МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Внедрение системы резервного копирования при реализации политики информационной безопасности в организации профессионального образования.

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасности в профессиональном образовании»

Выполнил:
студент группы ОФ-209/210-2-1,
Мезенов Алексей Сергеевич
Научный руководитель:
д.т.н., профессор
кафедры АТ, ИТ и МОТД
Дмитриев Михаил Сергеевич

Проверка на объём заимствований:
65,7% авторского текста
Работа рекомендована к защите
«___» _____2017 г.
Зав. кафедрой АТ, ИТ и МОТД
_____В.В. Руднев

Челябинск, 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информации, хранящейся в компьютерных системах, угрожает множество опасностей. Данные могут быть утеряны по причинам ошибок программного обеспечения, неумелой работы пользователей, сбоев физических носителей и средств связи, злонамеренной порчи данных. Абсолютной защиты от всех этих угроз не существует, риск утраты данных существует всегда.

Как показывают статистические данные по всему миру [4], основными причинами потери данных являются неправильная работа аппаратного обеспечения (44%) и человеческие ошибки (32%), в основном тех, у кого максимальный уровень доступа к системам хранения компании. Почти 14% всех случаев потери данных вызваны ошибками программного обеспечения, остальные 7% связаны с компьютерными вирусами, а из-за стихийных бедствий - всего 3%.

Сбои приводят к приостановке бизнес-процессов и потере данных, что ставит под сомнение существование работы в целом. Пожалуй, единственный способ надежно сохранить необходимую информацию - периодически создавать резервные копии [6].

Внедряя системы хранения и резервного копирования, организация сталкивается со сложными задачами оценки своих текущих потребностей, планирования будущих объемов данных, выбора технологий и архитектур, которые должны максимально соответствовать требованиям безопасности, возможности последующего масштабирования, соответствовать техническим требованиям скорости записи, чтение, восстановление данных и многим другим условиям. Определить оптимальное решение очень сложно, особенно учитывая широкий спектр существующих способов внедрения систем хранения и резервного копирования, а также довольно высокую динамику изменения цен и появление новых технологий на ИТ-рынке.

Резервное копирование в глазах большинства специалистов все еще не является достаточно надежным. 45% респондентов заявили, что в примерно 10% случаях испытывали неудовлетворительный результат при использовании всякого рода систем резервного копирования, причем по сравнению с данными опроса 2004 года этот показатель удвоился [6].

Отчасти это объясняется неверным выбором инструментов. По данным компании ШС, причиной 40% случаев полной утраты данных американскими компаниями является пренебрежительное отношение к технологиям хранения. При этом только 10% из этих организаций смогли вернуться к работе и лишь 4% из них выжили в течение последующих трех лет [6].

Действительно, построение высокоэффективной системы хранения данных, отвечающих реальным требованиям организации, а также выбор наиболее подходящей системы резервного копирования - процесс весьма сложный и трудоемкий.

Актуальность исследования. Создание системы резервного копирования является немаловажной задачей при построении ИТ-инфраструктуры и реализации политики информационной безопасности организации профессионального образования. Но почему-то важность резервирования данных многие осознают только после потери критически важной информации.

Анализ состояния проблемы информационной безопасности в организациях профессионального образования позволил выявить *противоречие* между целесообразностью использования комплексных мер при реализации политики ИБ образовательного учреждения и недостаточной защищенностью от потери или искажения данных.

Это определило проблему исследования, заключающуюся в необходимости внедрения системы резервного копирования для реализации политики безопасности в организации профессионального образования. На основе данной проблемы была определена и тема исследования, которая звучит следующим образом: «Внедрение системы резервного копирования

при реализации политики информационной безопасности в организации профессионального образования».

Цель исследования: теоретико-методическое обоснование и разработка плана мероприятий для внедрения системы резервного копирования.

Объект исследования: процесс обеспечения информационной безопасности в организации профессионального образования.

Предмет исследования: внедрение системы резервного копирования.

Гипотеза исследования: внедрение системы резервного копирования позволит повысить уровень информационной безопасности в организации профессионального образования.

Задачи исследования:

- проанализировать понятие, назначение, функции и особенности систем резервного копирования;
- выявить методы организации системы резервного копирования;
- выбрать средства, наиболее подходящие для реализации систем резервного копирования в организации профессионального образования;
- разработать план внедрения системы резервного копирования;
- разработать методические рекомендации работникам организации профессионального образования для эффективной работы системы резервного копирования данных.

Методологическая основа исследования: работы Давлетханов М. «Новое слово в корпоративном резервном копировании», В.Г. Казаков, С.А. Федосин «Технологии и алгоритмы резервного копирования», Дорофеев А.В. «Менеджмент информационной безопасности»

Методы исследования: изучение и анализ методической и специальной литературы в области информационной безопасности; изучение и анализ документации по организации систем резервного копирования; изучение интернет-ресурсов по проблеме исследования; методы логического структурирования материала.

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж».

Практическая значимость исследования заключается в:

а) анализе имеющихся на рынке систем резервного копирования и выборе наиболее подходящей для внедрения в систему информационной безопасности ГБПОУ "Южно-Уральский государственный технический колледж";

б) возможности применения данной системы резервного копирования в других учебных заведениях СПО.

Структура работы: диссертация содержит введение, две главы, выводы по главам, заключение, библиографический список и приложение.

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СИСТЕМ РЕЗЕРВНОГО КОПИРОВАНИЯ

1.1. Понятие, назначение, функции и особенности систем резервного копирования

Основные понятия, использованные в исследовании

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Политика информационной безопасности – набор законов, мероприятий, правил, требований, ограничений, инструкций, нормативных документов, рекомендаций и т.д., регламентирующих порядок обработки информации и направленных на защиту информации от определенных видов угроз.

Резервное копирование (англ. backup copy) — процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Система резервного копирования – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления.

Стратегия резервного копирования - одна или несколько операций резервного копирования данных.

Назначение систем резервного копирования

Система резервного копирования предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

Система резервного копирования является одним из необходимых методов обеспечения непрерывности деловых процессов. По данным Gartner, среди компаний, пострадавших от катастроф и переживших крупную необратимую потерю корпоративных данных, 43% не смогли продолжить свою деятельность.

Централизованная система резервного копирования имеет многоуровневую архитектуру. Она включает:

- Сервер управления резервным копированием. Сервер управления резервным копированием может совмещать функции сервера копирования данных.
- Один или несколько серверов копирования данных, к которым подключены устройства резервного копирования.
- Компьютеры-клиенты с установленными на них программами-агентами резервного копирования.
- Консоль администратора системы резервного копирования.

Функции и особенности систем резервного копирования

Что обеспечит система резервного копирования:

- защиту от потери критически важной информации;
- быстрое восстановление, как отдельных данных, так и всей системы полностью.

Когда может потребоваться восстановление информации:

- сбой оборудования или программного обеспечения;
- ошибочные действия пользователя;
- последствия вирусных атак;
- форс-мажорные ситуации;

Основные функции системы резервного копирования:

- создания резервных копий файлов, баз данных, приложений, системной информации и других необходимых данных;

- восстановление данных в случае утери информации;
- регулярное автоматизированное создание резервных копий на основании политик бэкапа;
- возможность восстановления нескольких версий файлов;
- надежное хранение резервных копий в течение установленного периода времени;
- обеспечение требуемого времени восстановления информации из резервных копий.

К системам хранения резервных данных предъявляются повышенные требования к отказоустойчивости. Если это домашний компьютер, то сохранить альбом семейных фотографий нетронутым, достаточно подключить съемный жесткий диск и дублировать необходимые папки на нем.

Если дело касается баз данных и систем документооборота для крупных предприятий, то вступают в силу абсолютно другие критерии надежности: для этого требуется внедрение отказоустойчивых систем хранения и дублирования, автоматизация или полуавтоматическое удаление ненужной информации (у которой, например, вышел срок хранения, и она больше не представляет ценность для владельцев) и так далее почти до бесконечности.

При внедрении данных технологий желательно максимально автоматизировать резервное копирование с целью минимального вмешательства администраторов и, соответственно, человеческого фактора.

К системам резервного хранения информации применяют три критерия и требования:

- Предельная простота и быстрота внедрения данных технологий в любых масштабах предприятия - от небольшой фирмы до больших корпораций;
- Надежность хранения информации – об этом критерии мы говорили выше;
- Предельная простота и автоматизация эксплуатации внедренных систем.

Различают следующие виды резервного копирования:

- Полное резервное копирование существующей информации (Full backup) – абсолютная копия всей информации, находящейся на машине, будь то хоть компьютер рядового пользователя, хоть сервер компании;
- Дифференциальное резервное копирование (Differential backup) – копирование информации, критичной для порчи или удаления, но не тотальное, как в предыдущем пункте, а выборочное, по определенным пользователем критериям;
- Добавочное резервное копирование (Incremental backup) – когда основной архив резервных копий уже создан, и в него по мере поступления добавляется новая информация или изымается ненужная;
- Пофайловый метод резервного копирования – при данном методе добавление информации в архив осуществляется только по определенным критериям, например, добавляются только файлы определенного формата;
- Блочное инкрементальное резервное копирование (Block level incremental) – при данном методе копирования добавление новой информации в уже существующие архивы осуществляется путем добавки к исходному нескольких блоков вновь созданных архивов.

Как можно хранить резервые копии информации:

- Магнитные ленты стримеров;
- Компакт-диски;
- Резервирование через специальные службы провайдеров (некоторые провайдеры предоставляют такие услуги);
- Запись критичных данных по локальной сети на любую машину, входящую в данную сеть;
- Жесткие диски компьютеров;
- Заливка нужной информации на различные FTP-серверы (лучше всего конечно не на публичные, а на собственные или арендованные);

- Запись информации на USB-устройства – внешние жесткие диски, флешки и т.д.

Почему же может потеряться та или иная информация, спросите Вы? Ну, причин может быть несколько. Постараемся сейчас их описать.

Это может быть и поломка оборудования вследствие его износа или заводского брака, вследствие случайной его механической поломки или скачка напряжения в сети. А как же с этим бороться? Да довольно элементарно: рекомендуется просто установить RAID-массив, или периодически вручную копировать нужную информацию на другие носители.

Потеря информации возможна вследствие непреодолимых обстоятельств – разгул стихии, землетрясение. Так что и нужно предусмотреть возможность восстановления информации вследствие всего этого. Лучше всего хранить информацию которую Вы зарезервировали, в другом помещении.

Если же информация повредилась в результате вирусной атаки или действия вредоносного программного обеспечения, нужно установить хорошую антивирусную защиту на все компьютеры, входящие в локальную сеть, и периодически обновлять антивирусные базы сигнатур. При этом нужно еще и хранить копии важной информации в таком месте, до которого вредоносное программное обеспечение даже теоретически добраться не сможет.

При сбое или уничтожении информации по вине человеческого фактора нужно тщательнейшим образом распределить все права доступа к ресурсам в сети, организовать регулярное резервное копирование информации, и регулярно обновлять используемое на компьютерах программное обеспечение.

1.2 Методы организации системы резервного копирования

Защита данных (к которым можно отнести и установленное программное обеспечение) от удаления или искажения задача непростая даже при отсутствии преднамеренных действий со стороны злоумышленников. Как правило, для ее решения требуется использовать комплекс программно-технических мер, основными из которых являются:

- резервное копирование данных;
- продуманная настройка и поддержание требуемых («безопасных») значений системных параметров;
- заблаговременная установка и освоение специализированных программных средств восстановления данных.

Приведенные меры обязаны быть предоставлены на этапе разработки политики безопасности организации и отражены в соответствующих нормативных документах (в документе о политике безопасности, в личных инструкциях структурных подразделений и в обязанностях исполнителей). Резервное копирование можно рассматривать как панацею практически во всех ситуациях, связанных с потерей или искажением данных. Однако подлинно универсальное резервное копирование происходит только в том случае, если вы следуете правилам его применения.

Резервное копирование обычно осуществляется в соответствии с одним из трех основных методов: ***полным, инкрементальным и дифференциальным***.

При использовании полного резервирования каждый раз производится копирование всего набора данных. Например, копируется вся файловая система, база данных или указанный каталог на диске. Этот метод требует много времени для записи и приводит к большому расходу резервного носителя. С другой стороны, в этом случае восстановление информации происходит быстрее, чем с любым другим методом, поскольку резервная

копия соответствует текущему состоянию всего набора данных (с учетом периодичности копирования). Полное копирование является наиболее привлекательным решением при резервном копировании системной информации и служит отправной точкой для других методов.

Инкрементальный (или добавочный) метод основан на последовательном частичном обновлении резервной копии. На первом этапе создается полная копия набора данных. Последующие сеансы резервного копирования разделяются на два вида: частичное копирование и полное. При очередном частичном копировании на резервный носитель помещаются только файлы, которые были модифицированы по сравнению с предыдущей частичной копией (на рис. схематично показана процедура инкрементального резервного копирования для недельного цикла). Модифицированными считаются файлы, у которых изменились содержание, атрибуты или права доступа. По истечении определенного пользователем времени (или системным администратором) полная копия создается снова, а затем цикл повторяется. Этот метод является самой быстрым с точкой зрения создания промежуточных копий и приводит к минимальному потреблению резервного носителя.

Однако процедура восстановления занимает много времени: информацию сначала требуется восстановить с полной копии, а затем последовательно со всех частичных (инкрементальных) копий. Тем не менее, это самый популярный метод резервного копирования.

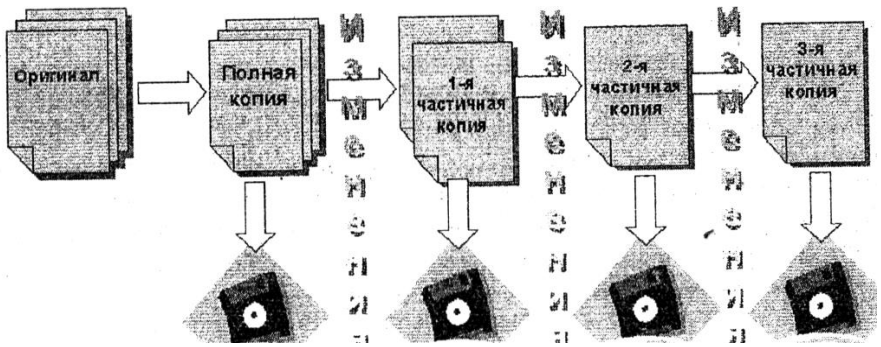


Рис 1. Схема инкрементального резервного копирования для недельного цикла

При дифференциальном (разностном) способе на первом шаге также формируется абсолютная копия. На следующих шагах копируются только файлы, модифицированные со времени проведения полного копирования (на рис.2 приведена схема дифференциального резервного копирования для еженедельного цикла). Через данный интервал времени возобновляется полный цикл, то есть опять формируется абсолютная резервная копия набора данных. По сравнению с инкрементальным способом, дифференциальное копирование требует больше времени на создание выборочной (дифференциальной) копии, но восстановление информации производится быстрее, так как используются лишь 2 копии: абсолютная и последняя дифференциальная.

Основной проблемой инкрементального и дифференциального копирования является проблема выбора достоверного аспекта модификации файла. Традиционно в качестве такового выступает атрибут Archive (для систем DOS/Windows), время создания/модификации файлов, размер файла либо контрольная сумма содержимого файла. К огорчению, все они имеют те либо другие недочеты, связанные с особенностями обработки атрибутов и прав доступа отдельными прикладными программами.

Некоторые из современных средств резервного копирования предлагают принципиально иной подход к созданию резервных копий, который иногда называют копированием «на лету». Его идея заключается в том, что любые изменения файлов, заданные пользователем при настройке программы, немедленно переносятся в резервную копию. При очевидной простоте метода он имеет ряд недостатков. Главное, что внесенные изменения могут быть вызваны ошибочными действиями пользователя или работой вредоносных программ. В результате может оказаться невозможным вернуться к «правильной» версии файла.

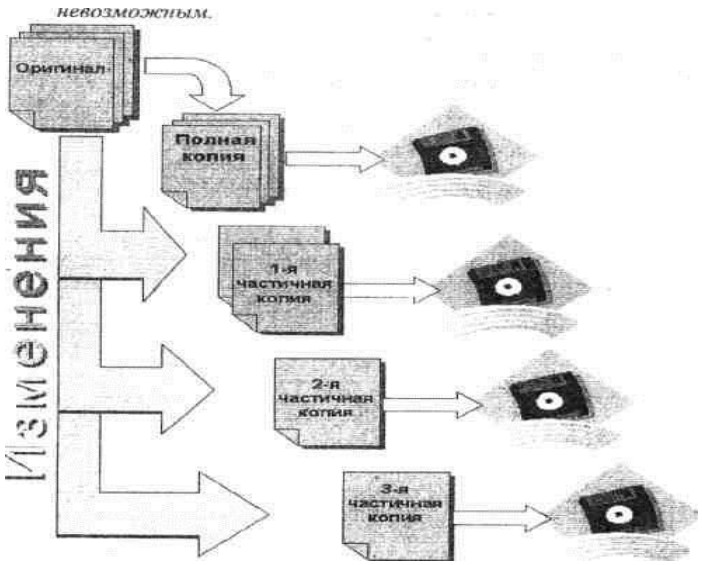


Рис 2. Схема дифференциального резервного копирования для недельного цикла

Иная проблема связана с выбором периодичности создания выборочных копий и численностью таковых копий в течение полного цикла.

С одной стороны, чем чаще производится копирование, тем наиболее «свежая» информация будет храниться в виде резервной копии. С иной стороны, для каждого сеанса резервного копирования потребуются дополнительные издержки: время и резервный носитель.

Для оптимизации числа используемых резервных носителей разработаны специальные алгоритмы замены носителей (так называемые *схемы* ***ротации носителей).*** Наиболее часто используют следующие схемы:

- одноразовое копирование;
- «дед, отец, сын»;
- простая ротация;
- «10 наборов».
- «Ханойская башня»;

Одноразовое копирование - это наиболее простая схема, которая, по сути, вообще не предусматривает ротации носителей. При ее использовании резервируемые данные каждый раз копируются на один и тот же перезаписываемый носитель (например, на дискету или на CD-RW). Другой вариант применения такой схемы - когда очередная копия данных

помещается на новый не перезаписываемый носитель (например, на CD-R). Такая схема обычно используется в тех случаях, когда объем резервируемых данных невелик, либо когда резервирование не носит регулярного характера (например, когда создается единственная резервная копия системы на CD-R).

Простая ротация подразумевает, что некий набор носителей используется циклически. Например, цикл ротации может составлять неделю, и тогда один носитель выделяется для определенного рабочего дня недели. При такой схеме полная копия обычно делается в пятницу, а в другие дни - частичные копии (инкрементальные или дифференциальные). Таким образом, для недельного цикла достаточно иметь пять носителей. По окончании цикла все повторяется сначала, и запись выполняется на том же носителе. Недостатком этой схемы является то, что она не очень подходит для архивирования полных копий, так как количество носителей в архиве быстро растет. Кроме того, достаточно частая перезапись частичных копий на одном носителе приводит к ухудшению последних и, соответственно, увеличивает вероятность их отказа.

Методика «дед, отец, сын» имеет иерархическую структуру и подразумевает использование набора из 3-х комплектов носителей. Раз в неделю делается абсолютная копия дисков компьютера, раз в день ведется инкрементальное (дифференциальное) копирование. Дополнительно раз в месяц производится еще одно полное копирование. Набор для каждодневного инкрементального копирования называется «сыном», для недельного - «отцом», а для ежемесячного - «дедом». Состав носителей в каждодневном и недельном наборах считается неизменным. При этом в каждодневном наборе любой носитель соответствует конкретному дню недели, а в недельном наборе – каждой неделе месяца. Носители из «ежемесячного» набора обычно заново не используются и откладываются в архив. Недостаток предоставленной схемы состоит в том, что в архиве пребывают лишь данные, имевшиеся на конец месяца. Как и при простой

ротации, каждодневные копии подвергаются значительному износу, в то время как нагрузка на недельные копии сравнимо мала.

Методика «Ханойская башня» изредка употребляется пользователями «домашних» компьютеров. Она построена на использовании нескольких наборов носителей. Их численность никак не регламентируется, однако традиционно ограничивается пятью-шестью. Любой набор специализирован для еженедельного цикла копирования, как в схеме простой ротации. Каждый набор охватывает один носитель с полной еженедельной копией и носители с каждодневными инкрементальными (дифференциальными) копиями. На рисунке 3 приведена методика ротации для 5 наборов носителей.

№ набора	Номера недель																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	x		x		x		x		x		x		x		x		x	
2		x				x				x				x				x
3				x								x						
4								x										
5																x		

Рис. 3. Схема ротации «Ханойская башня» для 5 наборов носителей

Каждый следующий по порядку набор используется в два раза реже, чем предыдущий. Таким образом, набор N1 перезаписывается каждые две недели, набор N2 - каждые четыре недели, и т. д.

Методика «10 наборов» также употребляется редко. Как следует из наименования, методика рассчитана на внедрение 10 наборов носителей. Период из 40 недель распределяется на 10 циклов. В пределах цикла за любым набором прикреплен один день недели. По прошествии четырехнедельного цикла исполняется переход к последующему набору. К примеру, если в первом цикле понедельнику соответствовал набор 1, а за вторник - набор 2, то во втором цикле понедельнику станет соответствовать

набор 2, а вторнику - набор 3. Такая методика позволяет умеренно разделить нагрузку и, как следствие, выровнять износ носителей.

Программно-технические средства резервного копирования

Существующие в настоящее время программы резервного копирования избавляют пользователей и системных администраторов от необходимости «вручную» отслеживать периодичность создания и обновления резервных копий, замены носителей и т. п. Правда, перечень предоставляемых такими программами сервисных возможностей существенно зависит от категории программы. Все программы резервного копирования можно условно разделить на три категории:

- Системы начального уровня, включаемые в состав операционных систем. К ним можно также отнести большинство бесплатных и условно- бесплатных программ резервного копирования. Эти программы предназначены для индивидуальных пользователей и небольших Организаций.
- Системы среднего уровня; при относительно невысокой цене они обладают широкими возможностями по резервному копированию и архивации данных. Подобных систем довольно много (в частности, ARCserveIT компании Computer Associates, Backup Exec от Seagate Software и Net Worker компании Legato Systems).
- Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интеграции с системами управления сетью и обеспечивают возможность резервного копирования/архивирования с использованием разнообразных типов накопителей. К подобным системам можно отнести ADSM компании ЮМ и OpenView OmniBack II от Hewlett Packard. Однако для многих

организаций (не говоря уже об индивидуальных пользователях) они весьма дороги.

Одной из важных характеристик программ резервного копирования является перечень поддерживаемых типов сменных носителей.

Вместе с тем, при создании резервной копии в «ручном» режиме, вы вольны использовать любое из существующих на сегодняшний день устройств хранения данных. Их перечень с краткой характеристикой приведен в табл.

Таблица 1

«Устройства хранения данных, применяемые при резервном копировании»

Тип устройства	**Достоинства**	**Недостатки**
Жесткий диск (HDD)	емкость, быстродействие, высокая надежность, долговечность, многократная перезапись, низкая стоимость, возможность загрузки резервной копии	Ненадежность при транспортировке, воздействие ЭМ излучений, (подключение ..)
CD-R, CD-RW	Приемлимое быстродействие и скорость , н. стоимость, надежность, долговечность	Емкость, Не все виды ПК оснащены
DVD	Большая емкость, тоже что CD …	Специализация, Не все виды ПК оснащены
Карты памяти SD, MS, (CF), MMC,…	Емкость, скорость, надежность, Приемлимое быстродействие и скорость, возможность использования для переноса м-ду разнотипными устр	
Модули флеш памяти	То же	
Внешний жесткий диск	USB	

Mobile Rack, Стример, флоппи, ZIP, ZIV, магнитооптические		

Краткие итоги сравнительной оценки параметров представленных в таблице носителей.

Та или иная схема ротации может быть реализована только для устройств со сменными носителями, к числу которых относятся оптические (CD и DVD) (и магнитооптические диски). При этом для «среднестатистического» пользователя один носитель емкостью в несколько

гигабайт явно «великоват» для хранения одной копии данных. Единственное исключение - когда речь идет о создании образа целого раздела жесткого диска.

Таким образом, по совокупности характеристик оптимальным вариантом на сегодняшний день можно считать резервное копирование на базе перезаписываемых оптических дисков (CD или DVD).

Относительно использования жесткого диска в качестве резервного носителя необходимо сделать несколько дополнительных замечаний.

Первое: если имеется необходимость хранить жесткий диск с резервной копией данных отдельно от компьютера, на котором они создавались, то целесообразно использовать (так называемый *переносной диск* (Mobile Rack) жесткий диск с USB интерфейсом. .

Второе: если ваш компьютер работает под управлением операционной системы Windows XP Professional, и на нем установлены как минимум два жестких диска, вы можете использовать отказоустойчивые технологии RAID-1 и RAID-5.

Третье: при наличии единственного жесткого, диска достаточно большой емкости целесообразно разбить его на несколько логических разделов, один из которых (по крайней мере) может быть использован в качестве резервного диска; такой логический резервный диск будет защищен

от многих напастей, грозящих «рабочим» разделам (хотя, разумеется, далеко не от всех);

Технология RAID

В достаточно крупных организациях для резервного копирования критически важных данных применяется технология RAID (Redundant Array of Independed Disks - избыточный массив независимых дисков), основанная на системе специальным образом сконфигурированных жестких дисков. Исходной целью создания технологии RAID являлось повышение производительности дисковой памяти за счет использования нескольких взаимосвязанных жестких дисков вместо одного.

Всего на сегодняшний день промышленными стандартами предусмотрено восемь уровней (модификаций) RAID:

- RAID-0- объединение пространства нескольких физических дисков в один виртуальный том, для которого применяется метод чередования (striping, от strip - «полоса»): информация делится на блоки, поочередно записывающиеся на все накопители тома (рис. 4.3). RAID-0 обеспечивает высокую скорость обмена данных, но надежность виртуального тома несколько ниже, чем у любого другого уровня и ниже надежности каждого из входящих в том дисков, так как при выходе из строя хотя бы одного из них вся информация теряется.
- RAID-1 - дублирование, или «зеркалирование» (mirroring-зеркальное отражение) дисков. В этом случае информация одновременно записывается на два (как правило) диска. При выходе из строя одного из них данные считываются с «зеркала». К этому уровню относят также применение дуплексных томов (Duplex Volume), когда физические диски, используемые в качестве зеркал, обязательно должны быть подключены к разным контроллерам. Реализация восстановления после сбоев при использовании RAID-1 достаточно проста, однако имеет место высокая (100%) избыточность.

- RAID-2 - предполагает создание на основе нескольких физических дисков одного массива (тома), данные в который записываются с использованием контрольного кода (кода Хемминга). Для хранения контрольных кодов отводится специально выделяемый диск.
- RAID-3 - массив с чередованием и использованием кода четности для обнаружения ошибок. Информация о четности, как и в случае RAID-2, хранится на отдельном диске, но имеет меньшую избыточность.
- RAID-4 - подобен уровню 3, но данные разбиваются на блоки, записывающиеся на разные диски, причем возможно параллельное обращение к нескольким блокам, что существенно повышает производительность.
- RAID-5 - аналогичен уровню 4, но информация о четности хранится не на выделенном диске, а циклически распределяется между всеми дисками тома.
- RAID-6 - в отличие от уровня 5, использует две независимые схемы четности, что увеличивает как избыточность, так и надежность хранения информации.
- RAID-7 - отказоустойчивый массив, оптимизированный для повышения производительности. Данный уровень RAID поддерживается лишь специализированными ОС.

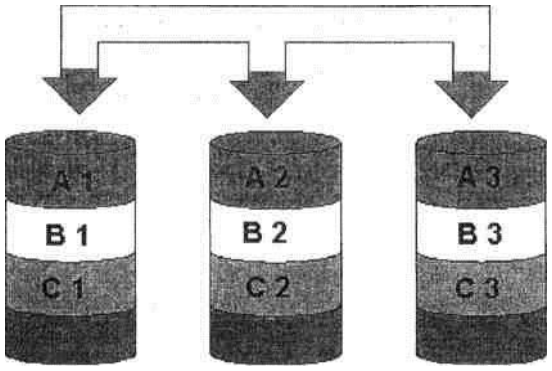


Рис 4. Схема использования RAID-0

Технология RAID на сегодняшний день реализуется как на аппаратном уровне, так и программно.

Аппаратная реализация является более эффективной и основана на подключении жестких дисков через специальные RAID-контроллеры. Такой контроллер выполняет функции связи с сервером (рабочей станцией), генерации избыточной информации при записи и проверки при чтении, распределения информации по дискам в соответствии с алгоритмом функционирования.

Принцип работы программно управляемого тома RAID-1 состоит в следующем. На основе двух разделов, расположенных на двух разных физических дисках, создается так называемый зеркальный том (Mirror Volume). Ему присваивается собственная буква диска (исходные разделы дисков лишаются таковой вообще), и при выполнении каких-либо операций над данными этого тома все изменения синхронно отражаются в обоих исходных разделах. При выходе из строя (отказе или сбое) одного из двух дисков система автоматически переключается на работу с оставшимся в живых «последним героем». При возникновении такой ситуации пользователь может разделить зеркала, и затем объединить исправный раздел с другим разделом в новый зеркальный том. В зеркальный том можно включить практически любой раздел, в том числе системный и загрузочный.

1.3 Анализ стратегий резервного копирования

В большинстве случаев стратегия резервного копирования должна предусматривать некоторый тип ежедневного резервного копирования и полного резервного копирования как минимум раз в неделю. Также необходимо регулярно проверять файлы журналов резервного копирования и выполнять тестовые восстановления данных, чтобы быть уверенными, что данные на носителях корректно записаны.

Большая часть стратегии резервного копирования зависит от важности данных, частоты их изменения и суммарного объема данных, резервное копирование которых надо выполнять. Данные с более высокой важностью или данные, которые часто изменяются, должны копироваться чаще, чем другие данные. По мере увеличения объемов копируемых данных необходимо масштабировать решения по реализации резервного копирования. Если сразу имеются большие объемы данных, то необходимо определить, сколько времени займет их резервное копирование. Чтобы гарантировать, что резервное копирование пройдет за необходимое время, возможно, придется приобрести более быстрое оборудование или устройства резервного копирования с несколькими ленточными накопителями.

Необходимо планировать отдельно резервное копирование системных файлов и файлов данных.

Системные файлы используются операционной системой и приложениями.

Эти файлы изменяются, только когда устанавливаются новые компоненты, пакеты обновлений или заплатки. Системные файлы содержат данные о состоянии системы.

Для систем, которые не являются контроллерами домена, данные состояния системы включают важные загрузочные файлы, ключевые системные файлы и базу данных регистрации классов COM+, а также данные реестра. Для контроллеров домена данные состояния системы также включают базу данных Active Directory и файлы системного тома (SysVol).

Файлы данных создаются приложениями и пользователями. Файлы приложений содержат параметры конфигурации и данные. Файлы пользователей содержат результат их ежедневной работы и могут включать документы, электронные таблицы, мультимедиа-файлы и т. д. Эти файлы изменяются каждый день.

Администраторы часто выполняют полное резервное копирование всей машины на один носитель резервной копии. С такой стратегией связано несколько проблем. Во-первых, системные файлы не изменяются часто в отличие от файлов данных. Во-вторых, обычно файлы данных надо восстанавливать чаще, чем системные файлы. Файлы данных восстанавливаются при повреждении, потере или случайном удалении. Системные файлы надо восстанавливать, когда существуют серьезные проблемы с системой; обычно в этом случае выполняется восстановление всей машины.

Также необходимо следить за временем выполнения резервного копирования. В Microsoft Windows 2000 и более ранних версиях операционных систем Microsoft Windows приходилось заботиться о том, в какой момент выполняется резервное копирование. Резервное копирование должно было выполняться, когда использование системы было низким, так как в это время доступно больше ресурсов и меньше файлов заблокированы и используются. В Windows Server 2003 встроена усовершенствованная технология резервного копирования Shadow Copy API, так что теперь на время резервного копирования можно, обращать меньше внимания, чем раньше. Все программы, реализованные с использованием Shadow Copy API, позволяют выполнять резервное копирование файлов, которые открыты и заблокированы. Это означает, что можно выполнять резервное копирование даже тогда, когда файлы используются приложениями, и не заботиться о сопутствующих проблемах.

Когда дело доходит до резервного копирования, не существует универсального решения, подходящего во всех случаях. Обычно для одной системы реализуется одна стратегия, для другой - другая. Все зависит от важности данных, частоты их изменения и объема данных, резервное

копирование которых надо выполнять. Не нужно также забывать о важности скорости восстановления. Для разных стратегий резервного копирования требуется разное время восстановления.

Ключевые службы, работающие в системе, имеют уникальные функции резервного копирования. Используйте эти механизмы резервного копирования в качестве первой линии обороны на случай аварии. Помните, что резервное копирование состояния системы (System State) включает полное копирование реестра сервера и что конфигурация сервера включает конфигурацию всех служб, работающих в системе. Однако если какая-то служба перестанет функционировать, намного проще и быстрее восстановить эту конкретную службу, чем пытаться восстановить весь сервер. У вас будет меньше проблем и меньше вероятность того, что что-то пойдет не так.

Для ключевых служб существуют следующие методы резервного копирования и восстановления:

Для DHCP вы должны периодически выполнять резервное копирование конфигурации и базы данных DHCP, как описывается в разделах «Сохранение и восстановление конфигурации DHCP» и «База данных DHCP: управление и обслуживание».

Для DNS ваша стратегия резервного копирования будет зависеть от того, какие зоны вы используете - зоны, интегрированные в Active Directory, стандартные зоны или и те, и другие. При использовании зон, интегрированных в Active Directory, конфигурация DNS хранится в Active Directory. По умолчанию при использовании стандартных зон конфигурационные данные DNS хранятся в папке %SystemRootOfo\System32\DNS, а резервные копии - в папке %System Root% \System32\DNS\Ьackup.

Для групповой политики вы должны периодически выполнять резервное копирование конфигурации объекта групповой политики (group policy object, GPO), как рассказывается в разделе «Обслуживание групповой политики и решение проблем».

Для серверов печати вы должны периодически выполнять резервное копирование конфигурации принтеров, как рассказывается в разделе «Подготовка к выходу из строя сервера печати».

Для файловых серверов вы должны использовать теневое копирование томов (Volume Shadow Copy) всех общих сетевых папок. Это облегчит восстановление предыдущих версий Файлов. Дополнительно вы должны выполнять регулярное резервное копирование всех Файлов пользователей на Файловом сервере.

Методы подготовки к авариям, описанные в разделе «Процедуры подготовки к аварии» - это ваша следующая линия обороны. Для каждой системы должно быть предусмотрено периодическое резервное копирование (ASR), а также загрузочный диск. Таким образом, вы сможете восстановить систему до возможности загрузки и решить проблемы с загрузкой без необходимости восстанавливать систему с нуля.

И, наконец, вы должны выполнять резервное копирование системных и пользовательских данных. Большинство программ для резервного копирования, включая Windows Backup, которая входит в состав Windows Server 2003, поддерживают несколько видов резервного копирования. Тип резервного копирования определяет, как много данных будет копироваться и что будет делать программа при выполнении резервного копирования.

Большинство операций резервного копирования используют атрибут архивации, который может быть установлен для файлов. Атрибут архивации файла может быть включен или выключен для каждого файла. В большинстве случаев программа резервного копирования будет отключать (очищать) атрибут архивации при выполнении резервного копирования. Бит архивации включается (устанавливается) снова, когда позже операционная система или пользователь модифицируют файл. Когда программа резервного копирования снова запустится, она будет знать, что должны быть скопированы только файлы с атрибутом архивации, потому что только эти файлы изменились

Выводы по главе I

В ходе работы с научно-методологической литературой была подтверждена необходимость внедрения системы резервного копирования при реализации политики информационной безопасности.

Дано определение понятия «система резервного копирования» и выделены её основные функции. *Система резервного копирования* – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления и выполняющий следующие функции:

- защиту от потери критически важной информации;
- быстрое восстановление, как отдельных данных, так и всей системы полностью.

Выявлены методы организации систем резервного копирования:

- полный;
- инкрементальный;
- дифференциальный.

Также проанализированы и описаны программно-технические средства резервного копирования.

ГЛАВА II ВНЕДРЕНИЕ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ В ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.

2.1 Выбор средств реализации систем резервного копирования в организации профессионального образования

В процессе выполнения резервного копирования данных появляется проблема выбора технологии хранения резервных копий и данных. В настоящее время особой популярностью пользуются следующие виды носителей:

1) накопители на магнитных лентах;
2) сетевые технологии;
3) дисковые накопители.

Накопители на магнитных лентах

Не только в крупных корпорациях, но и на предприятиях малого бизнеса хорошо понимают необходимость резервного копирования и восстановления информации. В системах масштаба предприятия и сетях крупных департаментов, в небольших компаниях и у индивидуальных пользователей одинаковым успехом пользуются потоковые накопители, или стримеры. В основе их конструкции лежит лентопротяжный механизм, работающий в инерционном режиме. Имеют низкую стоимость хранения информации. Основная проблема при использовании накопителей на магнитной ленте сегодня заключается в том, что множество таких устройств использует несовместимые друг с другом форматы записи данных на магнитной ленте. Это часто затрудняет не только выбор конкретного накопителя, но и обмен данными при его эксплуатации. Предпринято немало усилий для решения этой проблемы, но в целом можно констатировать, что кардинальных перемен пока не произошло (хотя некий прогресс в этом направлении есть) Наиболее широко сегодня применяются такие технологии, как Travan, DLT (Digital Linear Type), DAT-DDS (Digital Audio Tape – Digital Data Storage), LTO (Linear Tape Open), Mammoth и AIT (Advanced Intelligent

Tape). Для обоснованного выбора системы резервного копирования надо ясно представлять себе достоинства и недостатки разных устройств, которые во многом определяются емкостью системы, ее быстродействием, надежностью и ценой. Основные стимулы к повышению производительности ленточных устройств среднего и старшего класса – это широкое использование Интернета и распространение корпоративных интрасетей, увеличение числа серверов (нужных, чтобы обеспечить рост этих сетей), а также ужесточение требований к хранению информации и ее восстановлению в случае аварий. Спрос на системы резервного копирования и хранения данных особенно подстегивается все более активным использованием таких приложений, как мультимедиа, видео по запросу, звуковое информационное наполнение, обработка изображений и т.п. Применяются два метода записи на магнитную ленту: наклонный и линейный серпантинный. В системах наклонной записи несколько считывающих / записывающих головок размещают на вращающемся барабане, установленном под углом к вертикальной оси (аналогичная схема применяется в бытовой видеоаппаратуре). Движение ленты при записи / чтении возможно только в одном направлении. В системах линейной серпантинной записи считывающая / записывающая головка при движении ленты неподвижна. Данные на ленте записываются в виде множества параллельных дорожек (серпантина). Головка размещается на специальной подставке; по достижении конца ленты она сдвигается на другую дорожку. Движение ленты при записи / чтении идет в обоих направлениях. На самом деле таких головок обычно устанавливается несколько, чтобы они обслуживали сразу несколько дорожек (они образуют несколько каналов записи / чтения).

Плюсы хранения данных на ленточном носителе:

1) низкая стоимость;
2) низкое энергопотребление накопителя;
3) большие объемы данных;

4) простой способ увеличения объема хранимых данных без значительных инвестиций.

Минусы хранения данных на ленточном носителе:

1) низкая скорость доступа к данным;

2) сложный процесс обработки параллельных запросов к данным.

Сетевые технологии

Сетевое хранение данных построено на трех фундаментальных компонентах: коммутации, хранении и файлах. Все продукты хранения можно представить в виде комбинации функций данных компонентов. Поначалу это может вызвать замешательство: поскольку продукты хранения разрабатывались по совершенно разным направлениям, функции часто перекрывают друг друга.

В сети работает множество приложений типа «клиент-сервер» и различных видов распределенных приложений, но в то же время хранение является уникальным и специализированным типом приложения, которое может функционировать в нескольких сетевых средах. Поскольку процессы хранения тесно интегрированы с сетями, будет уместно напомнить, что сетевые хранилища представляют собой системные приложения. Сервисами, которые предоставляются сетевыми приложениями хранения, могут пользоваться сложные корпоративные программы и пользовательские приложения. Как и в случае со многими технологиями, некоторые типы систем лучше отвечают требованиям сложных приложений высокого уровня.

Термин «коммутация» применяется ко всему программному и аппаратному обеспечению и к службам, которые обеспечивают транспортировку хранения и управление ею в сетевом хранилище. Сюда входят такие различные элементы, как разводка кабелей, сетевые контроллеры ввода-вывода, коммутаторы, концентраторы, аппаратура выборки адресов, контроль связи данных, транспортные протоколы, безопасность и резервы ресурсов. В сетевых хранилищах все еще широко

используются технологии шин данных SCSI и ATA, и, скорее всего, они будут использоваться еще долго. Фактически продукты SCSI и ATA сегодня применяются гораздо чаще в технологии NAS. Существуют два важных различия между сетями хранения SAN и обычными локальными сетями LAN. Сети хранения SAN автоматически синхронизируют данные между отдельными системами и хранилищами. В сетевых хранилищах необходимы компоненты высокой степени точности для обеспечения надежной и предсказуемой среды. Несмотря на ограничения по расстоянию, параллельная SCSI – чрезвычайно надежная и предсказуемая технология. Если новые технологии коммутации, такие как FibreChannel, Ethernet и InfiniBand, сменят SCSI, они должны будут продемонстрировать аналогичный или лучший уровень надежности и предсказуемости. Имеется и такая точка зрения, которая рассматривает коммутацию как канал хранилища. Сам термин «канал», берущий свое начало в среде больших вычислительных машин, предполагает высокую надежность и работоспособность.

Хранение в основном затрагивает блочные операции адресного пространства, включая создание виртуальной среды, когда адреса логического блока хранения отображаются из одного адресного пространства в другое. Вообще говоря, в сетевых хранилищах функция хранения почти не изменилась, если не считать двух заметных отличий. Первое – это возможность нахождения технологий виртуализации устройства, например управление устройством внутри оборудования сетевого хранения. Этот вид функции иногда называют контроллером домена хранения или виртуализацией LUN. Второе главное отличие хранения заключается в масштабируемости. Продукты хранения, такие как подсистемы хранения, имеют значительно больше контроллеров / интерфейсов, чем предыдущие поколения шинной технологии, а также намного больший объем хранения.

Функция организации файлов представляет абстрактный объект конечному пользователю и приложениям, а также организует разметку

данных на реальных или виртуальных устройствах хранения. Основную часть функциональности файлов в сетевых хранилищах обеспечивают файловые системы и базы данных; их дополняют приложения управления хранением, например, операции резервного копирования, также являющиеся файловыми приложениями. Сетевое хранение к настоящему времени почти не изменило файловые функции, за исключением разработки файловых систем NAS, в частности файловой системы WAFL компании NetworkAppliance. Кроме упомянутых технологий хранения данных NAS и SAN, ориентированных на крупные и глобальные сети, в небольших локальных сетях доминирующее положение занимает технология DAS, в соответствии с которой хранилище находится внутри сервера, обеспечивающего объем хранилища и необходимую вычислительную мощность.

Простейшим примером DAS может служить накопитель на жестком диске внутри персонального компьютера или ленточный накопитель, подключенный к единственному серверу. Запросы ввода-вывода (называемые также командами или протоколами передачи данных) непосредственно обращаются к этим устройствам. Однако такие системы плохо масштабируются, и компании с целью расширения объема хранилища вынуждены приобретать дополнительные серверы. Эта архитектура очень дорогая и может использоваться только для создания небольших по объему хранилищ данных.

Дисковые накопители

Существует два наиболее часто встречающихся вида дисковых накопителей: накопители на жёстких магнитных дисках и накопители на оптических дисках.

Накопители на жестких магнитных дисках (HardDiskDrive, HDD) являются основными устройствами оперативного хранения информации. Для современных одиночных накопителей характерны объемы от сотен мегабайт

до нескольких гигабайт при времени доступа 5–15 мс и скорости передачи данных 1–10 Мбайт/с. Относительно корпуса сервера различают внутренние и внешние накопители. Внутренние накопители существенно дешевле, но их максимальное количество ограничивается числом свободных отсеков корпуса, мощностью и количеством соответствующих разъемов блока питания сервера. Установка и замена обычных внутренних накопителей требует выключения сервера, что в некоторых случаях недопустимо. Внутренние накопители с возможностью «горячей» замены (HotSwap) представляют собой обычные винчестеры, установленные в специальные кассеты с разъемами. Кассеты обычно вставляются в специальные отсеки со стороны лицевой панели корпуса, конструкция позволяет вынимать и вставлять дисководы при включенном питании сервера. Для стандартных корпусов существуют недорогие приспособления (MobileRack), обеспечивающие оперативную съемность стандартных винчестеров. Внешние накопители имеют собственные корпуса и блоки питания, их максимальное количество определяется возможностями интерфейса. Обслуживание внешних накопителей может производиться и при работающем сервере, хотя может требовать прекращения доступа к части дисков сервера.

Для больших объемов хранимых данных применяются блоки внешних накопителей – дисковые массивы и стойки, представляющие собой сложные устройства с собственными интеллектуальными контроллерами, обеспечивающими, кроме обычных режимов работы, диагностику и тестирование своих накопителей. Более сложными и надежными устройствами хранения являются RAID-массивы (Redundant Array of Inexpensive Disks – избыточный массив недорогих дисков). Для пользователя RAID представляет собой один (обычно SCSI) диск, в котором производится одновременная распределенная избыточная запись (считывание) данных на несколько физических накопителей (типично 4–5) по правилам, определяемым уровнем реализации (0–10).

Устройства считывания компакт-дисков CD-ROM расширяют возможности системы хранения данных NetWare. Существующие накопители обеспечивают скорость считывания от 150 кбайт/с до 300/600/900/1500 Кбайт/с для 2-, 4-, 6- и 10-скоростных моделей при времени доступа 200–500 мс. NetWare позволяет монтировать компакт-диск как сетевой том, доступный пользователям для чтения. Объем тома может достигать 682 Мбайт (780 Мбайт для Mode 2). Устройства CD-ROM выпускаются с различными интерфейсами, как специфическими (Sony, Panasonic, Mitsumi), так и общего применения: IDE и SCSI. Сервер NetWare обслуживает только CD-ROM с интерфейсами SCSI, новые драйверы существуют и для IDE; устройства со специфическими интерфейсами могут использоваться только в DOS для инсталляции системы. С точки зрения повышения производительности предпочтительнее использование CD-ROM SCSI, однако они существенно дороже аналогичных IDE-устройств. В сервере с дисками SCSI применение CD-ROM с интерфейсом IDE может оказаться невозможным из-за конфликтов адаптеров.

Достоинствами таких накопителей является:

1) быстрый доступ к данным;

2) возможность параллельного доступа к данным без значительной потери скорости.

Недостатки дисковых накопителей:

3) более высокая стоимость чем ленты;

4) более высокое энергопотребление;

5) более дорогое расширение системы хранения данных;

6) невозможность обеспечения высокой безопасности копий.

RAID – массивы

RAID (англ. redundant array of independent disks – избыточный массив независимых дисков) – массив из нескольких дисков (запоминающих устройств), управляемых контроллером, связанных между собой скоростными каналами передачи данных и воспринимаемых внешней

системой как единое целое. В зависимости от типа используемого массива может обеспечивать различные степени отказоустойчивости и быстродействия. Служит для повышения надёжности хранения данных и / или для повышения скорости чтения / записи.

Аббревиатура «RAID» изначально расшифровывалась как «redundant array of independent disks» («избыточный (резервный) массив недорогих дисков», так как они были гораздо дешевле дисков SLED (SingleLargeExpensiveDrive)). Именно так был представлен RAID его создателями Петтерсоном (DavidA. Patterson), Гибсоном (Garth A. Gibson) и Катцом (Randy H. Katz) в 1987 году. Со временем «RAID» стали расшифровывать как «redundant array of independent disks» («избыточный (резервный) массив независимых дисков»), потому что для массивов приходилось использовать и дорогое оборудование (под недорогими дисками подразумевались диски для ПЭВМ).

Калифорнийский университет в Беркли представил следующие уровни спецификации RAID, которые были приняты как стандарт де-факто:

1) **RAID 0** – дисковый массив повышенной производительности с чередованием, без отказоустойчивости;

2) **RAID 1** – зеркальный дисковый массив;

3) **RAID 2** – зарезервирован для массивов, которые применяют код Хемминга;

4) **RAID 3 и 4** – дисковые массивы с чередованием и выделенным диском чётности;

5) **RAID 5** – дисковый массив с чередованием и «невыделенным диском чётности»;

6) **RAID 6** – дисковый массив с чередованием, использующий две контрольные суммы, вычисляемые двумя независимыми способами;

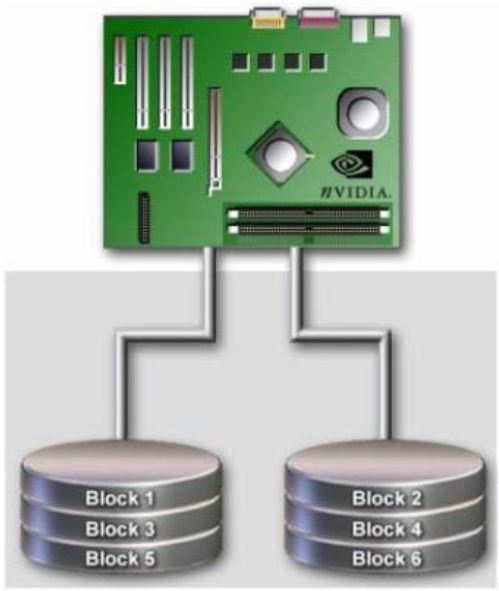
7) **RAID 10** – массив RAID 0, построенный из массивов RAID 1;

8) **RAID 50** – массив RAID 0, построенный из массивов RAID 5;

9) **RAID 60** – массив RAID 0, построенный из массивов RAID 6.

Аппаратный RAID-контроллер может поддерживать несколько разных RAID-массивов одновременно, суммарное количество жёстких дисков которых не превышает количество разъёмов для них. При этом контроллер, встроенный в материнскую плату, в настройках BIOS имеет всего два состояния (включён или отключён), поэтому новый жёсткий диск, подключённый в незадействованный разъём контроллера при активированном режиме RAID, может игнорироваться системой, пока он не будет ассоциирован как ещё один RAID-массив типа JBOD (spanned), состоящий из одного диска. JBOD – данная аббревиатура расшифровывается как «Just a BunchofDisks», то есть просто группа дисков. Данная технология позволяет объединять в массив диски различной емкости, правда, прироста скорости в этом случае не происходит, скорее, даже наоборот.

Расслоение дисков, также известное как режим RAID 0, уменьшает число обращений к дискам при чтении и записи для многих приложений. Данные делятся между несколькими дисками в массиве так, чтобы операции чтения и записи проводились одновременно для нескольких дисков. Этот уровень обеспечивает высокую скорость выполнения операций чтения / записи (теоретически – удвоение), но низкую надежность. Для домашнего пользователя – наверное, самый интересный вариант, позволяющий добиться существенного роста скорости чтения и записи данных с



накопителей.

Рис.5. Схема RAID 0

RAID 1 (mirroring – «зеркалирование») – массив из двух дисков, являющихся полными копиями друг друга. Не следует путать с массивами RAID 1+0, RAID 0+1 и RAID 10, в которых используется более двух дисков и более сложные механизмы зеркалирования.RAID 1 предназначен для тех, кто хочет легко резервировать наиболее важные данные. Каждая операция записи производится дважды, параллельно. Зеркальная, или дублированная, копия данных может храниться на том же диске или на втором резервном диске в массиве. RAID 1 обеспечивает резервную копию данных, если текущий том или диск поврежден или стал недоступен из-за сбоя в аппаратном обеспечении. Зеркалирование дисков может применяться для систем с высоким коэффициентом готовности или для автоматического резервирования данных вместо утомительной ручной процедуры дублирования информации на более дорогие и менее надежные носители.

Достоинства:

1) Обеспечивает приемлемую скорость записи и выигрыш по скорости чтения при распараллеливании запросов;

2) Имеет высокую надёжность – работает до тех пор, пока функционирует хотя бы один диск в массиве. Вероятность выхода из строя сразу двух дисков равна произведению вероятностей отказа каждого диска, т.е. значительно ниже вероятности выхода из строя отдельного диска. На практике при выходе из строя одного из дисков следует срочно принимать меры – вновь восстанавливать избыточность. Для этого с любым уровнем RAID (кроме нулевого) рекомендуют использовать диски горячего резерва.

Недостаток RAID 1 в том, что по цене двух жестких дисков пользователь фактически получает лишь один.

Рис.6.RAID 1

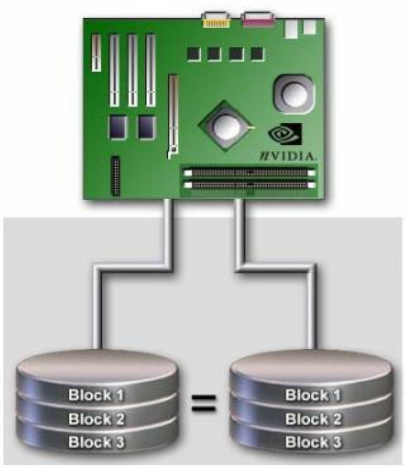


Рис.7. Схема RAID 1

RAID 10 – зеркалированный массив, данные в котором записываются последовательно на несколько дисков, как вRAID 0. Эта архитектура представляет собой массив типа RAID 0, сегментами которого вместо отдельных дисков являются массивы RAID 1. Соответственно, массив этого уровня должен содержать как минимум 4 диска (и всегда чётное количество). RAID 10 объединяет в себе высокую отказоустойчивость и производительность.

Утверждение, что RAID 10 является самым надёжным вариантом для хранения данных, ошибочно, т. к., несмотря на то, что для данного уровня RAID возможно сохранение целостности данных при выходе из строя

половины дисков, необратимое разрушение массива происходит при выходе из строя уже двух дисков, если они находятся в одной зеркальной паре.

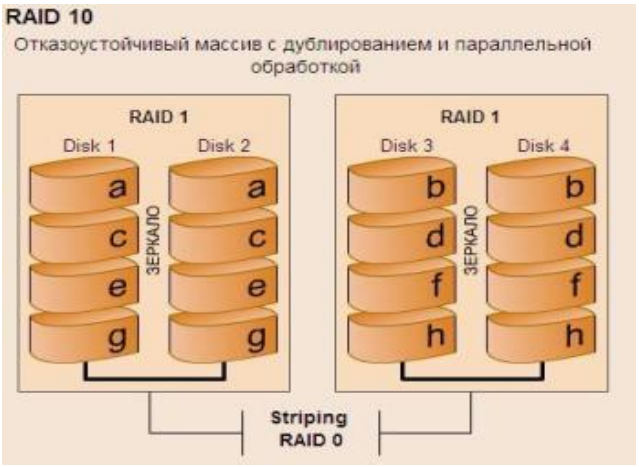


Рис.8. Схема RAID 10

Обзор программ резервного копирования

На сегодняшний день существует множество программных продуктов для обеспечения технологии резервного копирования данных.

Рассмотрим следующие программы:

–Acronis True Image Home.

–Paragon Drive Backup Server Edition.

–Symantec Backup Exec.

– R-Drive Image

Acronis True Image Home – популярная программа для резервного копирования данных. Программа решает проблему резервного копирования данных, гарантируя полную сохранность всей информации, хранящейся на жестких дисках компьютера. С ее помощью можно производить резервное копирование отдельных файлов и папок, любых категорий пользовательских данных по выбору, а также целых дисков или их разделов. В случае какого-либо сбоя, нарушившего доступ к информации или работу системы, а также в случае нечаянного удаления нужных файлов, легко можно восстановить работу системы и утраченную информацию.

Возможности программы:

- Создание точной копии жесткого диска;

- Резервное копирование сообщений электронной почты, параметров и данных Outlook;
- Защита параметров конфигурации установленных приложений;
- Резервное копирование и восстановление данных по категориям: музыка, видео, документы и т.п.;
- Try&Decide™ (Пробный режим): удобный инструмент для безопасной установки и испытания новых приложений;
- Автоматическое резервное копирование по расписанию: в определенное время или при возникновении определенных событий;
- Защита личных данных.

Paragon DriveBackup Server Edition – надежная защита операционной системы и данных жесткого диска как персональных компьютеров, так и корпоративных сетей. В дополнение к средствам резервного копирования и восстановления пользователь обладает уникальной возможностью удаленного управления задачами резервного копирования на других сетевых компьютерах. PARAGON DriveBackup предоставляет полный набор инструментов для создания резервных копий, восстановления и копирования жестких дисков и их разделов. Используя программу, вы можете создавать резервные копии данных, в том числе автоматическую резервную копию диска, тем самым безопасно хранить архив на удобном носителе и создавать компакт-диск восстановления, который позволяет запускать систему и восстанавливать информацию после сбоя системы.

Возможности программы:

- Резервное копирование Windows систем без прерывания работы с использованием Microsoft Volume Shadow Copy Service (MS VSS) или Paragon Hot Processing;
- Организация автоматизированной системы защиты данных, которая полностью соответствует политике резервного копирования «установить и забыть»;

- Эффективные инструменты миграции Windows систем на различные аппаратные платформы, как физические, так и виртуальные (P2V, P2V Восстановление, V2P, V2V, P2P), способствуют минимизации затрат на обновление центров хранения данных, позволяет более рационально использовать ресурсы аппаратного и программного обеспечения;
- Комплексные среды восстановлении данных на основе Linux/DOS и WinPE*** доступны на CD/DVD/Blu-ray, флэш-носителе или из Архивной капсулы, позволяют быстро восстановить работоспособность системы. Кроме того, с их помощью можно извлечь информацию с поврежденного жесткого диска или выполнить развертывание архива на машину без предустановленной операционной системы
- Интеграция всего функционала виртуализации компании, включая уникальную технологию монтирования виртуальных дисков для проведения любого типа миграции и обслуживания виртуальных сред;
- Восстановление на гранулярном уровне сокращает время недоступности ресурсов и сервисов, если нет необходимости производить полное восстановление данных из архива;
- Устранение проблем загрузки без восстановления данных (изменение реестра ОС Windows в режиме оффлайн, коррекция MBR, BCD, файла Boot.ini и т.д.).

BackupExec 2012 - это единый интегрированный продукт, предназначенный для защиты виртуальных и физических сред, упрощения процедур резервного копирования и повышения возможностей восстановления. Благодаря поддержке технологии Symantec V-Ray BackupExec 2012 позволяет восстанавливать целые серверы, критически важные приложения Microsoft и виртуальные среды VMware или Microsoft Hyper-V, что значительно сокращает время простоя.

Особенности:

- Простое восстановление виртуальных систем, приложений, баз данных, файлов и папок или отдельных объектов из одной резервной копии в секундах с запатентованной технологией V-Ray;
- Резервное копирование виртуальных систем без агента;
- Интегрированные средства восстановления с нуля на другой аппаратной платформе с преобразованием физической среды в виртуальную (P2V);
- Лучшие в своем классе средства дедупликации данных позволяют оптимизировать любую стратегию резервного копирования путем дедупликации в клиентской системе, на резервном сервере или в аппаратных и программных системах;
- Advanced Advanced Administration Console обеспечивает более эффективную конфигурацию резервного копирования, управление политиками резервного копирования, аварийное восстановление и преобразование резервных копий серверов в виртуальные системы для немедленного аварийного восстановления;
- Защищать большое количество операционных систем, платформ, приложений и баз данных в виртуальной и физической среде с поддержкой устройств хранения на дисках и магнитных лентах.

R-Drive Image - является эффективной утилитой для создания файлов образа диска и резервного копирования данных. Файл образа диска, содержащий точную, "байт в байт" копию жесткого диска, раздела или логического диска, может быть создан без перезагрузки компьютера и с различным уровнем сжатия данных. Созданный образ диска может быть сохранен на носителях различного вида, включая такие съемные носители, как CD-R(W)/DVD, Iomega Zip и Jazz диски.

R-Drive Image восстанавливает образ диска на оригинальный диск, на другой раздел или на свободное неформатированное пространство диска без перезагрузки системы. Для восстановления системного или заблокированного раздела R-Drive Image переключается в

псевдографический режим напрямую из Windows или запускается загрузочная версия программы с CD/DVD или комплекта дискет.

Используя R-Drive Image, вы можете быстро и полностью восстановить систему после тотальной потери данных, вызванной сбоем системы, вирусной атаки или аварией аппаратного обеспечения компьютера. Вы также можете использовать R-Drive Image для массового клонирования системы в случаях, когда необходимо установить одну, уже настроенную систему, на несколько идентичных компьютеров. Другими словами, вы можете вручную настроить одну систему, создать её образ и затем развернуть этот образ на остальных идентичных компьютерах, экономя время и средства. При необходимости восстановления лишь нескольких файлов, образ диска может быть присоединен как виртуальный диск; данные с него, т.е. напрямую с образа диска, легко копируются посредством Проводника Windows или других файловых утилит.

Возможности R-Drive Image:

- Простой и удобный интерфейс пользователя - не требуются углубленные познания управления компьютером.
- Выполнение операций "на лету": Образы диска создаются без необходимости остановки и перезагрузки операционной системы Windows. В процессе создания образа и до его завершения все остальные операции записи сохраняются в кеш-память. Восстановление образа также осуществляется "на лету" за исключением системного раздела. При восстановлении системного раздела, необходимо перезагрузить программу в псевдо-графический режим непосредственно из Windows или с помощью заранее созданных загрузочных дисков (CD/DVD или дискет).
- Сжатие файлов образов. Для экономии дискового пространства файлы образов могут быть сжаты.
- Поддержка съемных медиа устройств. Файлы образов могут быть сохранены на съемные медиа устройства типа CD-R(W)/DVD, Iomega Zip и Jazz диски.

- Загрузочная версия. Загрузочная версия используется для создания образа / восстановления / копирования заблокированных ОС разделов. Компьютер перезагружается в загрузочный режим либо непосредственно из Windows, либо при помощи съемного носителя USB, CD/DVD диска или комплекта из 6 дискет. Загрузочная версия имеет графический интерфейс или псевдографический режим (запускается на компьютере, видеокарта которого не поддерживается в графическом интерфейсе). Поддержка UEFI загрузки для современных компьютеров.
- Поддержка USB 2.0 и 3.0 в загрузочной версии. В то время как стоимость жестких дисков постоянно уменьшается, IDE-USB 2.0 или 3.0 кейс с соответствующим жестким диском может являться наиболее оптимальным и надежным решением для резервного копирования системных и других разделов, которые могут быть восстановлены только в загрузочной версии. Больше нет необходимости использования ненадежных CD/DVD и медленных CD/DVD записывающих устройств. Помните: при создании образа в инкрементальном режиме данный диск не должен быть слишком большим.
- Поддержка сетей в загрузочной версии. Загрузочная R-Drive Image версия поддерживает сохранение образа диска на удаленном компьютере и его восстановление с удаленного компьютера на локальный в сетях Microsoft (CIFS протокол).
- Расширенный Список поддерживаемых устройств в загрузочной версии. Добавлены новые аппаратные компоненты компьютера, поддерживаемые в загрузочной версии R-Drive Image. СМОТРЕТЬ СПИСОК
- Образ диска может быть подсоединен как виртуальный диск, доступный только для чтения. Содержание такого диска может быть просмотрено и скопировано.
- Восстановление отдельных файлов и папок. Из образа могут быть восстановлены отдельные файлы и папки либо при выполнении

соответствующего действия, либо при подсоединении образа как виртуального диска.

- Разделение файла образа. Файл образа диска может быть разделен на несколько файлов при недостатке места для его хранения на одном носителе.
- Защита образа диска. Файл образа может быть защищен паролем и содержать дополнительные комментарии.
- Создание новых разделов. Данные образа диска могут быть восстановлены на свободное дисковое пространство. Размер восстанавливаемого раздела может быть изменен.
- Замена разделов. Данные образа диска могут быть восстановлены на любой существующий раздел. Программа может удалить существующий раздел и восстановить образ диска на освобожденное свободное пространство.
- Копирование Диска на Диск. Целый диск может быть скопирован на любой другой, такой же или большей емкости.
- Проверка созданного образа. Файл образа диска может быть проверен на предмет корректности его создания до того, как он сохранен и/или восстановлен.
- Расписание. Задача создания образа диска может быть установлена и выполнена в определенное время в автоматическом режиме.
- Создание скрипта для частых и автоматических действий. Интерфейс программы позволяет создавать скрипты для автоматического создания файла образа и добавления данных в существующий файл образа диска. Скрипты выполняются из командной строки, и такая строка может быть включена в любой командный файл.
- Уведомление о выполненных операциях. Программа автоматически создает и отправляет уведомление по электронной почте, а также может запустить внешнюю утилиту, когда образ диска успешно создан или операция по его созданию не выполнена.

- Поддержка файловой системы ReFS (Устойчивая Файловая Система), новой локальной файловой системы, которую Микрософт ввел в ОС Windows 2012 Server. Поддерживаются все дисковые действия, за исключением изменением размера раздела.
- Полная поддержка разметки диска стандарта GPT. R-Drive Image может создавать GPT диски, изменять их размеры и менять разметку диска во время операций копирования/восстановления.
- Поддержка Windows Storage Spaces (Windows 8/8.1 и 10), томов Linux Logical Volume Manager и MacRAID.

Проанализировав все вышеизложенные продукты я остановлюсь на R-Drive Image т.к. эта программа является наиболее подходящей по соотношению цена – функционал и наиболее простой и понятной в своей работе.

Применение R-Drive Image

Для внедрения данного продукта понадобится установочный файл данной программы, который можно загрузить с сайта компании разработчика и персональный регистрационный ключ, который можно получить на электронную почту оплатив заказ на сайте разработчика. А также нам понадобится NAS устройство входящее в локальную сеть организации.

По существу, NAS является обычным компьютером, который помещен в компактный (по возможности) корпус, оснащен массивом из нескольких жестких дисков и подключен к домашней компьютерной сети. Классический NAS предназначен исключительно для длительного и надежного хранения разнообразной информации и предоставления к ней доступа из любого места домашней сети.

Так как он не предназначен для выполнения никаких вычислительных задач или прямого взаимодействия с пользователем, то в подавляющем большинстве случаев к NAS не подключаются клавиатура, мышка и монитор. Весь процесс взаимодействия с хранилищем происходит через сеть, в том числе и его первоначальная настройка. Как правило, эта настройка происходит через веб-интерфейс.

2.2. План резервного копирования

Прежде чем приступить к созданию самого плана кратко определим конфигурацию копируемой системы и параметры плана резервного копирования.

Структура дисков копируемого сервера

До начала создания плана резервного копирования рассмотрим структуру дисков копируемого сервера или компьютера. Как правило это системный диск и диск с данными. При этом это могут быть два логических диска как на одном физическом, так и на двух разных, также это могут быть и отдельные тома входящие в состав RAID (с т.ч. RAID 0 для системного диска).

В любом случае необходимо копировать и системный диск и диск с данными. Для обоих дисков лучше всего содать резервную копию тома на дисковом а не на файловом уровне. Резервное копирование путем создания образа всего диска более быстрый процесс, более надежно и позволяет полностью сохранить структуру файлов/папок на томе. Это важно не только для системного диска, где определенные файлы должны находиться в определенных папках, но также и для дисков с данными, так как многие базы данных имеют сложные структуры файлов/папок.

В нашем примере мы будет копировать два логических диска на одном физическом: системный диск (C:) и диск с данными (D:).

План резервного копирования

Зададим чтобы резервная копия создавалась в автономном режиме после окончания рабочего дня и в течение выходных. В этом случае данный процесс не будет пересекаться с основной работой, когда требуется доступ к данным.

План резервного копирования системного диска включает следующее:

- Создавать полный образ первое воскресенье каждого месяца в 14:00.
- Создавать образ в дифференциальном режиме каждое воскресенье в 17:00.
- Резервные копии хранятся в течение трех месяцев.

Данный план позволит произвести "откат" системы на состояние любой недели в течение последних трех месяцев. Например, если критический сбой в работе системы произошел во вторник, то необходимо будет переделать только то что было сделано с момента создания последней резервной копии, т.е. с 17:00 предыдущего воскресенья. Это означает что будут утрачены только около 2 дней работы. Самое большее, что вы можете утратить, это изменения конфигурации системы за последние 7 дней - например, если сбой в работе системы случился в воскресенью до 17:00. Это достаточно приемлемый уровень риска учитывая то что какие-либо изменения системы выполняются не часто.

План резервного копирования диска с данными включает следующее:

- Создавать полный образ первую субботу каждого месяца в 17:00.
- Создавать образ в дифференциальном режиме каждое воскресенье в 17:00.
- Создавать образ в инкрементальном режиме каждый рабочий день в 23:00.
- Резервные копии хранятся в течение трех месяцев.

В соответствии с данным планом состояние данных сохраняется один раз в день, при этом возможно произвести "откат" данных на состояние любого дня в течение последних трех месяцев. Резервная копия создается по субботам а не по воскресеньям и поэтому данное действие не пересекается с копированием системного диска. В этом случае максимум что может быть утрачено это изменения сделанные в течение одного дня - например, если вы сохранили файл во вторник утром и после обеда произошел сбой в работе системы, то можно будет восстановить состояние файлов на вечер

понедельника. Если файл был сохранен во вторник вечером до 23:00, а сбой в работе системы произошел на следующее утро, то ничего не будет утрачено.

Таблица 2

«Режимы создания образа: преимущества и недостатки»

Полный образ	Файл содержащий полный образ всего диска. Преимущества: Для восстановления всего диска необходим только этот единственный файл. Недостатки: Большой размер.
Образ в дифференциальном режиме	Файл содержащий изменения, сделанные на диске от момента создания полного образа до текущего момента. Преимущества: Размер меньше размера полного образа. Недостатки: Размер как правило больше размера инкрементального образа. Для восстановления диска необходим один образ в дифференциальном режиме и полный образ.
Образ в инкрементальном режиме	Файл содержащий изменения, сделанные на диске от момента создания последнего образа (полного, дифференциального или инкрементального) до текущего момента. Преимущества: Меньший размер по сравнению с дифференциальным или полным образом. Недостатки: Для восстановления данных могут потребоваться другие инкрементальные/дифференциальные образы помимо полного образа. Если какой-либо из инкрементальных образов поврежден, то не удастся также восстановить и данные из более поздних инкрементальных копий.

Место хранения резервных копий

Наиболее безопасным местом для хранения резервных копий будет удаленный сервер, физически расположенный где-то в другом месте. Это

убережет сервер с резервными копиями и ваши данные от, например, пожара или каких-либо других форс-мажорных обстоятельств, которые могут случиться в вашем здании. Другой вариант это хранить резервные копии на каком-либо другом оборудовании в том же здании. Это защитит вас от утраты данных при сбое в работе аппаратной части (т.к. если резервные копии находятся на используемом в работе физическом диске, то при сбое могут быть утрачены как сами данные, так и их резервные копии).

Рис.9. Рекомендуемая схема сети при резервном копировании небольшого корпоративного сервера

В качестве удаленного сервера не обязательно использовать какое-либо дорогостоящее оборудование. Здесь вполне может подойти экономичное и надежное сетевое хранилище данных (устройство NAS). Его возможно приобрести практически в любом магазине торгующем компьютерами и IT оборудованием.

Обратите внимание, что многие устройства NAS выпускаются с поддержкой внутренних томов RAID. Для хранения резервных копий используйте отказоустойчивые уровни RAID - например, RAID 1, RAID 4, RAID 5 или RAID 6. Не используйте чередующиеся тома (RAID 0) - если один из его дисков выйдет из строя, то все данные будут утрачены.

R-Drive Image совместим с любой серверной платформой поддерживающей сетевой протокол SMB. Среди них Windows, MAC OS и

Linux. В большинстве устройствах NAS используются разновидности ОС Linux.

В нашем примере мы будем хранить резервную копию на удаленном сервере в сети *(BCK-UBUNTU)*.

Email уведомления

После завершения создания резервной копии отправляется сообщение электронной почты о результатах операции. Его пример можно посмотреть в разделе *Примеры E-mail Уведомления* в конце данной статьи.

Подробные инструкции по созданию плана резервного копирования описаны в приложении 1.

2.3 Экономические затраты и план внедрения

Составим статьи расходов

Таблица 3

«Статьи расходов»

Статьи расходов	Сумма, руб
Постоянные расходы:	
1. Расход электроэнергии	196,56
2. Заработная плата персонала	3 400
Итого:	3 596,56
Переменные расходы:	
1. Покупка оборудования	46 250
2. Покупка программного средства R-Drive Image	1260 (одна лицензия)
Итого:	47 510

Рассмотрим постоянные расходы:

- Расход электроэнергии

Усредненный тариф (Городское население, дневная зона с 7-00 до 23-00 часов) на электроэнергию на 10.03.2009 - 1,82 руб./кВт ч

Примерный расход кВт в час для сервера резервного копирования (не пиковая загруженность сервера) - 0,15 кВт

Время работы сервера(в месяц) - 720 часов, предполагается постоянная работа сервера

ИТОГО: 0,15 х 720 х 1,82 = 196,56 руб

- Заработная плата персонала

1 сотрудник на полставки инженера-программиста 11 разряда (почасовая форма расчета з/п)

52,5 руб. - час, норма - 80 ч./месяц.

52,5 руб. х 80 ч = 3 400

ИТОГО: 3 400 руб.

Рассмотрим переменные расходы:

- Покупка оборудования

Сервер S4000B (S4286LGi): Core 2 Quad Q9550/ 4 Гб/ 2 x 1 Тб SATA RAID, производитель: НИКС

Цена на 10.03.2017: 46 250 руб.

- Покупка программного обеспечения

Стоимость одной лицензии на R-Drive Image – 1260 руб.

Необходимое количество зависит от конкретного учебного заведения, ориентировочно 20 штук.

20шт. x 1260 руб. = 25200 руб.

Сведем полученные результаты в таблицу 4 — Инвестиции в проект

Таблица 4

«Инвестиции в проект»

Сумма начальных инвестиции	71 400 руб.
Ежемесячное содержание	3 596,56 руб

Составим план – график сведрения системы резервного копирования - таблица 5

Таблица 5

«План-график внедрения R-Drive Image»

Этап	Временные затраты	Особые условия
Анализ программного средства	10-12ч.	Инженер-программист, отвечающий за написание документации по окончанию анализа.

Покупка программного средства	X	Необходима регистрация на сайте
Установка программного средства	20-23 ч.	Инженер-программист, отвечающий за установку и последующие написание детальной инструкции.
Тестирование, отладка программного продукта	2-3 дня	Группа инженеров. Создание критических ситуаций. Запись времени копирования, восстановления.
Написание отчета	14-16ч	Работник, отвечающий за детальный отчет о проделанной работе

Выводы по главе II

Во второй главе было сделано следующее:

- Рассмотрены технологии резервирования дисковых накопителей, выявлены их достоинства и недостатки;
- Рассмотрены программные продукты, предназначенные для осуществления процесса резервирования данных, выявлены их достоинства и недостатки;
- Выбран наиболее подходящий программный продукт и аппаратные средства;
- Составлено описание практического применения программного средства;
- Описаны экономические затраты и план внедрения системы резервного копирования.

ЗАКЛЮЧЕНИЕ

На основании изученных информационных источников по теме исследования можно сделать вывод о практической необходимости внедрения системы резервного копирования в образовательных учреждениях. Вопрос по защите и резервному копированию информации стоит сегодня очень актуально ввиду безусловного развития информационных технологий и влечет за собой большой рост количества обрабатываемой и сохраняемой информации. Поэтому исследования и разработки в сфере хранения и резервного копирования информации всегда будут востребованы, аппаратно-программные средства и в дальнейшем будут развиваться, совершенствоваться и подстраиваться под потребности пользователей. Система резервного копирования предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

На основании всего вышеизложенного можно сделать вывод, что внедрение систем резервного копирования безусловно необходимо при организации политики информационной безопасности образовательного учреждения.

Нами были проанализированы решения по организации систем резервного копирования и выбран программный продукт R-Drive Image, который в сочетании с сетевым хранилищем можно рассматривать как систему резервного копирования.

Благодаря выстроенному плану создания резервных копий можно максимально минимизировать ущерб по потере информации.

Таким образом, цель исследования достигнута, задачи решены, гипотеза исследования подтвердилась.

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.
2. Coughlin Associates, Inc. Peripheral Concepts, Inc. The Future of Storage. An analysis based on 3 years of extensive end users surveys. www.tomcoughlin.com, 2006.
3. Frontec, Inc. Statistics. http://www.frontecbackup.com/features/stats.htm, 2006.
4. А.Н. Чекмарев, Д.Б. Вишнякова. Глава 8. Восстановление системы. Процедуры резервного копирования и восстановления // Microsoft Windows 2000: Server и Professional. Русские версии. – Санкт-Петербург: БХВ – Санкт-Петербург, 2000.
5. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.
6. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право.- Спб.: Изд-во «Юридический центр Пресс», 2001.
7. БеловЕ.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.
8. Бесплатные программы для резервного копирования. 3DNews Daily Digital Digest [Электронный ресурс]. – 2012. – Режим доступа: http:// http://www.3dnews.ru. – Дата доступа: 24.03.2017.
9. Бильд Г. Большой выбор с еще большим отсевом. LAN, #02/2007. http://www.osp.ru/lan/2007/02/3965478/, 2007.
10. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004.
11. Блэк У. Интернет: протоколы безопасности. Учебный курс. - СПб.: Питер, 2001.

12. Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1: Учебное пособие. Пенза: Изд-во ПГУ, 2005.
13. В. Куртис Престон. Резервное копирование и восстановление Unix, O'Reilly&Associates.
14. В.Г. Казаков, С.А. Федосин «Технологии и алгоритмы резервного копирования»,
15. В.Н. Лопатин. Правовые основы информационной безопасности. Курс лекций. М., МИФИ, 2000.
16. Владимир Шаньгин. “Защита компьютерной информации. Эффективные методы и средства”, «ДМК Пресс» 2010.
17. Владимир Шаньгин. Защита компьютерной информации. Эффективные методы и средства, «ДМК Пресс» 2010.
18. Войтов Н.М. Администрирование Red Hat Enterprise Linux. Учебное пособие. ДМК Пресс.2011.
19. Вомак Б. Перевод Елизаветы Серьгиной. HP приютит файлы на собственных серверах. РБК daily. http://www.rbcdaily.ru/2008/04/09/media/335033, 2008.
20. Гультяев А.К. Восстановление данных. – СПб.: Питер, 2005.
21. Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных сис-тем. М., Горячая линия-Телеком, 2005.
22. Давлетханов М. Новое слово в корпоративном резервном копировании. Softkey.info. http://www.softkey.info/reviews/review4797.php, 2008.
23. Давлетханов М. Новое слово в корпоративном резервном копировании. Softkey.info. http://www.softkey.info/reviews/review4797.php, 2008.
24. Дорофеев А.В. «Менеджмент информационной безопасности» Журнал «Вопросы кибербезопасности выпуск» № 3 (4) / 2014Пилипенко В. Ф., Ерков Н. В., Парфенов А. А. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика /М.: Из-во «Айрис-пресс», 2006. 192 с.

25. Егоров А. Резервное копирование данных пока обойдется без инноваций. CNews. http://www.cnews.ru/reviews/free/infrastructure2007/articles/reserve_copying.shtml, 2007.
26. Закон Российской Федерации «О государственной тайне» от 21.07.93 №5485-1.
27. Закон Российской Федерации «О международном информационном обмене» от 04.07.96 №85-ФЗ.
28. Закон Российской Федерации «О персональных данных» от 27.07.2006г. № 152-ФЗ.
29. Закон Российской Федерации «О сертификации продукции и услуг» от 10.06.93 №5151-1.
30. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ;
31. Закупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. №4
32. Информационная безопасность компьютерных систем и сетей: В.М. Шаньгин. – М.: Издательский дом "Форум", 2008. – 416с.
33. Казаков В.Г. Математические модели схем резервного копирования для получения оценок объема репозитория. Микроэлектроника и информатика – 2008. 15-я Всероссийская межвузовская научно-техническая конференция студентов и аспирантов: Тезисы докладов. – М.: МИЭТ, 2008. – С. 160 с.
34. Казаков В.Г., Федосин С.А. «Разработка программной файлово-ориентированной системы резервного копирования данных». Технологии Microsoft в теории и практике программирования. Материалы конференции / Под ред. проф. Р.Г. Стронгина. Нижний Новгород: Изд-во Нижегородского госуниверситета, 2007. – С. 108–110.

35. Казаков В.Г., Федосин С.А. Анализ алгоритмов резервного копирования для получения оценок объема репозитория. Кибернетика и высокие технологии XXI века. IX международная научно-техническая конференция. –Воронеж.: НПФ «Саквоее» ООО, 2008. – С. 697-709 с.
36. Казаков В.Г., Федосин С.А. Моделирование схем резервного копирования с целью получения сравнительной оценки объема данных для хранения в репозитории. Технологии Microsoft в теории и практике программирования. Материалы конференции / Под ред. проф. Р.Г. Стронгина. – Нижний Новгород: Изд-во Нижегородского госуниверситета, 2008. – С. 151-155
37. Казаков В.Г., Федосин С.А. Построение математических моделей алгоритмов резервного копирования для аналитической оценки требуемого объема репозитория. II международная научно-техническая конференция "Инфокоммуникационные технологии в науке,производстве и образовании (Инфоком-3)" г. Кисловодск, 2008 г.
38. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспече-ние информационной безопасности: Учебное пособие для студентов высш. учеб. заведений. - М.: Издательский центр «Академия», 2005.
39. Кенин А.М. Самоучитель системного администратора. СПб.: БХВ-Петербург, 2012.
40. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.:ил.
41. Краковский Ю.М. Информационная безопасность и защита информации: Уч. пособие, изд-во Март, 2008
42. Макарова Н.В. Информатика 9. – СПб: Питер, 2007
43. Мелов Г., Лось А. СХД для SMB. CITForum. http://www.citforum.ru/nets/storage/for_smb/, 2007.
44. Орлов С. CA провела Storage Day. Журнал LAN #11 2007. http://www.osp.ru/lan/2007/11/4588256/, 2007.

45. Орлов С. EMC провела форум в Москве. Журнал LAN #11 2007. http://www.osp.ru/lan/2007/11/4586176/, 2007.
46. Основы компьютерных сетей.: Б.Д. Виснадул. – М.: Издательский дом "Форум", 2007. – 272с.
47. Павел Хорев “Программно-аппаратная защита информации. Учебное пособие”, «Форум», 2009.
48. Павел Хорев. Программно – аппаратная защита информации. Учебное пособие, «Форум», 2009.
49. Пухов Е. Битва за рынок СХД разворачивается на поле виртуализации. CNews. http://www.cnews.ru/reviews/free/server2007/articles/virtual.shtml, 2007.
50. Резервное копирование [Электронный ресурс]. – 2012. – Режим доступа: http://storusint.com. – Дата доступа: 24.03.2017.
51. Резервное копирование [Электронный ресурс]. – 2012. – Режим доступа: http://msdn.microsoft.com. – Дата доступа: 24.03.2017.
52. Роберт И. В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты): 3-е изд. М: ИИО РАО,2010. 356 с.
53. Россия продолжает экономить на хранении. CIO- World, апрель 2008. http://www.cio-world.ru/analytics/353334/, 2008.
54. Руководство по системному администрированию Red Hat Enterprise Linux. Издательство Red Hat, 2005.
55. Савяк В. RAID Levels. http://www.ixbt.com/storage/raids.html. iXBT. http://www.ixbt.com/storage/raids.html, 1999.
56. Свободная энциклопедия Википедия [Электронный ресурс]. – 2010. – Режим доступа: http://ru.wikipedia.org. – Дата доступа: 24.03.2017.
57. Седых В., Мелов Г. Корпоративные СХД в примерах, или Идеи напрокат. CompDoc. http://www.compdoc.ru/peripherals/drives/corporative_ssd_in_example/, 2006.

58. Симонович С., Евсеев Г. Эффективная работа: познай свой компьютер. – СПб.: Питер, 2005.
59. Системы хранения данных и резервного копирования. http://network.xsp.ru/6_2.php, 2005.
60. Системы хранения данных компании DESTEN. КомпьютерПресс 4'2007. http://www.compress.ru/Article.aspx?id=17509, 2007.
61. Системы хранения данных компании DESTEN. КомпьютерПресс 4'2007. http://www.compress.ru/Article.aspx?id=17509, 2007.
62. Скиба В. Ю., Курбатов В. А Руководство по защите от внутренних угроз информационной безопасности. Издательство: Питер, 2008
63. Скотт Мюллер. "Модернизация и ремонт ПК", 17 изд., «Вильямс», 2007.
64. Скотт Мюллер. «Модернизация и ремонт ПК», 17 изд., «Вильямс», 2007.
65. Смит, К. Oracle 101. Резервное копирование и восстановление. / К. Смит, С. Хейсли– М.: Лори, 2005. – 464 с.
66. Техническая документация с официальных источников:://www.gfi.ru (сайт разработчиков GFI backup)://www.paragon.ru (сайт разработчиков Paragon Drive backup Workstation)://www.acronis.ru (сайт разработчиков продуктов Acronis)
67. Тищенко А. Новые уровни RAID: цифры, буквы и то, что за ними. Компьютерное Обозрение, №21 (589). http://www.itc.ua/node/28408, 2007.
68. Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.
69. Хмелевский Р. Российский бизнес "сорит деньгами" на СХД. CNews. http://www.cnews.ru/reviews/free/infrastructure2007/articles/storages_part3.shtml, 2007.
70. Шапиро Джефри, Бойс Джим. Глава 17. Архивация и восстановление данных // Windows 2000 Server. Библия пользователя = Windows 2000

Server. Bible. – Москва: Компьютерное издательство «Диалектика» Торговый дом «Вильямс», 2001.

71. Шпик В. Система резервного копирования – «последний бастион» защиты корпоративной информации. Connect! Мир Связи, октябрь, 2006. http://www.connect.ru/article.asp?id=7197, 2006.

72. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Учебное пособие / НИУ ИТМО. СПб., 2012.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Настройка плана резервного копирования

Ежемесячный полный образ системного диска

Первая часть в плане резервного копирования системного диска это ежемесячный полный образ, создаваемый в первое воскресенье каждого месяца в 14:00.

1. На этапе *Выбор Действия (Action Selection)* нажмите Планировщик задач / Создать Скрипт (Scheduler / Create a Script).

Рис. 2. Ежемесячный полный образ системного диска - этап Выбор Действия (Action Selection)

2. На этапе *Расписание выполнения Задач (Scheduled Tasks)* нажмите кнопку Создать задачу (Create a task).

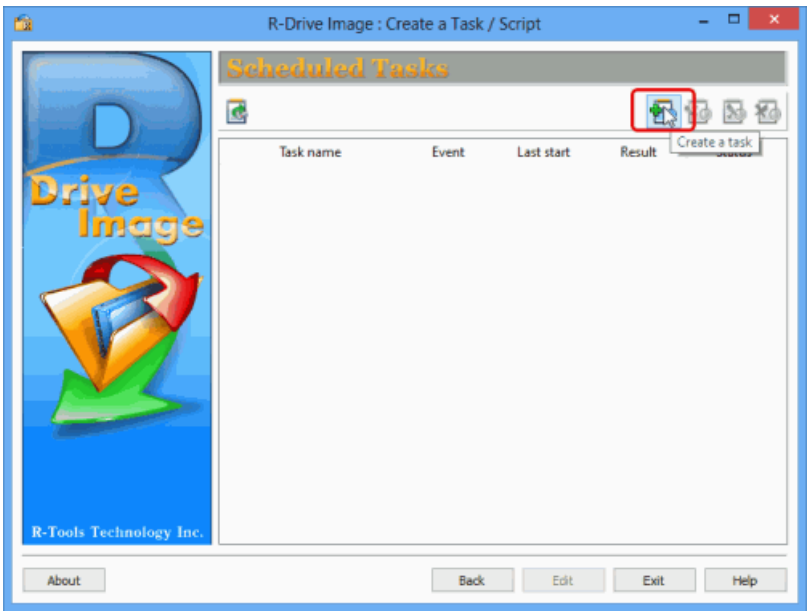


Рис. 3. Ежемесячный полный образ системного диска - этап Расписание выполнения Задач (Scheduled Tasks)

3. На этапе *Выбор Раздела (Partition Selection)* выберите системный раздел резервную копию которого вы будете создавать. В нашем примере системный раздел это C:.

Рис. 4. Ежемесячный полный образ системного диска - этап Выбор Раздела (Partition Selection)

При создании резервной копии системного диска Windows 7 и более поздней версии Windows не забудьте также выбрать небольшой активный

раздел на котором находится загрузчик системы. В более ранних версиях Windows такого раздела нет.

4. На этапе *Месторасположение Образа (Image Destination)* выберите месторасположение файла образа и имя файла.

В нашем примере мы выберем находящийся в сети сервер для резервных копий BCK-UBUNTU и папку Backups. Может потребоваться ввести имя пользователя и пароль для получения доступа к папке сетевого диска.

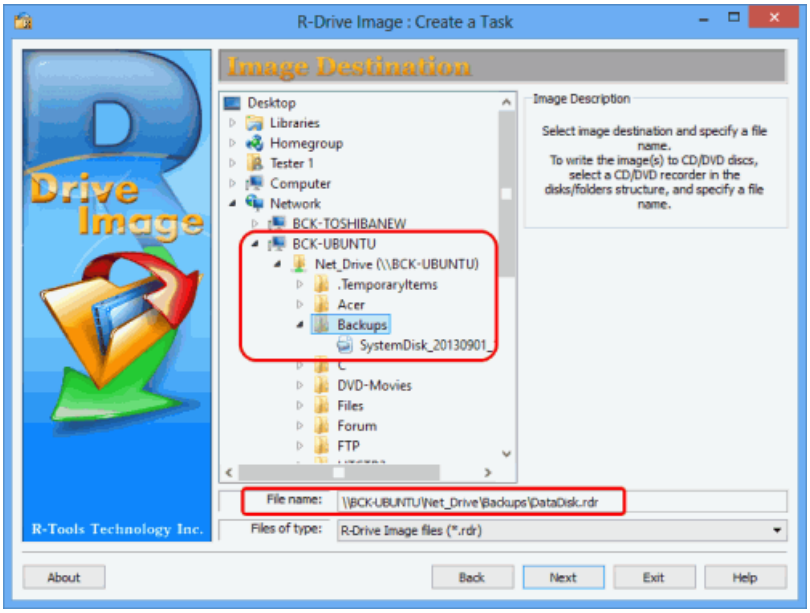


Рис. 5. Ежемесячный полный образ системного диска - этап Месторасположение Образа (Image Destination)

5. Задайте параметры резервных комплектов на этапе *Режим Создания Образа (Imaging Mode)* как показано на нижеприведенном рисунке.

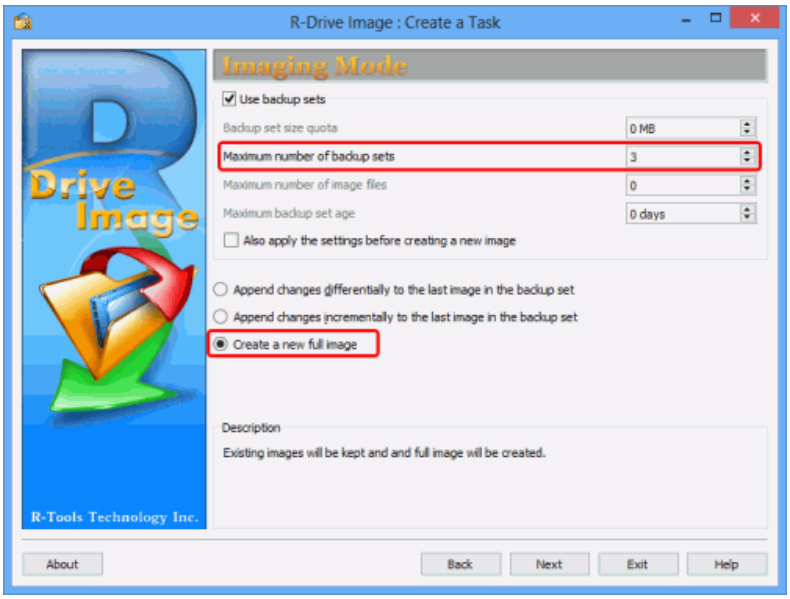


Рис. 6. Ежемесячный полный образ системного диска - этап Режим Создания Образа (Imaging Mode)

Введите 3 в поле *Максимальное число резервных комплектов (Maximum number of backup sets)* и установите радиокнопку Создать новый полный образ (Create a new full image). Более подробную информацию об остальных параметрах можно найти в R-Drive Image online Справке - раздел Резервные Комплекты (Backup Sets).

6. Задайте необходимые параметры на этапе *Параметры Образа (Image Options)* как показано на нижеприведенном рисунке.

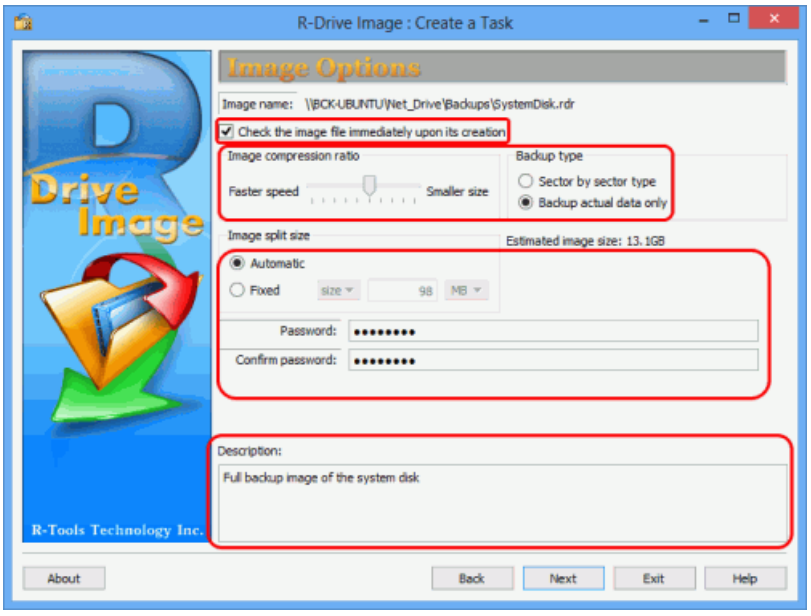


Рис. 7. Ежемесячный полный образ системного диска - этап Параметры Образа (Image Options)

Более подробную информацию об остальных параметрах можно найти в R-Drive Image online Справке - раздел Создание Образа (Create an Image).

7. Задайте необходимые параметры на этапе *Параметры Резервного Копирования (Backup Options)* как показано на нижеприведенном рисунке.

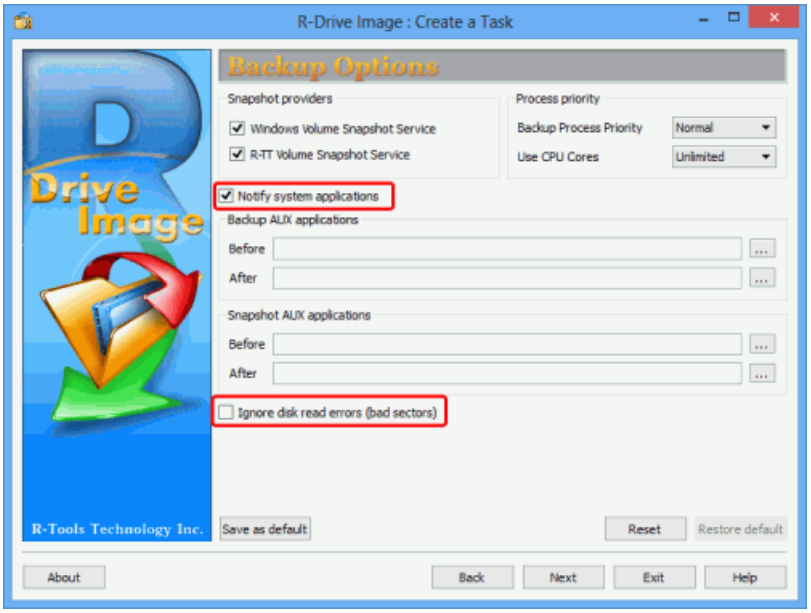


Рис. 8. Ежемесячный полный образ системного диска - этап Параметры Резервного Копирования (Backup Options)

Более подробную информацию об остальных параметрах можно найти в R-Drive Image online Справке - раздел: Создание Образа (Create an Image).

8. Задайте необходимые параметры на этапе *Время/Событие (Time/Event)* как показано на нижеприведенном рисунке.

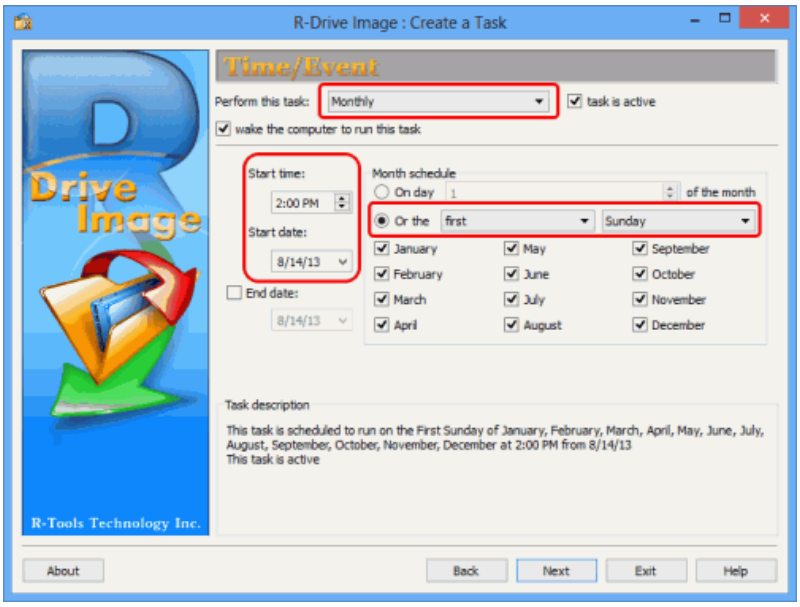


Рис. 9. Ежемесячный полный образ системного диска - этап Время/Событие (Time/Event)

9. Задайте необходимые параметры на этапе *Пользователь/Пароль (User/Password)*.

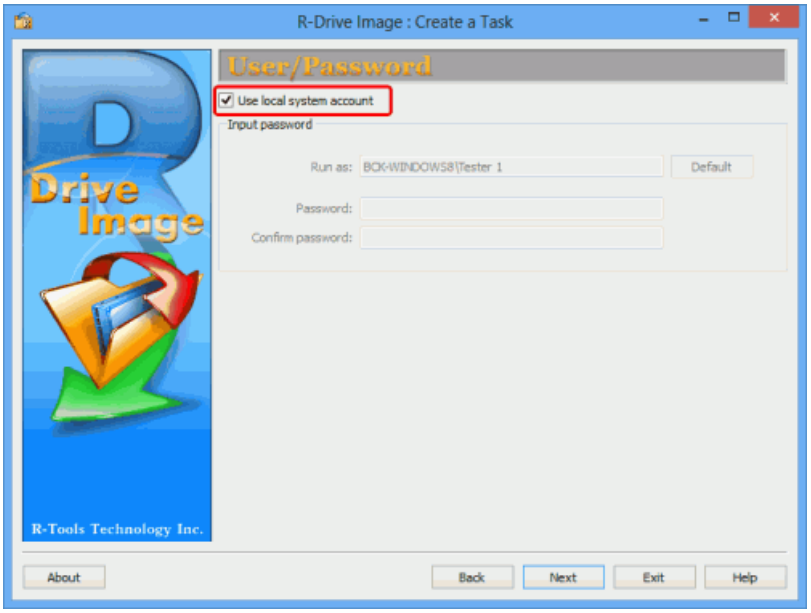


Рис. 10. Ежемесячный полный образ системного диска - этап Пользователь/Пароль (User/Password)

10. Задайте параметры E-mail уведомления на этапе *E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)* как показано на нижеприведенном рисунке.

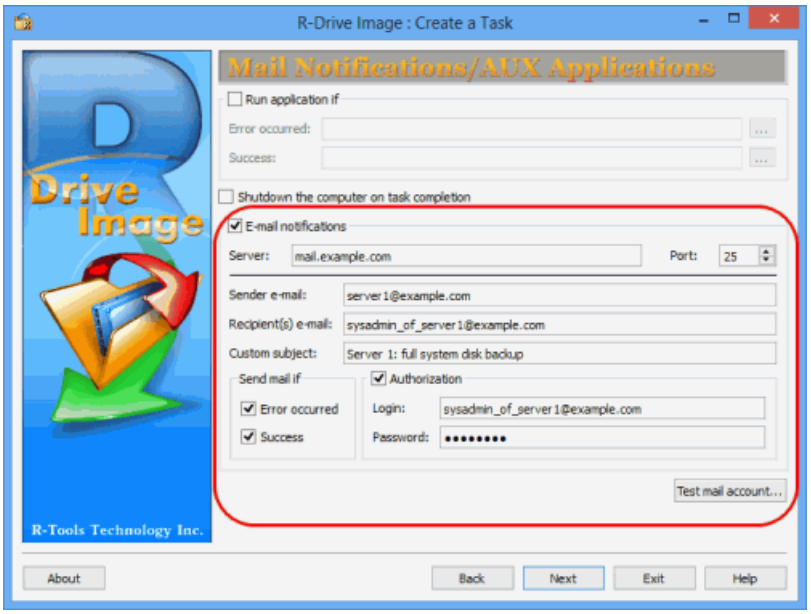


Рис. 11. Ежемесячный полный образ системного диска - этап E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)

На этом же этапе можно проверить настройки e-mail нажав кнопку Проверка E-mail... (Test mail account…). R-Drive Image отправит тестовое e-mail сообщение на указанный в настройках адрес.

11. Подтвердите корректность параметров задачи на этапе *Обработка (Processing)* и нажмите кнопку Сохранить (Save).

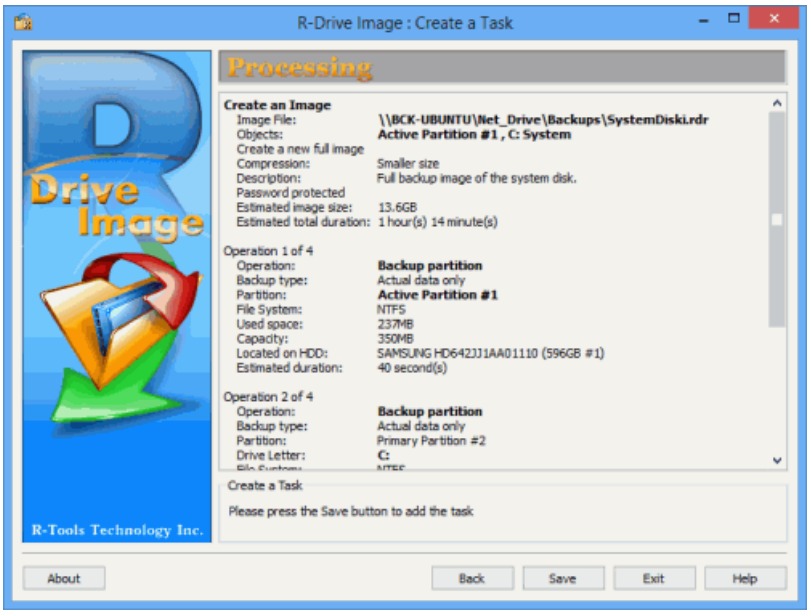


Рис. 12. Ежемесячный полный образ системного диска - этап Обработка (Processing)

Чтобы изменить какой-либо параметр задачи нажмите кнопку Назад (Back) и вернитесь на соответствующий этап.

Если вы нажмете кнопку Сохранить (Save), то созданная задача появится в списке на этапе *Расписание выполнения Задач (Scheduled Tasks)*.

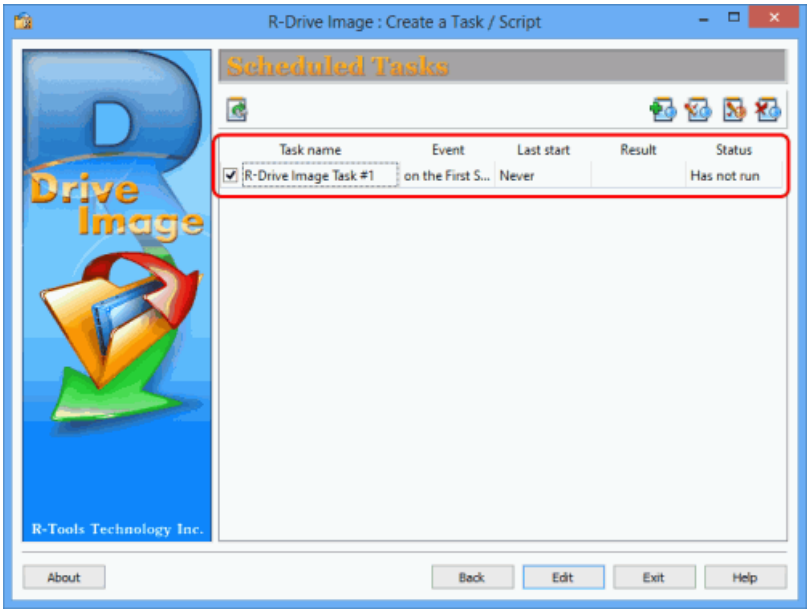


Рис. 13. Ежемесячный полный образ системного диска - этап Расписание выполнения Задач (Scheduled Tasks)

Еженедельный образ системного диска в дифференциальном режиме

Следующий этап это создание еженедельного образа в дифференциальном режиме. В состав резервной копии войдут только измененные или добавленные данные с момента последнего создания полного образа. Размеры файлов образов в этом случае будут меньше и на их создание потребуется меньше времени, что является более удобным при выполнении еженедельных операций резервного копирования.

1. Нажмите кнопку Создать задачу (Create a task) на этапе *Расписание выполнения Задач (Scheduled Tasks)*, выберите системный раздел на этапе *Выбор Раздела (Partition Selection)* и выберите на этапе *Месторасположение*

Образа (Image Destination) тот же самый файл образ что и при создании полного образа.

2. Задайте параметры резервных комплектов на этапе *Режим Создания Образа (Imaging Mode)*.

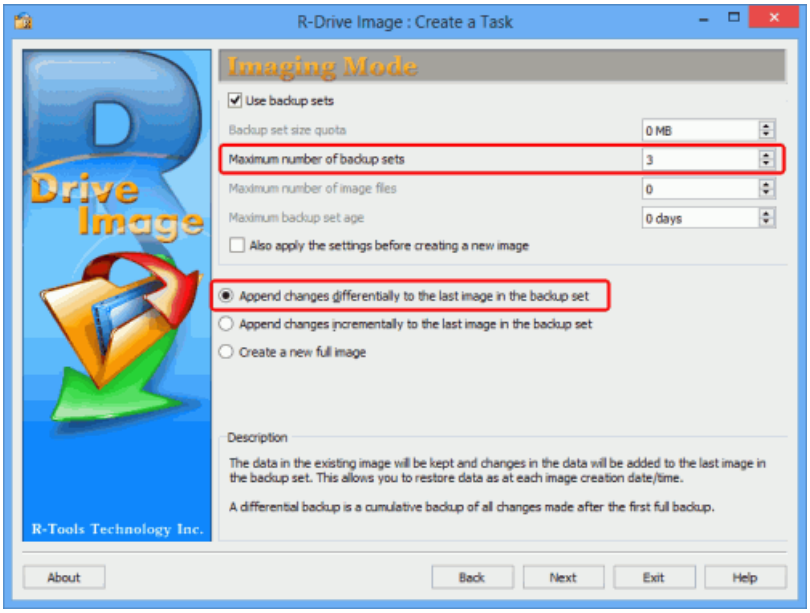


Рис. 14. Еженедельный образ системного диска в дифференциальном режиме - этап Режим Создания Образа (Imaging Mode)

Введите 3 в поле *Максимальное число резервных комплектов (Maximum number of backup sets)* и установите радиокнопку Добавлять изменения дифференциально к последнему образу в резервном комплекте (Append changes differentially to the last image in the backup set).

Если созданный полный образ диска был защищен паролем, то вам потребуется его ввести.

3. Задайте необходимые параметры на этапах *Параметры Образа (Image Options)* и *Параметры Резервного Копирования (Backup Options)* также как и при создании полного образа.

4. Задайте необходимые параметры на этапе *Время/Событие (Time/Event)*.

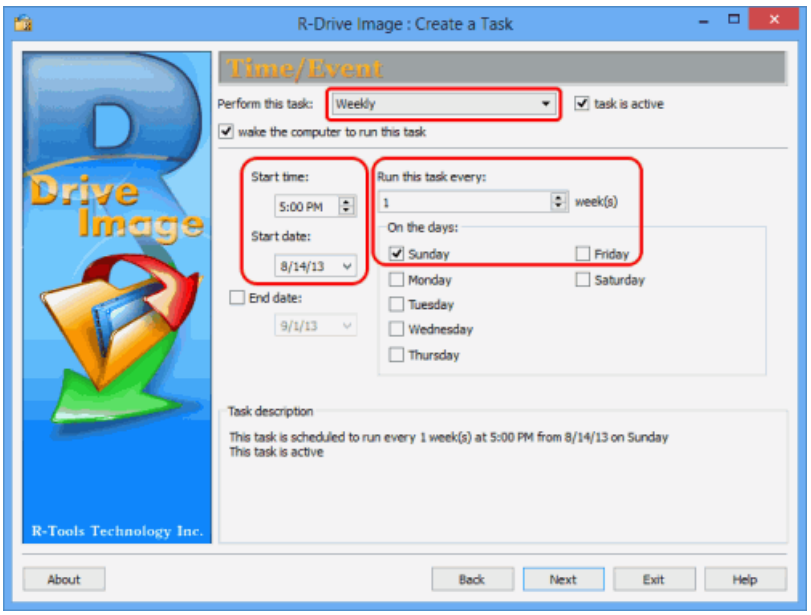


Рис. 15. Еженедельный образ системного диска в дифференциальном режиме - этап Время/Событие (Time/Event)

Проверьте чтобы *Время начала (Start time)* не совпадало со временем создания полного образа. В нашем примере ежемесячный полный образ создается в 14:00 и еженедельный образ в дифференциальном режиме в 17:00.

5. Задайте необходимые параметры на этапе *Пользователь/Пароль (User/Password).*

6. Задайте необходимые параметры на этапе *E-mail Уведомления/Внешние Утилиты (Mail Notifications/AUX Applications)* также как и при создании полного образа.

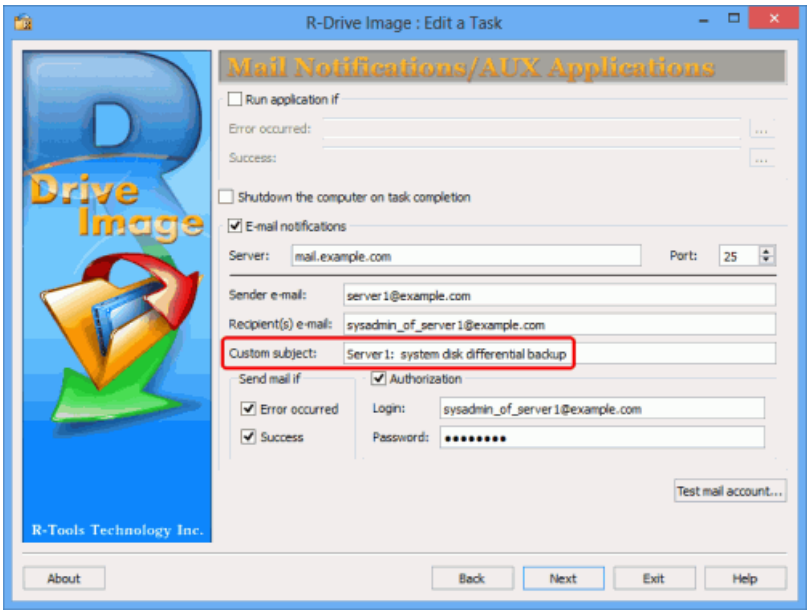


Рис. 16. Еженедельный образ системного диска в дифференциальном режиме - этап E-mail Уведомления/Внешние Утилиты (Mail Notifications/AUX Applications)

Измените *Тему уведомления: (Custom subject:)* на Server1: differential system disk backup.

7. Подтвердите корректность параметров задачи на этапе *Обработка (Processing)* и нажмите кнопку Сохранить (Save).

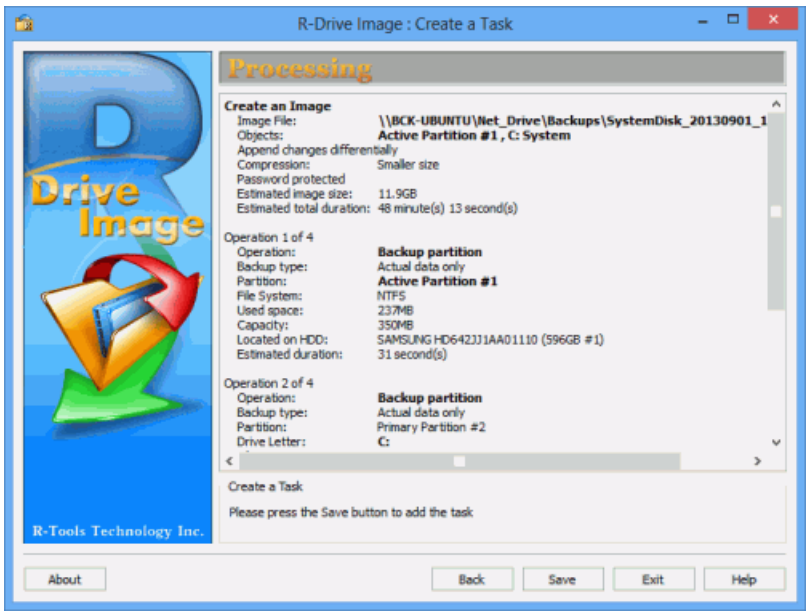


Рис. 17. Еженедельный образ системного диска в дифференциальном режиме - этап Обработка (Processing)

Созданная задача появится в списке на этапе *Расписание выполнения Задач (Scheduled Tasks)*.

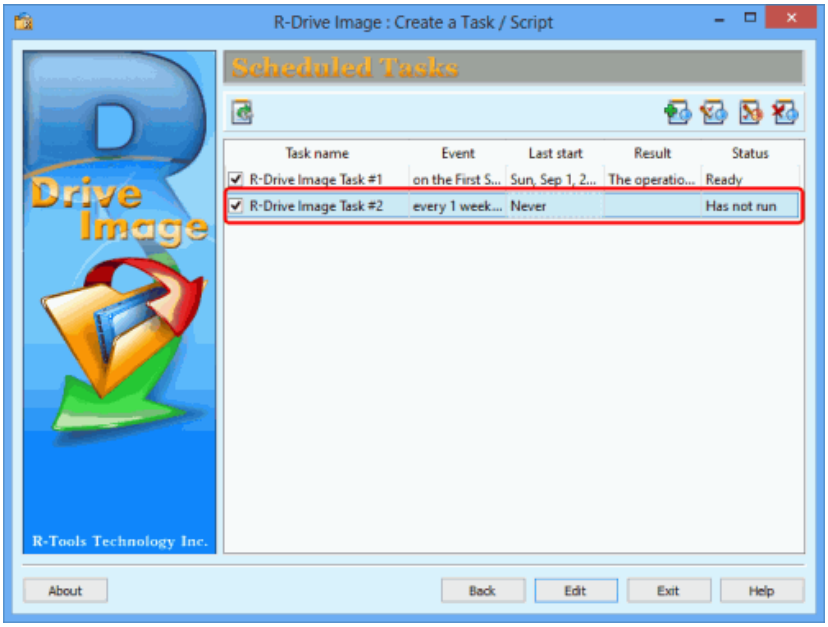


Рис. 18. Еженедельный образ системного диска в дифференциальном режиме - этап Расписание выполнения Задач (Scheduled Tasks)

Копирование Диска с Данными

Ежемесячный полный образ диска с данными

Данный процесс во многом схож с копированием системного диска за исключением того, что в этом случае создается образ раздела с данными (D:).

1. На этапе *Расписание выполнения Задач (Scheduled Tasks)* нажмите кнопку Создать задачу (Create a task).

2. Выберите раздел с данными (D:) на этапе *Выбор Раздела (Partition Selection)*.

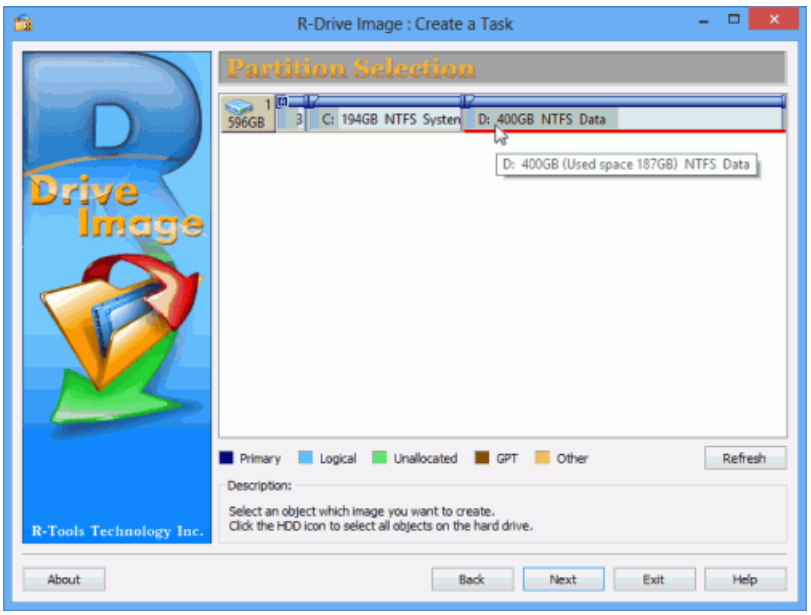


Рис. 19. Ежемесячный полный образ диска с данными - этап Выбор Раздела (Partition Selection)

3. На этапе *Месторасположение Образа (Image Destination)* выберите месторасположение файла образа и имя файла.

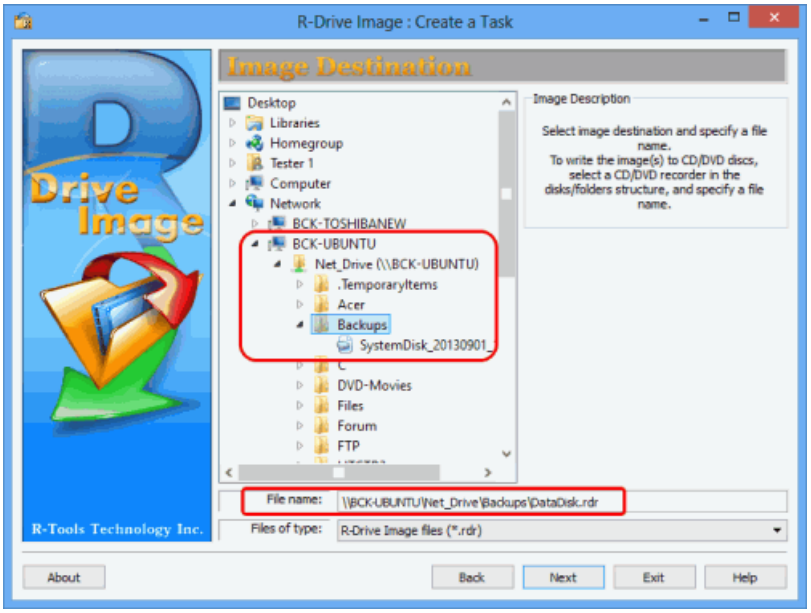


Рис. 20. Ежемесячный полный образ диска с данными - этап Месторасположение Образа (Image Destination)

4. Задайте параметры резервных комплектов на этапе *Режим Создания Образа (Imaging Mode)*.

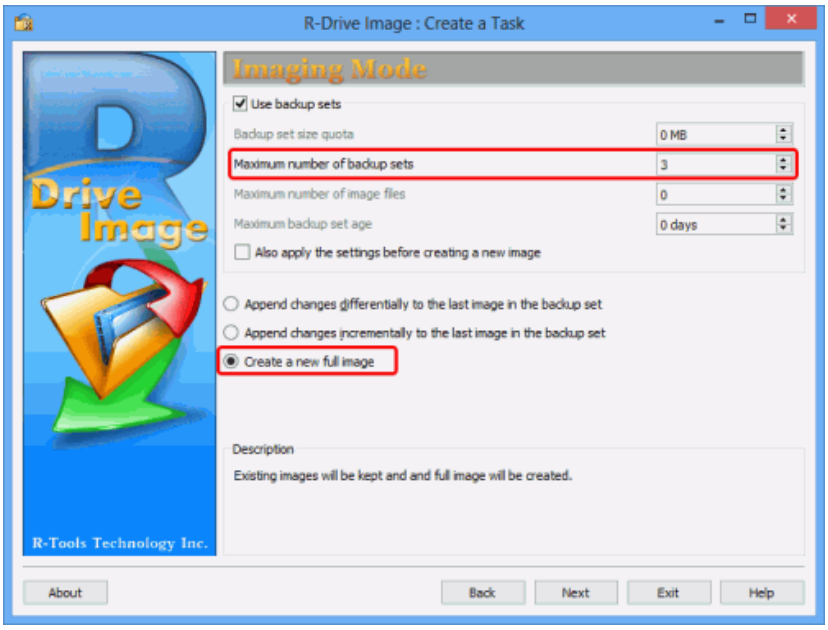


Рис. 21. Ежемесячный полный образ диска с данными - этап Режим Создания Образа (Imaging Mode)

Установите 3 в поле *Максимальное число резервных комплектов (Maximum number of backup sets)* и установите радиокнопку Создать новый полный образ (Create a new full image).

5. Задайте необходимые параметры на этапах *Параметры Образа (Image Options)* и *Параметры Резервного Копирования (Backup Options)* также как и при создании полного образа системного диска.

6. Задайте необходимые параметры на этапе *Время/Событие (Time/Event)*.

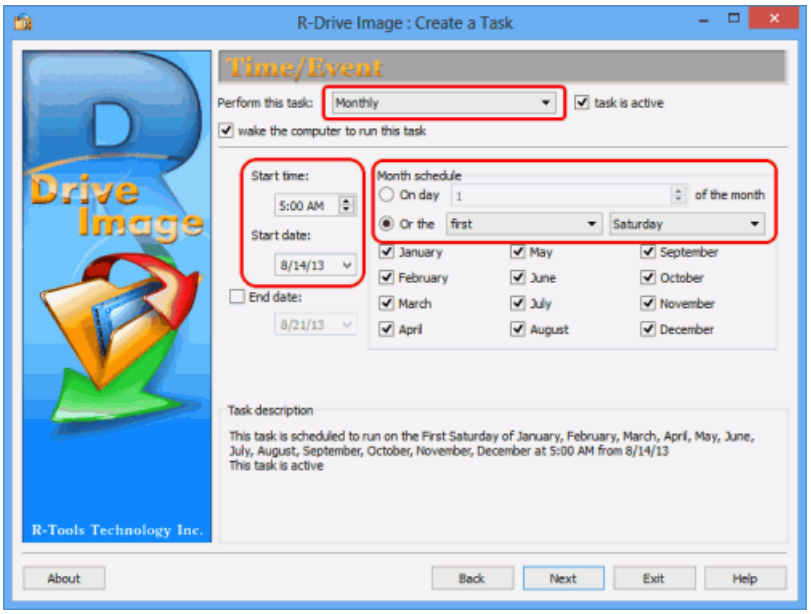


Рис. 22. Ежемесячный полный образ диска с данными - этап Время/Событие (Time/Event)

7. Задайте необходимые параметры на этапе *Пользователь/Пароль (User/Password)*.

8. Задайте параметры E-mail уведомления на этапе *E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)*.

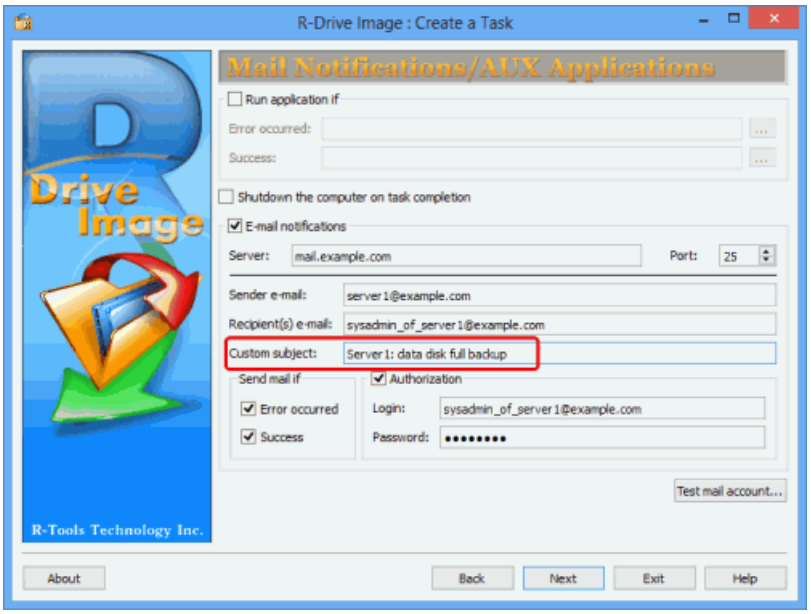


Рис. 23. Ежемесячный полный образ диска с данными - этап E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)

9. Подтвердите корректность параметров задачи на этапе *Обработка (Processing)* и нажмите кнопку Сохранить (Save).

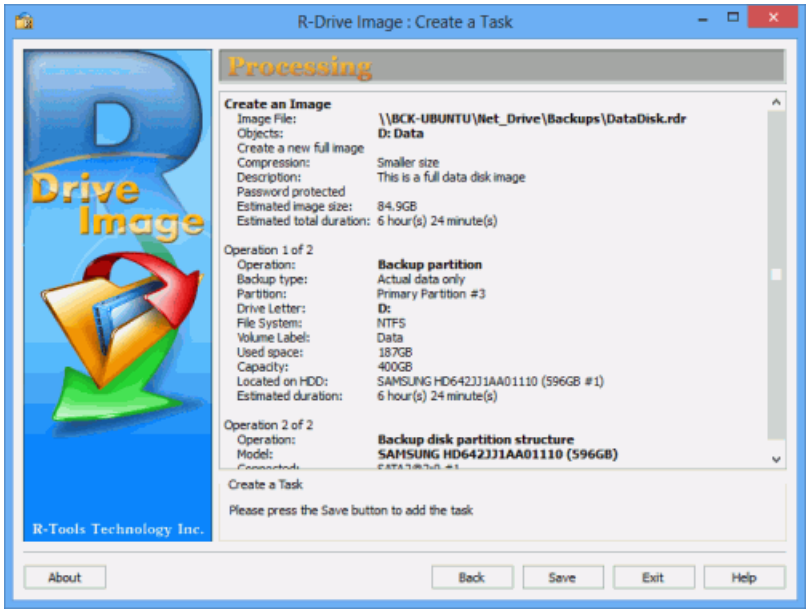


Рис. 24. Ежемесячный полный образ диска с данными - этап Обработка (Processing)

Созданная задача появится в списке на этапе *Расписание выполнения Задач (Scheduled Tasks).*

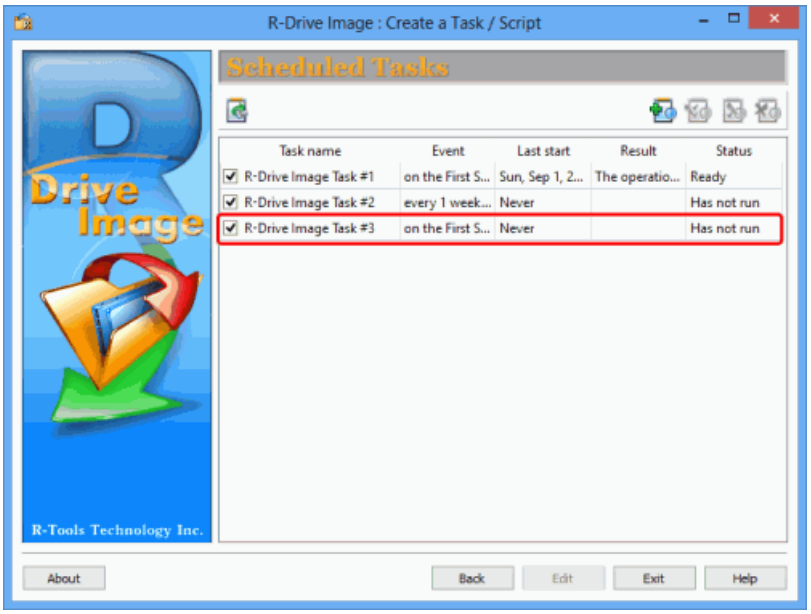


Рис. 25. Ежемесячный полный образ диска с данными - этап Расписание выполнения Задач (Scheduled Tasks)

Еженедельный образ диска с данными в дифференциальном режиме

Данный процесс также во многом схож с созданием образа системного диска в дифференциальном режиме за исключением того, что в этом случае создается образ раздела с данными (D:).

1. На этапе *Расписание выполнения Задач (Scheduled Tasks)* нажмите кнопку Создать задачу (Create a task), выберите раздел с данными (т.е. D:) на этапе *Выбор Раздела (Partition Selection)* и выберите месторасположение файла образа и имя файла (то же файл образ что и при создании полного образа диска с данными) на этапе *Месторасположение Образа (Image Destination)*.

2. Задайте параметры резервных комплектов на этапе *Режим Создания Образа (Imaging Mode)*.

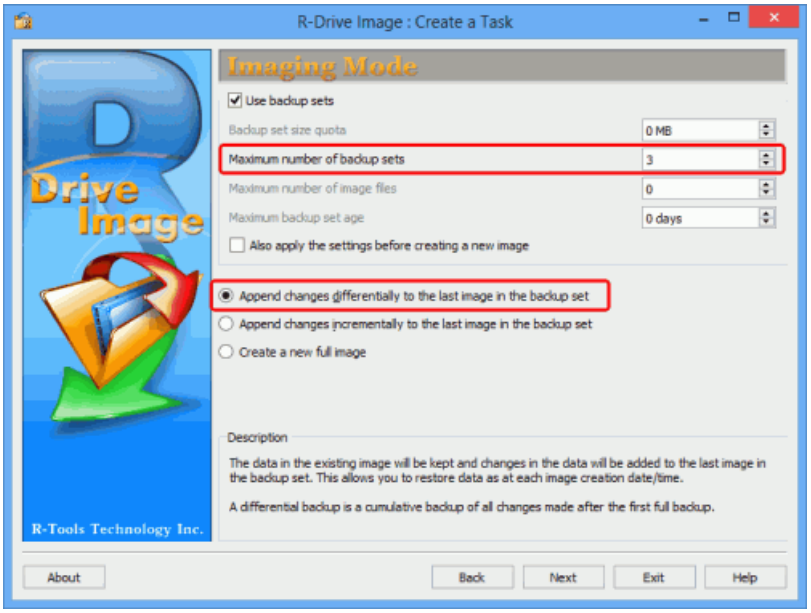


Рис. 26. Еженедельный образ диска с данными в дифференциальном режиме - этап Режим Создания Образа (Imaging Mode)

Введите 3 в поле *Максимальное число резервных комплектов (Maximum number of backup sets)* и установите радиокнопку Добавлять изменения дифференциально к последнему образу в резервном комплекте (Append changes differentially to the last image in the backup set).

3. Задайте необходимые параметры на этапах *Параметры Образа (Image Options)* и *Параметры Резервного Копирования* также как и при создании полного образа диска с данными.

4. Задайте необходимые параметры на этапе *Время/Событие* (Time/Event).

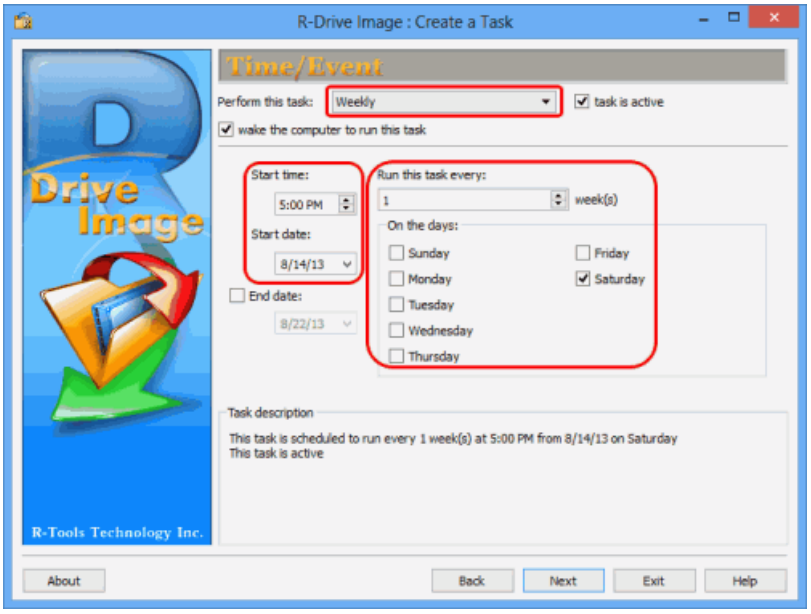


Рис. 27. Еженедельный образ диска с данными в дифференциальном режиме - этап Время/Событие (Time/Event)

5. Задайте необходимые параметры на этапе *Пользователь/Пароль (User/Password)*.

6. Задайте параметры E-mail уведомления на этапе *E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)*.

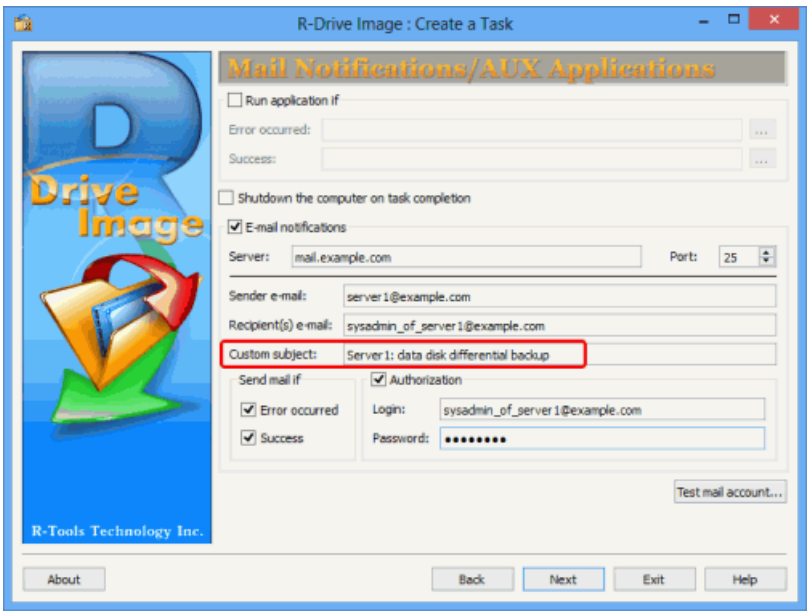


Рис. 28. Еженедельный образ диска с данными в дифференциальном режиме - этап E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)

7. Подтвердите корректность параметров задачи на этапе *Обработка (Processing)* и нажмите кнопку Сохранить (Save).

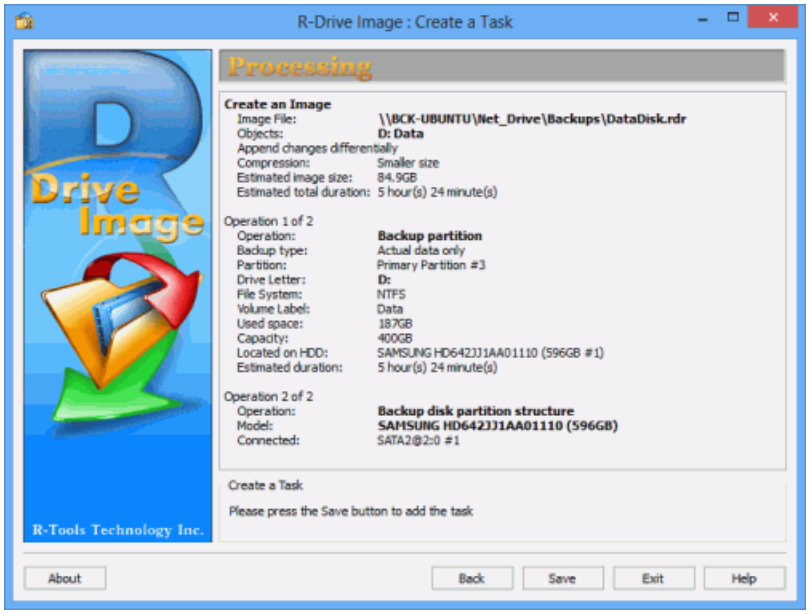


Рис. 29. Еженедельный образ диска с данными в дифференциальном режиме - этап Обработка (Processing)

Созданная задача появится в списке на этапе *Расписание выполнения Задач (Scheduled Tasks)*.

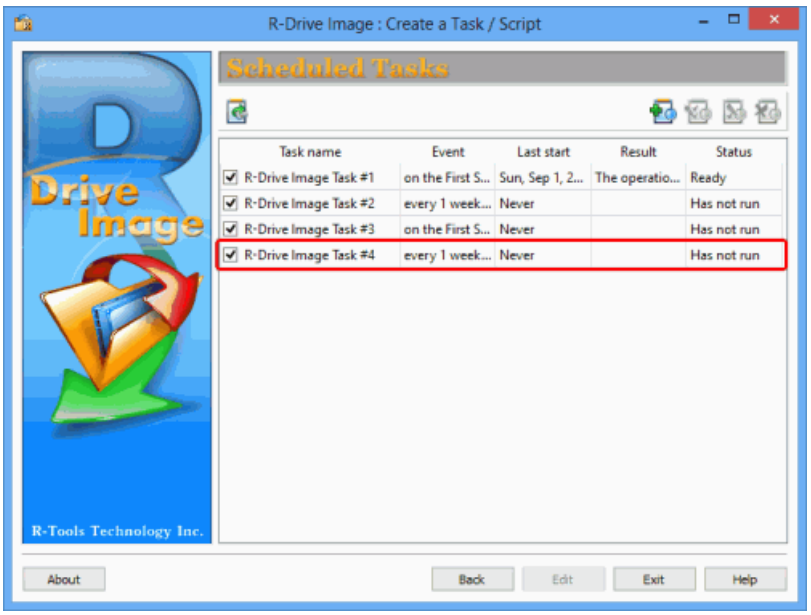


Рис. 30. Еженедельный образ диска с данными в дифференциальном режиме - этап Расписание выполнения Задач (Scheduled Tasks)

Ежедневный образ диска с данными в инкрементальном режиме

Образ в инкрементальном режиме содержит измененные или добавленные данные с момента последнего любого резервного копирования (полного, дифференциального или инкрементального). Размеры файлов образов в этом случае будут меньше размеров файлов образов созданных в дифференциальном режиме, что является более удобным при выполнении ежедневных операций резервного копирования.

1. Нажмите кнопку Создать задачу (Create a task) на этапе *Расписание выполнения Задач (Scheduled Tasks)*, выберите раздел с данными на этапе *Выбор Раздела (Partition Selection)* и выберите на этапе *Месторасположение Образа (Image Destination)* тот же самый файл образ что и при создании полного образа диска с данными.

2. Задайте параметры резервных комплектов на этапе *Режим Создания Образа (Imaging Mode)*.

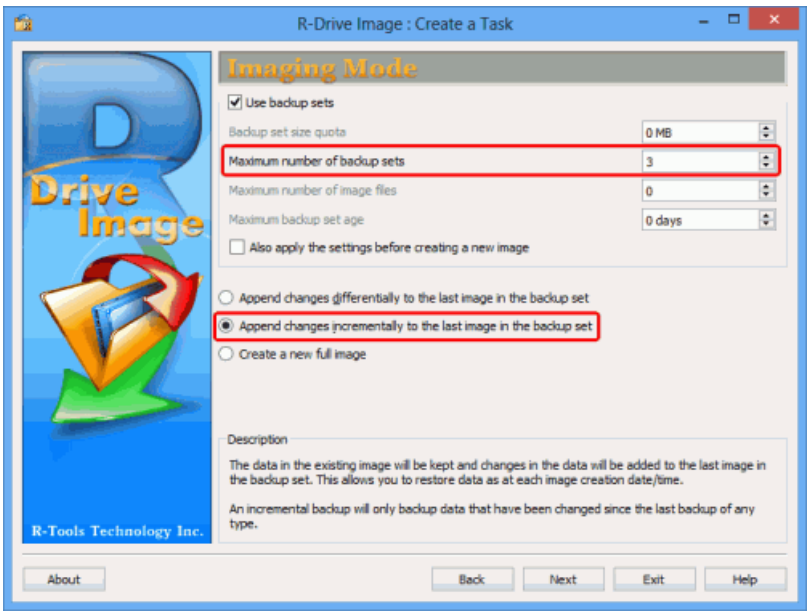


Рис. 31. Ежедневный образ диска с данными в инкрементальном режиме - этап Режим Создания Образа (Imaging Mode)

Введите 3 в поле *Максимальное число резервных комплектов (Maximum number of backup sets)* и установите радиокнопку Добавлять изменения инкрементально к последнему образу в резервном комплекта (Append changes incrementally to the last image in the backup set).

3. Задайте необходимые параметры на этапах *Параметры Образа (Image Options)* и *Параметры Резервного Копирования (Backup Options)* также как и при создании полного образа диска с данными.

4. Задайте необходимые параметры на этапе *Время/Событие (Time/Event)*.

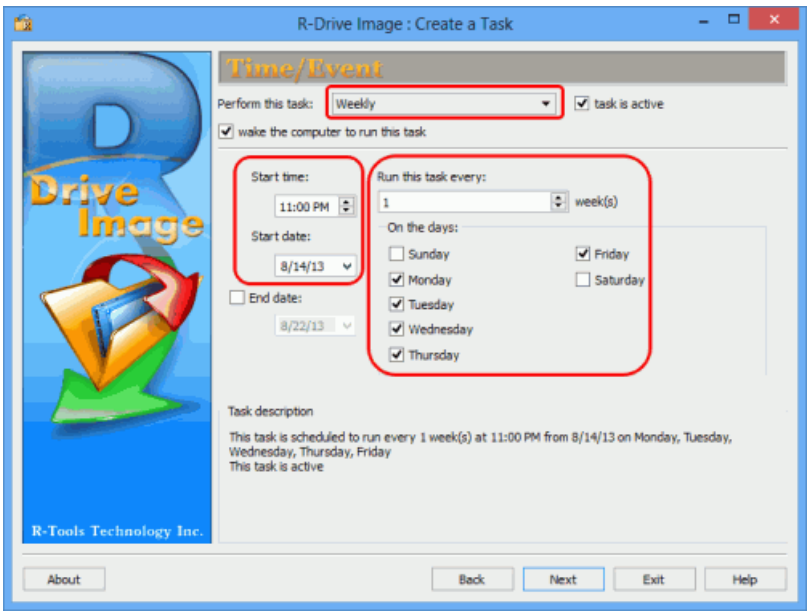


Рис. 32. Ежедневный образ диска с данными в инкрементальном режиме - этап Время/Событие (Time/Event)

5. Задайте необходимые параметры на этапе *Пользователь/Пароль (User/Password)*.

6. Задайте параметры E-mail уведомления на этапе *E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)*

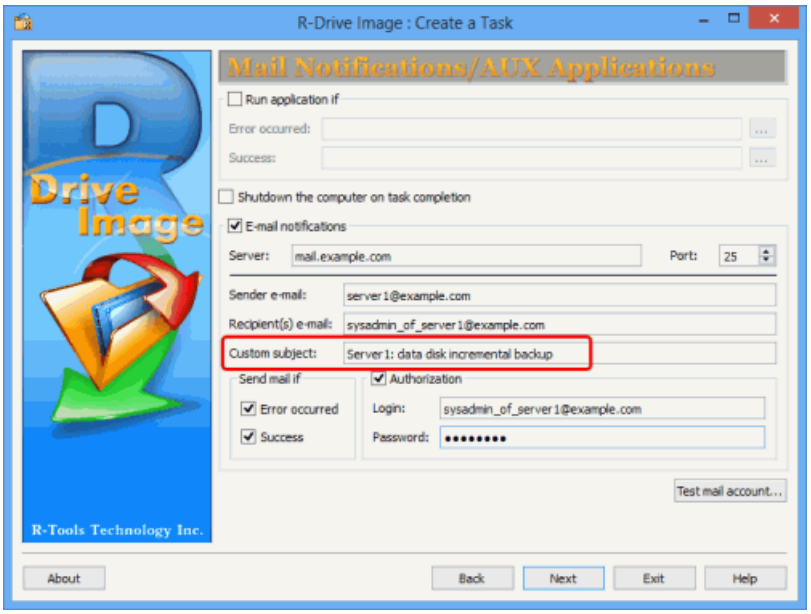


Рис. 33. Ежедневный образ диска с данными в инкрементальном режиме - этап E-mail Уведомления/Внешние Утилиты (Mail Notification/AUX Applications)

7. Подтвердите корректность параметров задачи на этапе *Обработка (Processing)* и нажмите кнопку Сохранить (Save).

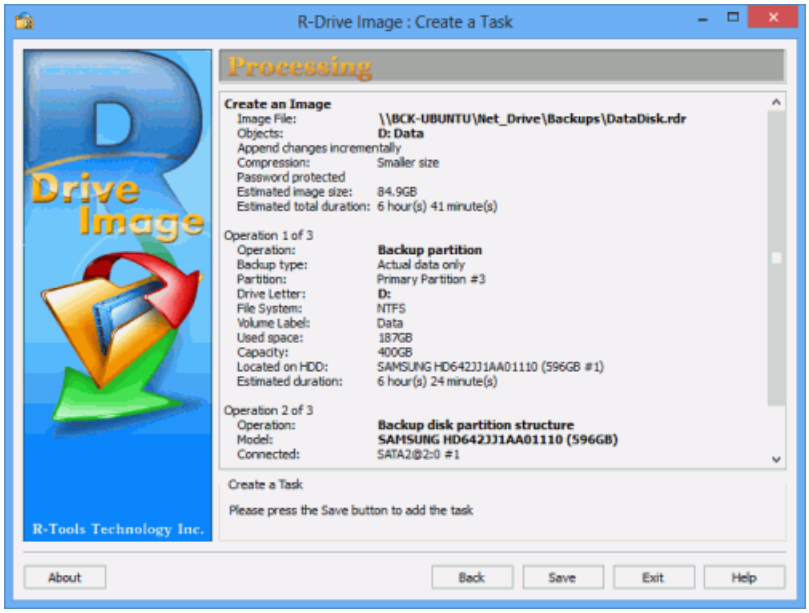


Рис. 34. Ежедневный образ диска с данными в инкрементальном режиме - этап Обработка (Processing)

Созданная задача появится в списке на этапе *Расписание выполнения Задач (Scheduled Tasks)*.

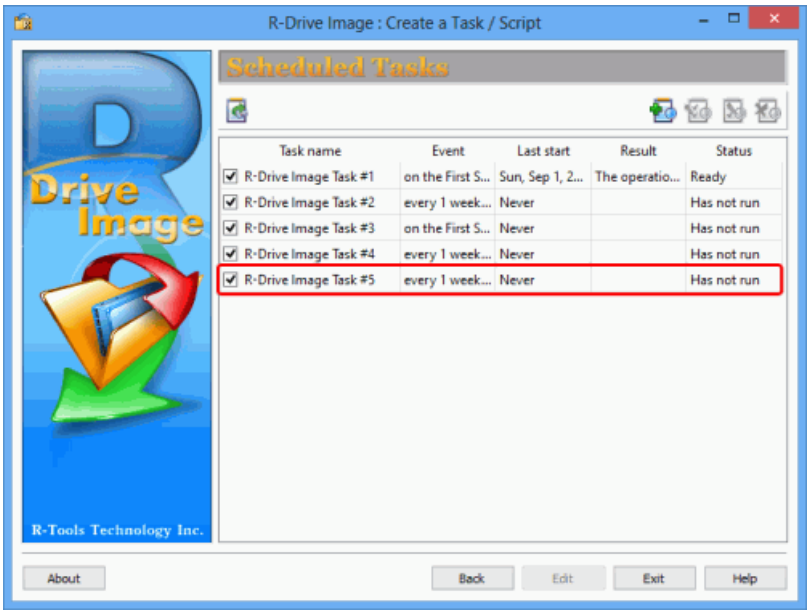


Рис. 35. Ежедневный образ диска с данными в инкрементальном режиме - этап Расписание выполнения Задач (Scheduled Tasks)

Протоколирование

Можно сохранить файл журнала операций R-Drive Image. Для этого нажмите кнопку О программе (About) на этапе *Выбор Действия (Action Selection)*, установите флажок Протоколирование (Logging) и задайте имя и путь к файлу.

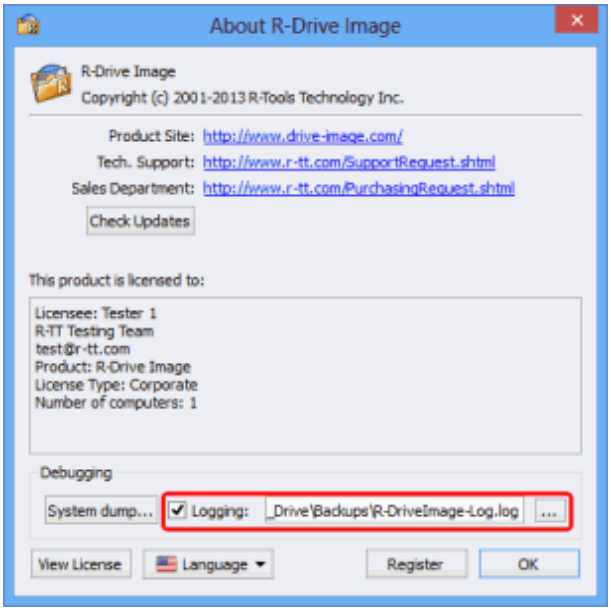


Рис. 36. R-Drive Image: Протоколирование

Примеры E-mail Уведомления

После завершения операции резервного копирования R-Drive Image будет отправлять E-mail уведомление.

При *Успешном завершении операции* уведомление будет иметь следующий вид:

R-Drive Image 5.1 (Build 5100)
Command: create /a /o -
s="hdd_size=640135028736+part_num=1+hdd_num=1+hdd_target_id=0+hdd_bus_type=sata2
+part_ofs=1048576+hdd_name=SAMSUNG HD642JJ1AA01110+part_size=367001600+hdd_port_num=2
+hdd_serial=S1AFJ1MQ400283+part_fs=ntfs+hdd_vtype=real,hdd_size=640135028736+part_num=2
+hdd_num=1+hdd_target_id=0+hdd_bus_type=sata2+part_label=System+part_ofs=368050176
+part_mounted=C:\+hdd_name=SAMSUNG HD642JJ1AA01110+part_size=209348198400

+hdd_port_num=2+hdd_serial=S1AFJ1MQ400283+part_fs=ntfs+hdd_vtype=real"
-a="\\BCK-UBUNTU\Net_Drive\Backups\SystemDisk.rdr" -p="******" -r="Full backup image of the system disk."
-c="6" -u -check -bs -bs-num-b="3" -ms="mail.example.com:25" -ml="******" -ma="server1@example.com"
-mr="sysadmin_of_server1@example.com" -mc="Server 1: full system disk backup" -mx -me
Start at: Sun, 01 Sep 2013 14:00:00 -0500
Finish at: Sun, 01 Sep 2013 15:08:39 -0500
Success

Operations:
Create an Image: \\BCK-UBUNTU\Net_Drive\Backups\SystemDisk.rdr
Backup partition [SAMSUNG HD642JJ1AA01110 (596GB #1)]
Active Partition #1 (NTFS 350MB)
C: System (NTFS 194GB #2)
Backup disk partition structure
SAMSUNG HD642JJ1AA01110 (596GB #1)
Check an Image File

Execution log:
* Create an Image: \\BCK-UBUNTU\Net_Drive\Backups\SystemDisk.rdr
Backup partition [SAMSUNG HD642JJ1AA01110 (596GB #1)]
Active Partition #1 (NTFS 350MB)
C: System (NTFS 194GB #2)
Backup disk partition structure
SAMSUNG HD642JJ1AA01110 (596GB #1)
Check an Image File
* Operation completed successfully

Если *операция завершилась неудачно*, то уведомление будет выглядеть так:

R-Drive Image 5.1 (Build 5100)
Command: create /a /o -
s="hdd_size=522713088+part_num=1+hdd_num=2+hdd_target_id=0
+hdd_bus_type=usb+part_label=RS+part_ofs=65536+hdd_name=Flash Disk 4.00
+part_size=522647552+hdd_port_num=0+hdd_serial=078163578514+part_fs=fat16+hdd_vtype=real"
-a="D:\Backups\HDD2_2-image.rdr" -u -check -ms="smtp.example.com:25"
-ml="******" -ma="sender@example.com" -mr="receiver@example.com"
-mc=" Flash backup" -mx -me
Start at: Sun, 01 Sep 2013 18:06:47 -0500
Finish at: Sun, 01 Sep 2013 18:06:49 -0500
ERROR: Internal error (error #0:3831)

Operations:
Create an Image: D:\Backups\HDD2_2-image.rdr
Backup partition [KingstonDataTraveler 400PMAP (3.74GB #2)]
Active Partition #1 NEW VOLUME (FAT32 3.73GB)
Backup disk partition structure
KingstonDataTraveler 400PMAP (3.74GB #2)
Check an Image File

Execution log:
! KingstonDataTraveler 400PMAP: Partition at 32 extends beyond disk bounds
! KingstonDataTraveler 400PMAP: Partition at 32 extends beyond disk bounds
* Create an Image: D:\Backups\HDD2_2-image.rdr
Backup partition [KingstonDataTraveler 400PMAP (3.74GB #2)]
Active Partition #1 NEW VOLUME (FAT32 3.73GB)
Backup disk partition structure
KingstonDataTraveler 400PMAP (3.74GB #2)
Check an Image File
! Read disk KingstonDataTraveler 400PMAP at position 16896 failed after 2 attempts. The handle is invalid (6)
! Read disk KingstonDataTraveler 400PMAP at position 16896 failed after 2 attempts. The handle is invalid (6)
! Read disk at position 2671616 failed after 2 attempts. The handle is invalid (6)
! Operation failed: Internal error (error #0:3831)