бюджетное профессиональное
образовательное учреждение
Вологодской области
«Великоустюгский
многопрофильный колледж»

УТВЕРЖДЕН
приказом директора
колледжа
от 19.02.2019 г. № 74

РЕГЛАМЕНТ

«19» 02 2019 г. № 37

г. Великий Устюг

резервного копирования и восстановления данных в бюджетном профессиональном образовательном учреждении Вологодской области «Великоустюгский многопрофильный колледж»

Список терминов и определений

Учреждение – бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский многопрофильный колледж».

ГСА (группа системных администраторов) - группа сотрудников Учреждения, обеспечивающая развитие и устранение сложных неисправностей ИТ-инфраструктуры Учреждения.

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 Учреждения из числа ГСА.

Заявка – запрос сотрудника Учреждения 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 Учреждения – сотрудник Учреждения, принимающий решения о создании новых Ресурсов.

ИСМ – информационная система мониторинга ИТ-инфраструктуры Учреждения.

ЭЦП – электронная цифровая подпись.

GPG – программное обеспечение для шифрования и ЭЦП данных.

Согласование Заявки – направление электронного сообщения (email) подтверждающего Заявку.

Ответственный за ресурс – сотрудник Учреждения указанный ответственным в заявке на создание ресурса.

1. Общие положения

1.1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на компьютерах и серверах ИТ-инфраструктуры Учреждения разработан с целью:
- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем Учреждения 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 Учреждения, 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:
- 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);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- справочно-информационная информация систем общего использования («Гарант», «Консультант+» и т.п.);
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

2. Порядок резервного копирования

2.1. 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.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне (Приложение №1), в установленные сроки и с заданной периодичностью.

2.3. Методика проведения резервного копирования описана в Приложении №3.

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

3. Контроль результатов резервного копирования

3.1. 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.

3.2. 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.

4. 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 автоматизированных систем в случае отказа любого из устройств резервного копирования.

4.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, осуществляются администратором резервного копирования.

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

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

5. Восстановление информации из резервных копий

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

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

5.3. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

СОГЛАСОВАНО
Советом Учреждения
Протокол № 2
«18» 02 20 19 г.

В дело № 01-14
«19» 02 20 19 г.

Приложение №1

Перечень резервируемой информации

№ п/п	Адрес хранения информации	Примечание
1		
2		
3		

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, selectionlists, оповещений). Запуск в промышленную эксплуатацию системы резервного копирования.	
2	Внесение существенных изменений в настройку системы резервного копирования.	
3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротирования носителей.	
4	Ротирование носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне офиса на случай катастрофы.	

Приложение № 3

Методика резервного копирования

1. Для организации системы резервного копирования используется программное обеспечение (далее - ПО) фирмы _____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.

2. 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.

3. Настройка всех трех серверов одинакова. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в ночное время.

4. 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 ежесуточно, 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.

5. Различаются три принципиально разных источника информации, подлежащей резервированию:

- информация, хранимая в ExchangeServer.
- информация, хранимая непосредственно в файловой системе - MS Windows.
- базы данных Прикладной информационной системы.

6. Для резервирования информации, хранимой в ExchangeServer, почтовые ящики и общие папки, (см. пункт 1-й, выше), используется ПО _____ 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.

7. Для резервирования информации, хранимой непосредственно в файловых системах (см. пункт 2-й, выше), используется ПО _____с установленной OpenFileOption, 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.

8. 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 ПО _____ формируются задания на проведение резервного копирования этого каталога. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Приложение № 4

Методика восстановления данных

1. Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонент, выполняется на основании заявки, поданной в IT отдел Учреждения.

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

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