**Для служебного**

|  |  |
| --- | --- |
| **УТВЕРЖДАЮ:** |  |
| **Директор СПб ГУ**  **«Центр занятости населения \_\_\_\_\_\_\_\_\_\_\_\_ района»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.** |  |

**пользования**

**«Инструкция по организации резервного копирования и восстановления программного обеспечения, конфиденциальной информации автоматизированных систем и баз данных, содержащих персональные данные, информационных систем ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района»**

**Санкт – Петербург**

**2010 год**

Оглавление

[Введение 1](#_Toc279050608)

[Список терминов и определений 1](#_Toc279050609)

[Общие положения 1](#_Toc279050610)

[Порядок резервного копирования 2](#_Toc279050611)

[Контроль результатов резервного копирования 3](#_Toc279050612)

[Ротация носителей резервной копии. 3](#_Toc279050613)

[Восстановление информации из резервных копий 4](#_Toc279050614)

[Приложения 5](#_Toc279050615)

[Приложение №1. Заявка-запрос 5](#_Toc279050616)

[Приложение №2. Перечень лиц ответственных за резервное копирование 6](#_Toc279050617)

[Приложение №3. Методика резервного копирования 7](#_Toc279050618)

[Приложение №4. Методика восстановления данных 9](#_Toc279050619)

# Введение

Настоящая «Инструкция по организации резервного копирования и восстановления программного обеспечения, конфиденциальной информации автоматизированных систем и баз данных, содержащих персональные данные, информационных систем ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района» (далее Инструкция) разработана с целью определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных (далее АС) и информационных (далее ИС) систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.).

# Список терминов и определений

Администратор резервного копирования – сотрудник ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района, осуществляющий управление процедурами резервного копирования и восстановления информации.

Заявка – запрос сотрудника ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района к администратору резервного копирования (администратору сети) на:

* включение дополнительных данных в регламент резервного копирования или на восстановление информации (Приложение №1);
* создание или удаление ресурса общего доступа в составе АС или ИС ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района (Приложение №1).

Ресурс общего доступа – это каталог на сервере в составе АС или ИС ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района, предназначенный для хранения файлов в целях, указанных в заявке на создание ресурса, предоставленный в общий доступ средствами операционной системы.

# Общие положения

Настоящая Инструкция разработана с целью:

* определения порядка резервирования данных для последующего восстановления работоспособности АС и ИС 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

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

* резервное копирование;
* контроль резервного копирования;
* хранение резервных копий;
* полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

* Персональная информация пользователей (личные каталоги на файловых серверах);
* Групповая информация пользователей (общие каталоги отделов);
* Информация, необходимая для восстановления службы каталога Windows (домена KZN021), серверов, систем управления базами данных (далее – СУБД), рабочих станций (если необходимо);
* Персональные профили пользователей сети (если необходимо);
* Информация АС и ИС (базы данных, журнальные файлы, конфигурационные файлы и т.д.);
* Рабочие копии установочных компонент программного обеспечения рабочих станций и серверов, а так же программное обеспечение ИС;
* Регистрационная информация системы информационной безопасности.

Машинным носителям информации, содержащим резервную копию, присваивается гриф «Конфиденциально» если на них содержатся сведения (данные, информация) указанные в документе «Перечень сведений конфиденциального характера и персональных данных автоматизированных и информационных систем ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района».

# Порядок резервного копирования

Резервное копирование производится на основании следующих данных:

* состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных - по форме, приведенной в Приложении №1);
* максимальный срок хранения резервных копий -1 месяц;
* хранение 3-х следующих архивов
  + архив на 1-е число текущего месяца
  + архив пятница-суббота текущей недели
  + архив сделанный в текущую ночь

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 №3.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, сообщается руководителю ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района служебной запиской в течение рабочего дня после обнаружения указанного события. Ответственным является администратор резервного копирования (согласно Приложению №1).

# Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, указанными в Приложении №2, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает об этом лицу ответственному за выполнение процедур резервного копирования. Выполняется анализ причины возникновения ошибки и принятие мер исключающих ее повторение на очередном цикле создания резервной копии этих данных. При необходимости создается внеочередная резервная копия данных.

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

# Ротация носителей резервной копии.

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

По истечении срока эксплуатации (при повреждении) производится замена испорченных носителей информации новыми. Если носитель имел гриф «Конфиденциально» то, в соответствии с инструкцией «Инструкция по ведению журнала «Журнал учета носителей, содержащих конфиденциальную информацию и персональные данные», делается соответствующая запись в журнале «Журнал учета носителей, содержащих конфиденциальную информацию и персональные данные». Носитель данных при этом выводится из эксплуатации способом, делающим невозможным считывание с него информации.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их в область хранения и обратно, осуществляются администратором резервного копирования.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек (ротация носителей).

Запрещено использовать носители с грифом «Конфиденциально» для записи не конфиденциальной информации и наоборот.

# Восстановление информации из резервных копий

В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации согласованной с администратором сети и администратором безопасности ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района..

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации (Приложение №4).

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

# Приложения

## Приложение №1. Заявка-запрос

Прошу осуществить:

* резервное копирование информации;
* восстановление информации;
* создание ресурса общего доступа;
* удаление ресурса общего доступа,

так как это необходимо для выполнения должностных обязанностей (производственного процесса). Согласовано с руководителем отдела (подразделения). Согласовано с администратором безопасности. Передано к исполнению лицу, ответственному за резервное копирование информации в АС и ИС ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района.

Описание:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Точное расположение ресурса (\\сервер\каталог\файл)** | **Имя ресурса общего доступа (только при создании или удалении)** | **Гриф конфиденциальности информации** | **Действие (резервное копирование, восстановление, создание, удаление)** | **Переодичность (для процедуры резервирования информации (если необходимо))** | **Дата (начала процедуры копирования данных для резервирования, выбора набора для восстановления, создания ресурса, удаления ресурса)** | **Ответственный за ресурс** |
| 1 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Приложение №2. Перечень лиц ответственных за резервное копирование

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Роль ответственного лица (номер(а) из перечня)** | **Ответственное лицо** | **Дата начала периода ответственности** | **Подпись сотрудника** |
| 1 |  |  |  |  |

Перечень ролей в системе резервного копирования информации ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района

1. Первоначальная настройка системы резервного копирования (создание наборов носителей, планирование расписаний, первоначальный выбор ресурсов, создание оповещений).
2. Внесение существенных изменений в настройку системы резервного копирования (добавление заданий, удаление заданий, работа с наборами данных, восстановление данных и т.д.).
3. Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротации носителей.
4. Ротация носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне офиса на случай катастрофы.

Допускается присвоение нескольких ролей одному ответственному лицу.

## Приложение №3. Методика резервного копирования

Для организации системы резервного копирования используется стандартное программное обеспечение (далее ПО), входящее в состав операционной системы Windows, а так же ПО HP OmniBack Dataprotector. Учитывая пропускные способности каналов, объёмы резервируемых данных, представляется оптимальным установить независимый сервер резервного копирования на площадке ГУ ЦЗН \_\_\_\_\_\_\_\_\_\_\_\_ района. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на встроенный в сервер привод магнитной ленты или на жёсткий диск.

С помощью указанного ПО выполняются следующие действия:

* задание режимов и составление расписания резервного копирования данных;
* осуществляются операции по загрузке и выгрузке носителей информации;
* проводится контроль за состоянием выполнения заданий;
* запускаются процедуры восстановления информации.

Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации проводятся в нерабочее (ночное) время. Существуют три набора резервных копий:

1. Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования.
2. Недельная копия. Записывается в ночь на субботу. Срок хранения – до следующей субботы. Хранится на сервере резервного копирования.
3. Ежедневная копия. Записывается ежесуточно, по завершению рабочего дня, кроме ночи на субботу. Срок хранения – сутки. Хранится на сервере резервного копирования.

Различаются три принципиально разных источника информации, подлежащей резервированию:

1. Информация, хранимая в базе данных прикладной ИС, содержащая персональные данные.
2. Информация, хранимая непосредственно в файловой системе Windows, содержащая данные пользователей.
3. База данных службы каталогов Windows, содержащая информацию о конфигурации домена.

Для резервирования информации, хранимой в базах данных прикладной ИС (см. пункт 1-й, выше), в качестве промежуточного звена автоматизации используются средства конфигурирования ИС и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных прикладной ИС. Посредством ПО HP OmniBack Dataprotector формируются задания на проведение резервного копирования этого каталога. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Для резервирования информации, хранимой непосредственно в файловых системах (см. пункт 2-й, выше), используется ПО, входящее в состав операционной системы Windows, а так же ПО HP OmniBack Dataprotector, посредством которых формируются задания на проведение резервного копирования информации, находящейся в каталогах файловых систем Windows. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Для резервирования информации базы данных службы каталогов Windows, содержащей информацию о конфигурации домена, (см. пункт 3-й, выше), используется ПО, входящее в состав операционной системы Windows, а так же ПО HP OmniBack Dataprotector, посредством которого формируются задания на проведение резервного копирования информации, находящейся в базе данных службы каталогов Windows. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

## Приложение №4. Методика восстановления данных

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности АС и ИС или их компонентов, выполняется на основании Заявки (Приложение №1).

Восстановление информации, относящейся к базам прикладной ИС, происходит при совместном взаимодействии с администратором прикладной ИС.

В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системам резервного копирования ПО, входящего в состав операционной системы Windows, а так же ПО HP OmniBack Dataprotector.

Запрещается восстановление информации с грифом «Конфиденциально» на носитель не имеющий грифа «Конфиденциально» и наоборот.