

**АДМИНИСТРАЦИЯ**

**КАЛАЧЕЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**ВОРОНЕЖСКОЙ ОБЛАСТИ**

**РАСПОРЯЖЕНИЕ**

от "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. № \_\_\_\_\_\_

г. Калач

**Об утверждении регламента проведения**

**резервного копирования информации,**

**обрабатываемой на средствах вычислительной**

**техники (СВТ) в администрации Калачеевского**

**муниципального района Воронежской области**

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 **п р и к а з ы в а ю**:

1. Утвердить Регламент проведения резервного копирования информации обрабатываемой на средствах вычислительной техники (СВТ) согласно приложению № 1 к настоящему приказу
2. Довести приказ до сотрудников, в части их касающейся.
3. Контроль за исполнением настоящего распоряжения возложить на руководителя аппарата администрации Калачеевского муниципального района Бондарева Виктора Михайловича.

Глава администрации Калачеевского

муниципального района Н.Т. Котолевский

Приложение №1

к распоряжению от \_\_\_\_ декабря 2024 г. № \_\_\_\_\_

**РЕГЛАМЕНТ**

**проведения резервного копирования информации, обрабатываемой на средствах вычислительной техники (СВТ)**

1.1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на автоматизированных рабочих местах Финансового отдела администрации Калачеевского муниципального района Воронежской области разработан с целью:

1) Определение порядка резервирования данных для последующего восстановления работоспособности средств вычислительной техники, информационных систем и информационных систем персональных данных, при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайной ситуацией (пожаром, стихийным бедствием, кибератакой, воздействием вредоносного программного обеспечения и т.д.);

2) Определение порядка восстановления информации в случае возникновения такой необходимости;

3) Упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации;

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

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

полное или частичное восстановление данных и приложений.

1.3. Резервному копированию подлежит информация следующих основных категорий:

персональные данные;

информация пользователей (личные каталоги с носителей информации сотрудников);

групповая информация пользователей (общие каталоги на файловом сервере);

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

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

Порядок резервного копирования

2.1. Состав и объем копируемых данных, периодичность проведения резервного копирования определяется «Перечнем информации резервного копирования» (Приложение №2).

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне (Приложение №2), в установленные сроки и с заданной периодичностью. «Методика проведения резервного копирования» описана в Приложении №3.

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 ответственному за обеспечение безопасности персональных данных Администрации.

2.4. Резервные копии хранятся на сетевом оборудовании в изолированном помещении, физический доступ к которому только у сотрудника, ответственного за резервного копирование.

Контроль результатов резервного копирования

* 1. Контроль результатов всех процедур резервного копирования информации осуществляется сотрудником, ответственным за обеспечение безопасности персональных данных.

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 в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей резервного копирования, а также их перемещение, осуществляются ответственным за резервное копирование. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

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

Восстановление информации из резервной копии

5.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя. Процедура восстановления информации из резервной копии осуществляется в соответствии с Методикой восстановления информации (Приложение №4).

5.2. После поступления заявки, восстановление данных осуществляется ответственным за резервное копирование в максимально короткие сроки, но не более одного рабочего дня.

Приложение №2

к распоряжению от \_\_\_\_ декабря 2024 г. № \_\_\_\_\_

**Перечень информации резервного копирования**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Копируемый ресурс | Метод копирования | Тип копирования | Место размещения | Расписание копирования | Временные характеристики |
| Локальные каталоги сотрудников | Резервное копирование данных с помощью стандартных системных служб | Сетевое копирование | Сетевое оборудование для хранение резервных копий | 1 раз в неделю | 6 месяцев |
| Базы данных программного обеспечения «1С», SQL сервера | Резервное копирование данных с помощью специализированного программного обеспечения для автоматического создания резервного копирования по расписанию | Сетевое копирование | Сетевое оборудование для хранение резервных копий | 1 раз в неделю | 6 месяцев |
| Сетевые каталоги файлового сервера | Резервное копирование данных с помощью специализированного программного обеспечения для автоматического создания бекабов по расписанию | Сетевое копирование | Сетевое оборудование для хранение резервных копий | 1 раз в неделю | 6 месяцев |
| Средства электронно-цифровой подписи | Копирование данных с помощью стандартных системных служб | Внешний носитель | Надежно запираемый сейф | 1 раз в 15 месяцев | 15 месяцев |

Приложение №3

к распоряжению от \_\_\_\_ декабря 2024 г. № \_\_\_\_\_

**Методика резервного копирования**

Для организации системы резервного копирования используются стандартные средства операционной системы и специализированное программное обеспечение с возможностью автоматизировать процесс резервного копирования по расписанию.

Копии создаются один раз в неделю (или по мере необходимости). Срок хранения: шесть месяцев.

Копии хранятся на внешнем машинном носителе информации или сетевом оборудовании для хранения резервных копий.

Информация, подлежащая резервированию, определяется «Перечнем информации резервного копирования» (Приложение №2).

Требования к сетевому оборудованию для хранения резервных копий:

1. Высокая производительность:
   1. Обеспечьте высокую скорость чтения и записи данных для быстрого восстановления информации.
   2. Используйте SSD-накопители для повышения производительности.
2. Большой объем памяти:
   1. Объем памяти должен быть достаточным для хранения всех необходимых данных. Рекомендуемый объем накопителей: 5 ТБ.
   2. Возможность расширения объема памяти с помощью дополнительных дисков.
3. Высокая отказоустойчивость:
   1. Использование технологий RAID (например, RAID 1) для обеспечения высокой сохранности данных.
   2. Регулярное тестирование и обслуживание RAID-массивов.
4. Источник бесперебойного питания (ИБП):

4.1 Оборудование должно быть подключено к ИБП для защиты данных от потери в случае сбоя электропитания.

4.2. ИБП должен обеспечивать достаточное время автономной работы для завершения операций записи и выключения системы.

1. Ограниченный физический доступ:

5.1 Ограничьте физический доступ к оборудованию для предотвращения несанкционированного вмешательства.

5.2 Установка оборудования в помещении с контролем доступа.

Приложение №4

к распоряжению от \_\_\_\_ декабря 2024 г. № \_\_\_\_\_

**Методика восстановления резервируемых данных**

Любое восстановление информации выполняется на основании заявки пользователя ответственному за обеспечение безопасности персональных данных финансового отдела администрации Калачеевского муниципального района Воронежской области 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, прилагающийся к специализированному программному обеспечению для автоматического создания резервных копий.