

СОГЛАСОВАНО
Педагогическим советом
ОГПОБУ «Технический
колледж» Протокол №
от «30» июня 2016 г.



УТВЕРЖДЕНО
Приказом директора ОГПОБУ
«Технический колледж»
от «5» июня 2016 г.

ПОЛОЖЕНИЕ

о резервном копировании ОГПОБУ «Технический колледж»

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности ОГПОБУ «Технический колледж» в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами и устанавливает порядок проведения резервного копирования данных в ОГПОБУ «Технический колледж» (далее Организация).

1.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

1.3. Резервному копированию подлежат информация следующих основных категорий:

~ персональная информация пользователей (личные каталоги на файловых серверах);

~ групповая информация пользователей (общие каталоги отделов);

~ информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);

~ информация автоматизированных систем, в т.ч. баз данных;

~ данные справочно-информационных систем общего использования ("Консультант+" и т.п.);

~ рабочие копии установочных компонент программного обеспечения рабочих станций;

~ данные с рабочих станций, содержащих критически важную информацию.

2. Основные термины, сокращения и определения

АС – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

Резервное копирование – это сохранение очередного текущего состояния информации (системы) без обязательного сохранения предыдущего.

Полное копирование - создание полной копии (одна копия);

Инкрементальное копирование - создание копий измененных данных, которые были изменены после последнего полного, инкрементального или дифференциального копирования (несколько копий, первая запись – это полная копия, вторая запись – копия только тех данных, которые были изменены со времени первой записи, а на третьем этапе копируются данные модифицированные со времени второго этапа и т.д.);

Дифференциальное копирование - создание последней копии измененных данных со времени проведения полного копирования (две копии, первая запись – это полная копия, а на последующих этапах копируются только данные, которые изменились со времени проведения полного копирования).

Архивирование – долгосрочное хранение информации, либо состояния системы.

Система резервного копирования – подсистема АС Организации, которая предназначена для создания резервных копий и восстановления данных.

Ресурс сервера (далее Ресурс) – это каталог, файл с данными, программное обеспечение или сервис на сервере.

3. Организация резервного копирования

3.1. Для обеспечения резервного копирования, восстановления и архивного хранения электронных данных приказом по Организации в каждом структурном подразделении назначается ответственный за резервное копирование. Ответственный за резервное копирование подчиняется заместителю директора по ИТ Организации, в своей работе руководствуется настоящим Положением, нормативными актами по защите информации, техническими инструкциями на серверное оборудование, систему хранения данных и другими документами.

3.2. Инструктивно-методическое руководство деятельностью ответственного за резервное копирование осуществляется администратором ИБ.

3.3. Основными задачами ответственного за резервное копирование являются:

- планирование резервного копирования и восстановления;
- установление жизненного цикла и календаря операций;
- ежедневный обзор логов процесса резервного копирования;
- защита данных резервного копирования от повреждения, модификации и несанкционированного доступа;
- развитие системы резервного копирования;

К ежедневным задачам ответственного за резервное копирование относятся:

- мониторинг заданий;
- отчеты о сбоях и успешном выполнении;
- анализ и разрешение проблем;
- манипуляции с резервными копиями;
- расписание выполнения заданий.

К еженедельным, ежемесячным и другим задачам ответственного за резервное копирование относятся:

- анализ производительности;
- тенденции изменения объемов и планирование этих изменений;
- рассмотрение и анализ методики резервного копирования;
- проверку возможности восстановления;
- планирование развития архитектуры, определение ежедневных, еженедельных и ежемесячных заданий.

3.4. Основные обязанности ответственного за резервное копирование:

- обеспечить функционирование и поддержание работоспособности средств системы резервного копирования информации;
- немедленно докладывать заместителю директора по ИТ Организации о выявленных ошибках и сбоях при резервном копировании информации, а также принимать необходимые меры по их устранению;
- обеспечить целостность и сохранность резервных копий информации.

3.5. Права ответственного за резервное копирование:

- требовать от пользователей АС Организации безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению резервного копирования и восстановления информации;
- вносить предложения и требовать прекращения обработки информации в случаях нарушения установленной технологии резервного копирования информации или нарушения функционирования средств системы резервного копирования;

3.6. На ответственного за резервное копирование возлагается персональная ответственность за качество проводимых им работ по обеспечению резервного копирования и восстановления информации в соответствии с функциональными обязанностями, определенными в настоящем Положении.

4. Порядок резервного копирования

4.1. В Организации должна быть реализована централизованная система резервного копирования, что позволит сократить совокупную стоимость владения ИТ-инфраструктурой за счет оптимального использования устройств резервного копирования и сокращения расходов на администрирование по сравнению с децентрализованной системой.

4.2. Ответственный за организацию резервного копирования в организации на основании п. 1.3. настоящего Положения и Перечня информационных ресурсов ОГПОБУ «Технический колледж» готовит Перечень данных, подлежащих резервному копированию и хранению (далее – перечень) по установленной форме (Приложение 1).

4.3. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне, в установленные сроки и с заданной периодичностью (Приложение 2. Расписание.)

4.4. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, сообщается к администратору ИБ.

5. Контроль результатов

5.1. Контроль результатов всех процедур резервного копирования осуществляется ответственным за резервное копирование в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

5.2. В случае обнаружения ошибки резервного копирования ответственный за резервное копирование выполняет повторное копирование информации вручную в максимально сжатые сроки не нарушая технологические процессы обработки информации пользователями АС Организации.

6. Хранение резервных копий

6.1 Хранение резервных копий данных осуществляется на сменных носителях информации (CD/DVD, внешние жесткие диски и т.п.), промаркированных ответственным за резервное копирование в соответствии с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование информационной системы данных.

6.2 Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

6.3. Срок хранения резервных копий определяется соглашением с лицом, ответственным за ведение соответствующего информационного ресурса

6.4. Хранение резервных копий осуществляется в соответствии с правилами работы с документами, содержащими информацию ограниченного доступа вместе, отличным от места их изготовления.

6.5 Удаление резервных копий для повторного использования носителя информации либо окончательное удаление производится начальником отдела по защите информации по согласованию с лицом, ответственным за ведение соответствующего информационного ресурса.

7. Восстановление данных с резервных копий

7.1. Восстановление данных с резервных копий производится в соответствии с планом обеспечения непрерывной работы и восстановления работоспособности, принятым в Организации.

7.2 Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

7.3. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.