

## **РЕГЛАМЕНТ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ**

## **СОДЕРЖАНИЕ**

<b>1.СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ .....</b>	<b>3</b>
<b>2.ОБЩИЕ ПОЛОЖЕНИЯ.....</b>	<b>3</b>
<b>3.ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ .....</b>	<b>4</b>
<b>4.КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ .....</b>	<b>4</b>
<b>5.РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ .....</b>	<b>5</b>
<b>6.ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ .....</b>	<b>5</b>
<b>ПРИЛОЖЕНИЕ №1 - ПЕРЕЧЕНЬ РЕЗЕРВИРУЕМОЙ ИНФОРМАЦИИ .....</b>	<b>5</b>
<b>ПРИЛОЖЕНИЕ №2 - ПЕРЕЧЕНЬ ЛИЦ ОТВЕТСТВЕННЫХ ЗА РЕЗЕРВНОЕ КОПИРОВАНИЕ .....</b>	<b>5</b>
<b>ПРИЛОЖЕНИЕ №3 - МЕТОДИКА РЕЗЕРВНОГО КОПИРОВАНИЯ.....</b>	<b>6</b>
<b>ПРИЛОЖЕНИЕ №4 - МЕТОДИКА ВОССТАНОВЛЕНИЯ ДАННЫХ.....</b>	<b>7</b>

## 1. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

- **Заказчик** – Компания ИП “FastHotPizza”
- **Исполнитель** – Компания “ООО ИС - 21”.
- **ГСА (группа системных администраторов)** - группа сотрудников Исполнителя, обеспечивающая развитие и устранение сложных неисправностей ИТ-инфраструктуры Заказчика.
- **ГТП (группа технической поддержки)** – группа сотрудников Исполнителя, обеспечивающая техническую поддержку сотрудников Заказчика.
- **ИТ-инфраструктура** - совокупность аппаратного и программного обеспечения компании Заказчика, а также правил и методов их настройки, обеспечивающих технологию совместной работы сотрудников Заказчика.
- **Администратор файлового сервера** – сотрудник Исполнителя из числа ГСА, осуществляющий управление файловым сервером
- **Сотрудник технической поддержки** – сотрудник Исполнителя из числа ГСА.
- **Заявка** – запрос сотрудника предприятия к службе технической поддержки на решение какой-либо технической проблемы. Заявка содержит описание проблемы и электронный адрес сотрудника.
- **Ресурс файлового сервера (далее Ресурс)** – это каталог на файловом сервере, предназначенный для хранения файлов в целях, указанных в заявке на создание ресурса.
- **Ответственный за информационные ресурсы Заказчика** – сотрудник Заказчика из числа руководителей принимающий решения о создании новых Ресурсов.
- **ИС «Helper»** – информационная система, обеспечивающая прием и обработку заявок сотрудников Заказчика.
- **ИСМ** – информационная система мониторинга ИТ-инфраструктуры Заказчика.
- **ЭЦП** – электронная цифровая подпись.
- **PGP** – программное обеспечение для шифрования и ЭЦП данных.
- **Согласование Заявки** – направление электронного сообщения (email) подтверждающего Заявку в ИС «Helper» с ЭЦП. Для создания ЭЦП используется программное обеспечение PGP.
- **Ответственный за ресурс** – сотрудник Заказчика указанный ответственным в заявке на создание ресурса.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах ИТ-инфраструктуры Заказчика разработан с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем Заказчика 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 Исполнителя и Заказчика, 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);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- рабочие копии установочных компонентов программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с «Перечнем сведений составляющих коммерческую тайну» Заказчика.

### **3. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ**

Резервное копирование автоматизированных систем 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 среда-четверг, либо 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 в Службу безопасности Заказчика служебной запиской в течение рабочего дня после обнаружения указанного события. Ответственным является администратор резервного копирования (согласно Приложению №1).

### **4. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ**

Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, указанными в Приложении №2, в срок до 21 часа рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает в ГТП до 19 часов текущего рабочего дня.

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.

## 5. 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. В случае необходимости замены испорченных носителей информации новыми, Исполнитель заблаговременно за 10 рабочих дней согласовывает с Заказчиком спецификации новых носителей информации.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их в Службу безопасности и обратно, осуществляются администратором резервного копирования по запросу и в присутствии ответственного сотрудника Службы безопасности Заказчика (согласно Приложению №2).

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

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

## 6. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ

В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации согласованной с Ответственным за информационные ресурсы Заказчика.

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, но не более одного рабочего дня.

### ПРИЛОЖЕНИЕ №1 - ПЕРЕЧЕНЬ РЕЗЕРВИРУЕМОЙ ИНФОРМАЦИИ

№ п/п	Адрес хранения информации	Примечание
1	\\serverpas\product\PizzaAssistanceSysytem	Главная(основная) часть ИС “PizzaAssistanceSystem“
2	\\serverpas\db\Database	Файлы базы данных “MySQL“ для обработки и хранения данных ИС.

### ПРИЛОЖЕНИЕ №2 - ПЕРЕЧЕНЬ ЛИЦ ОТВЕТСТВЕННЫХ ЗА РЕЗЕРВНОЕ КОПИРОВАНИЕ

№ п/п	Выполняемая роль	ФИО ответственного сотрудника
1	Первоначальная настройка системы резервного копирования (создание медиа-сетов, расписаний, selection lists, оповещений). Запуск в промышленную эксплуатацию системы резервного копирования.	Иванов Илья Александрович
2	Внесение существенных изменений в настройку системы резервного копирования.	Станкевич Даниил Дмитриевич

3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротирования носителей.	Новиков Никита Ильич
4	Ротирование носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне офиса на случай катастрофы.	Блощицын Виталий Юрьевич

### ПРИЛОЖЕНИЕ №3 - МЕТОДИКА РЕЗЕРВНОГО КОПИРОВАНИЯ

Для организации системы резервного копирования используется программное обеспечение компаний MySQL последней версии. Учитывая пропускные способности каналов, стоимость трафика между офисами, объемы резервируемых данных, представляется оптимальным установить независимые серверы резервного копирования в каждом из основных офисов. С целью оптимизации расходов на развертывание системы резервного копирования, запись резервной копии осуществляется на жесткий диск.

С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Настройка всех трех серверов одинакова. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в 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 среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере;
3. Ежедневная копия. Записывается ежедневно, кроме ночи на среду и ночи на субботу. Срок хранения – сутки. Записывается на съемный жесткий диск. Жесткий диск по отдельному расписанию выносится за пределы офиса. Различаются три принципиально разных источника информации, подлежащей резервированию:
  - Информация, хранимая в Exchange Server.
  - Информация, хранимая непосредственно в файловой системе - MS Windows.
  - Базы данных Прикладной информационной системы. Для резервирования информации, хранимой в Exchange Server, почтовые ящики и общие папки, используется ПО Microsoft Exchange Server с установленным Exchange агентом, посредством которого формируются задания на проведение резервного копирования информации, находящейся в хранилищах Exchange сервера. 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 system manager установленной OpenFile Option, посредством которого формируются задания на проведение резервного копирования информации, находящейся в каталогах файловых систем MS Windows. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Для резервирования информации, хранимой в базах данных Прикладной информационной системы (см. пункт 1-й, выше), в качестве промежуточного звена автоматизации используются

средства конфигурирования Прикладной информационной системы и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных Прикладной информационной системы. Посредством средства “Jira“ от компании ‘Atlassian’ формируются задания на проведение резервного копирования этого каталога. 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 информационной системы или ее компонент, выполняется на основании заявки, оформленной через систему Helper.

Восстановление информации, относящейся к базам Прикладной информационной системы, происходит при тесном взаимодействии с администратором Прикладной информационной системы.

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