие каталоги отделов);

информация, необходимая для восстановления сервера;

персональные профили пользователей сети;

информация автоматизированных систем, в том числе базы данных;

рабочие копии установочных компонент программного обеспечения рабочих станций;

регистрационная информация системы информационной безопасности.

1.2. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.3. Доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам ИСПДн. Список лиц формируется на основании письменной Заявки заместителя Главы или управляющего делами Администрации Марёвского муниципального округа, согласованной с заведующим информационным отделом. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности (ИБ), произошедших в процессе резервного копирования, сообщается в информационный отдел служебной запиской в течение рабочего дня после обнаружения указанного события.

2. Порядок резервного копирования

2.1 Резервное копирование информации производится на основании следующих данных:

состав и объем копируемых данных, периодичность проведения резервного копирования;

максимальный срок хранения резервных копий.

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

3. Периодичность резервного копирования

3.1. Для организации системы резервного копирования на рабочих станциях используются стандартные средства операционной системы. Резервное копирование осуществляется один раз в сутки.

3.2. Резервное копирование на сервере производится один раз в две недели. Срок хранения резервной копии составляет 1 месяц.

4. Восстановление данных из резервной копии

4.1. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

4.2. При частичном нарушении или исчезновении записей информации восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

4.3. Любое восстановление информации выполняется на основании заявки пользователя ответственному должностному лицу за организацию обработки персональных данных или в случае необходимости восстановления утерянной или поврежденной информации, подлежащей резервированию.

4.4. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы.

5. Ротация носителей резервной копии

5.1. Все процедуры по загрузке, выгрузке информации с носителей копий осуществляются ответственным работником. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

6. Ответственность за состояние резервного копирования

6.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на ответственное должностное лицо, осуществляющее резервное копирование.

6.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением Регламента, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.