

Acronis

8 фактов
о резервном копировании
и восстановлении

A

Большие данные стали нормой. Согласно исследованиям **IDC**, мировой объем данных удваивается каждые два года. В то же время данные превратились в один из важнейших активов компаний, который требует к себе внимательного отношения.

Становится все труднее защитить большой объем данных, которые зачастую могут находиться в разных средах и/или на разных устройствах. Как ИТ-специалисты могут справиться с такой нетривиальной задачей? Ключ к успеху — в восьми фактах о резервном копировании и восстановлении данных.

Компании, следующие этим рекомендациям, могут обеспечить полную сохранность своих данных, независимо от того, расположены ли они локально (на физических или виртуальных машинах) или в облаке.

Данные имеют значение, поэтому их потеря чревата серьезными последствиями для финансов и рабочего процесса. **Исследование, проведенное в прошлом году компанией Spiceworks,** показало, что

45%

МАЛЫХ КОМПАНИЙ сталкивались с потерей данных

14% из них так и не смогли восстановить СВОИ данные



В то же время, недавнее исследование IDC, проведенное совместно с Acronis, показало, что более



3/4 компаний оценивают каждый час простоя для критически важных приложений не менее **\$20 000** чем в

Факт №1

Данные — это все

Понятие «данные» шире, чем полагают многие ИТ-специалисты. Оно включает в себя как явные данные (сведения о клиентах, счета и финансовую информацию, важные документы и презентации PowerPoint и т. п.), так и менее заметную, но столь же важную информацию, которой ИТ-администраторы могут не придавать большого значения.

Примеры:

- Системные конфигурации
- Программные приложения (MS Office, ERP и т. д.)
- Исправления, обновления, пользовательские сценарии и рабочие процессы
- Отметки «Мне нравится» на Фейсбуке, записи в Твиттере и другая деятельность в социальных сетях
- Электронная почта

Эти данные необходимы для аналитики и непрерывности бизнес-процессов, а также для минимизации времени, необходимого для восстановления. Однако они менее осязаемы, поэтому компании не всегда делают их резервные копии. Вместо этого такие данные могут храниться в различных сервисах, в скрытой панели управления или специальной папке, созданной ИТ-администратором.

Когда любые данные, будь то информация по счетам или программный код, оказываются повреждены или потеряны, страдает общая производительность и доход компании. Финансовые риски особенно высоки в таких областях, как здравоохранение или финансы, где существуют строгие нормативные стандарты.

- ▶ **Медицинские компании** тратят **1,6 миллиарда долл. США в год** в виде расходов, связанных с нарушением безопасности, потерей данных и незапланированными простоями

В декабре 2013 г. **власти США** оштрафовали компанию Barclays на **3,75 млн. долл. США** за невыполнение обязательств по сохранению электронной почты, текстовых сообщений и электронных записей сделок и счетов. ◀

Потеря времени — еще одно следствие потери данных. Если происходит сбой, а резервные копии приложений не сделаны, ИТ-специалистам приходится переустанавливать каждую программу. Переустановить Word, Excel или PowerPoint достаточно легко, но серверы приложений, такие как Exchange, IIS, SQL Server и Active Directory, гораздо сложнее установить и настроить. ИТ-отдел также должен учитывать снижение производительности сотрудников в том случае, если приложения или вся сеть станут недоступны.

Процесс восстановления может быть сложным и занимать много времени, но без сети работать практически невозможно, а файлы бесполезны без соответствующих приложений. Это означает потерю времени на устранение проблемы для ИТ-отдела, потерю производительности для сотрудников и напрасно потраченное время для пользователей, которые до этого оптимизировали свои системы и приложения.

В современном бизнесе данные являются всем — и все является данными. Компании полагаются на них при обслуживании клиентов, повышении дохода, усовершенствовании продукции и принятии решений. Обладает ли защита данных наивысшим приоритетом или находится в конце списка задач, ответственность за нее, как правило, несет ИТ-отдел. Поэтому у ИТ-специалистов должен быть разработан план для постоянной и надежной защиты всех рабочих данных компании.

Факт №2

Защитить данные становится все сложнее



▲
Факт №1

Данные — это новая валюта современного цифрового мира.

И каждый день появляется все больше данных — на новых устройствах и в новых местах — которые нужно защитить и сохранить.

Средний сотрудник компании в США один производит более

1 750 ГБ данных **В ГОД**



В 2014 г. количество пользователей мобильных устройств в мире составит

4,55 миллиарда



Факт №2

Защитить данные становится все сложнее

Компании зависят от своих данных, поэтому важно регулярно сохранять и защищать их, чтобы обеспечить непрерывность работы. **Но если данные настолько важны, почему их не защищают должным образом?**

На это есть несколько причин:

Во-первых, объем создаваемых данных стремительно растет, и компании не успевают с ним справиться:

- К 2020 году мировой объем цифровых данных достигнет **40 триллионов гигабайт**
- **90 процентов** мирового объема данных было создано за последние два года
- В 2014 году количество пользователей мобильных устройств составит **4,55 миллиарда**
- **250 миллиардов фотографий** было загружено на Фейсбук
- Каждый день появляется **400 миллионов** записей в Твиттере

Во-вторых, постоянный доступ означает, что все больше данных производится круглосуточно, с самых разнообразных устройств и приложений. Таким образом сокращаются или вовсе исчезают временные окна, необходимые для резервного копирования.

Мобильные технологии и социальные сети еще больше увеличивают темп создания данных и их разнообразие, и конца этому не видно. Появляющийся так называемый «Интернет вещей» (IoT — Internet of things) **в несколько раз увеличит объем данных**, который компании будут производить, хранить и анализировать. К 2020 году, **по прогнозам компании Cisco**, в мире будет насчитываться до 50 миллиардов соединенных друг с другом устройств, производящих данные.

В-третьих, данные располагаются в гораздо большем количестве мест, чем раньше, включая локальные серверы, удаленные хранилища, личные устройства и облачные сервисы. Все эти факторы усложняют разработку и развертывание планов резервного копирования.

Вместе эти сложности ставят современных ИТ-специалистов в крайне затруднительное положение, так как постоянно увеличивается количество данных, поступающих из разных источников и хранящихся в разных местах. Кроме того, из-за круглосуточного режима работы, а также отсутствия выходных сокращаются окна резервного копирования.

ИТ-специалистам следует пересмотреть методы идентификации и защиты тех объемов данных, которые сотрудники круглосуточно производят на своих устройствах. Устаревшие стратегии резервного копирования (или полное отсутствие таковых) ставят под угрозу рабочие данные и ограничивают возможность их эффективного использования.

Факт №3

Аварии неизбежны. Потеря данных — обязательно.



▲
Факт №2

Суровая реальность состоит в том, что потеря данных непременно произойдет, если компания не примет необходимые меры. Оборудование подводит, люди совершают ошибки, случаются стихийные бедствия.

Средний ожидаемый срок службы жесткого диска составляет **6 ЛЕТ**

— но —

5% выходит из строя в течение первого года 



Даже самый подготовленный **ИТ-отдел** не застрахован от крупной потери данных

Факт №3

Аварии неизбежны. Потеря данных — не обязательно.

“ Вы можете считать свое оборудование надежным, но на самом деле это не так. Все, абсолютно все, может подвести, и когда это произойдет, вы можете потерять всю важную информацию на этом устройстве. Для любого технического устройства сбой — это лишь вопрос времени. ”

— пишет топ-менеджер Acronis **Нэт Мэйпл** на сайте [TechRadar](#).

Внутренние уязвимости также подвергают данные риску, что часто уходит от внимания ИТ-специалистов. **Опрос, проведенный Cisco**, показал, что 20 процентов ИТ-специалистов считают недовольных сотрудников наибольшей внутренней угрозой для корпоративных данных. Недавно обнаруженная уязвимость Heartbleed выявила другой скрытый риск: вредоносные программы.

Неважно, что послужило причиной — злонамеренные действия сотрудника, нечаянная ошибка, вредоносная программа, нелепое стечение обстоятельств или даже **стихийное бедствие** — потеря данных может быть необратимой. Такие данные уже не вернуть. Подумайте о медицинских записях, исчезнувших во время урагана Катрина, или системных конфигурациях, пользовательских программных кодах и исправлениях, утраченных во время урагана Сэнди.

Даже самый подготовленный ИТ-отдел не застрахован от крупной потери данных. Из-за недавнего сбоя платформы Microsoft Azure в веб-приложении Dedoose, которое используется для анализа научных и исследовательских данных, была потеряна информация пользователей за период **более трех недель**. В системе хранилищ компании также произошел сбой, в результате чего пользователи, не выполнявшие резервное копирование данных, остались ни с чем.

Наиболее частые причины потери данных:

- Аппаратные и программные сбои
- Ошибки пользователей
- Отключения электроэнергии
- Уязвимости в системе безопасности и вредоносные программы
- Вредоносные действия недовольных сотрудников
- Потеря или кража устройств
- Стихийные бедствия

Традиционные методы защиты данных устарели и не годятся для современных сложных гибридных сред. Резервное копирование нового поколения в сочетании с устоявшимися практиками, такими как **правило «3-2-1»**, снижает эти риски. Человеку свойственно думать, что с его рабочими данными ничего не случится. Однако не стоит игнорировать реальность: **потеря данных — лишь вопрос времени.**

Факт №4

Современным данным требуется защита нового поколения



▲
Факт №3

ИТ-среды усложняются с каждым днем

Новые требования к ИТ:
виртуализация, облако, рост
объема данных, мобильные
устройства, BYOD

Традиционные решения
для защиты данных были
разработаны для прошлого,
когда *серверы были
физическими, облака были
только в небе, а телефоны
использовались только
для звонков.*

Решения для защиты
данных нового
поколения
отличаются от прежних

Факт №4

Современным данным
требуется защита
нового поколения

**Решения для защиты данных нового поколения
отличаются от прежних.** Они разработаны для
современных виртуальных, физических, облачных
и мобильных сред.

Решения нового поколения могут защитить любые данные,
в любой среде, в любом месте и на любых устройствах.
Технология создания образа диска в сочетании с
абстрагированием данных фиксирует и сохраняет все
данные в универсальном формате резервной копии.
Эти технологии копируют все рабочие данные, сохраняют на
любом устройстве или носителе, восстанавливают на любую
платформу, гипервизор или операционную систему
и обеспечивают доступ с любого удаленного устройства
для уменьшения простоев и улучшения показателей
директивного времени восстановления (RTO — Recovery
Time Objective) и директивной точки восстановления
(RPO — Recovery Point Objective).

Защита данных нового поколения отличается гибкостью и масштабируемостью, а также поддерживает:

Любые виды защиты

Резервное копирование данных, восстановление на «голое железо», миграция и развертывание систем

Любые устройства

Серверы и рабочие станции

Любые серверы

Виртуальные и физические

Любые среды операционных систем

Windows® и Linux®

Любые файловые системы

NTFS, ReFS, FAT16/32, Ext2/3/4, ReiserFS3, XFS, JFS и другие

Любые гипервизоры

VMware®, Hyper-V®, XenServer®, Red Hat® Enterprise Virtualization, Parallels и другие

Любые виды миграции

V2V, V2P, P2V, P2P

Любые приложения

Exchange, SQL Server®, SharePoint® и Active Directory®

Любые расположения

Облачные, локальные и удаленные хранилища

И наконец, решения нового поколения обеспечивают двойную защиту благодаря прозрачной интеграции с облаком. Таким образом становится гораздо проще следовать **правилу «3-2-1»**, согласно которому необходимо иметь три копии данных, две из которых сохранены на разных типах носителей, а одна копия хранится вне офиса.

Факт №5

Образы дисков обеспечивают быструю и полную защиту



▲
Факт №4

**Резервная копия
образа диска**

Резервная копия, которая содержит посекторную копию диска или тома в архивном формате. Как правило, копируются только сектора, содержащие данные.

Acronis Backup также позволяет создать полный образ, то есть копию всех секторов диска, при использовании с неподдерживаемыми файловыми системами.

Можно создать **полную копию пользовательского диска** или **целой системы**



Факт №5

Образы дисков обеспечивают быструю и полную защиту

С помощью однопроходного резервного копирования образа диска можно создать полную копию пользовательского диска или целой системы. Сюда входят операционная система, приложения, файлы, сценарии, данные конфигурации, пользовательские настройки и программы. В то время как методы резервного копирования на уровне файлов требуют переустановки операционной системы, восстановления файлов, а затем восстановления баз данных.

Это процесс может быть и более сложным, в зависимости от количества серверов в кластере. После завершения этих этапов необходимо заново применить все системные конфигурации. Однопроходное резервное копирование образа диска сводит этот процесс к единственному этапу восстановления.

Преимущества:

Любые виды защиты

Резервное копирование данных, восстановление на «голое железо», миграция и развертывание систем

Простота

Выполняется резервное копирование всех данных, включая менее очевидные, такие как исправления, пользовательские сценарии и программный код, что позволяет не тратить время на определение объектов защиты.

Миграция

Позволяет выполнять миграцию из резервной копии образа между любыми средами. Это миграция из виртуальной среды в виртуальную (V2V), из виртуальной в физическую (V2P), из физической в виртуальную (P2V) и из физической в физическую (P2P), а также все программные и аппаратные преобразования (например, Microsoft в Linux).

Гибкость

Позволяет выполнять восстановление из резервной копии образа на «голое железо». Если ноутбук сотрудника вышел из строя, ИТ-специалист может восстановить всю систему, файлы и приложения из любой точки

восстановления. Это может оказаться ключевым фактором в критической ситуации, когда важно максимально быстрое восстановление.

Скорость

Наиболее быстрый способ скопировать все возможные данные, что дает ИТ-отделу необходимую гибкость и скорость для решения любых проблем резервного копирования и восстановления в критических ситуациях. Восстановление также ускоряется, поскольку нет необходимости отдельно восстанавливать базы данных приложений.

Надежность

Технология однопроходного резервного копирования образа диска снижает риск ошибок и потери данных. Технологии многопроходного резервного копирования, напротив, могут усложнить процесс, не делая его надежнее, поскольку между проходами в файлы вносятся изменения. Восстановление также может замедлиться, так как необходимо восстанавливать несколько файлов резервных копий в правильном порядке. При однопроходном резервном копировании все данные сохраняются сразу и могут быть легко скопированы из единого файла резервной копии для быстрого восстановления.

Резервное копирование образа — это интеллектуальное копирование, которое распознает файловые системы, организацию и пользовательские настройки, что значительно ускоряет и упрощает восстановление. Эти преимущества крайне важны для занятых ИТ-специалистов с множеством других обязанностей. Однопроходное резервное копирование образа диска упрощает защиту систем и обеспечивает быстрое восстановление приложений в критических ситуациях, когда даже короткое время простоя угрожает производительности.

Факт №6

Восстановление важнее всего

▲
Факт №5

Один час простоя может
вызвать серьезные
финансовые последствия

Средняя стоимость одного
часа простоя:

\$6 900
▶ для **малых***
компаний

\$74 000
▶ для **средних****
компаний

\$1,13
▶ **миллионов**
для **крупных*****
компаний

- * менее 100 сотрудников
- ** от 100 до 1000 сотрудников
- *** более 1000 сотрудников

Факт №6

Восстановление важнее всего

Будем откровенны: защита данных не исчерпывается созданием копий для заполнения пространства в хранилище. Смысл защиты данных в восстановлении. Если что-то пойдет не так, ИТ-отдел должен обеспечить скорейшее возобновление работы и свести к минимуму возможные потери.

Один час простоя может вызвать серьезные финансовые последствия. Согласно [исследованию группы Aberdeen](#), час простоя в среднем стоит малому предприятию (менее 100 сотрудников) 6 900 долл. США, а среднему (от 100 до 1 000 сотрудников) — 74 000 долл. США. Для крупных компаний со штатом более 1000 сотрудников средняя сумма составляет 1,13 миллиона долл. США в час.

Однако не все данные одинаково важны, поэтому компаниям необходимо решить, какие типы данных должны восстанавливаться и сколько времени может пройти до возобновления нормальной работы.

Эти показатели также называются **директивная точка восстановления (RPO)** и **директивное время восстановления (RTO)**.

RPO: за какой период компания может себе позволить потерять данные при восстановлении. Это может быть одна минута, пять часов или один день, в зависимости от отрасли или подразделения.

RTO: сколько времени и усилий требуется для восстановления всех данных и возобновления работы систем. При определении RTO стоит обратить внимание на **фрагментарное восстановление**. Эта тактика позволяет сэкономить время, восстановив только нужную часть данных (например, одно сообщение электронной почты или почтовые файлы одного пользователя), не останавливая службу Microsoft Exchange для всей компании.

Сроки RPO и RTO для разных систем будут отличаться. К примеру, возьмем систему оплаты труда. Если происходит потеря данных, важно возобновить работу системы, но восстановление вполне может занять пару дней, при условии что это не день выдачи зарплаты. В то же время, для большинства компаний недопустима остановка системы CRM. Необходимо возобновить ее работу как можно быстрее, чтобы сотрудники отдела продаж имели доступ к истории звонков и могли заключать новые сделки.

Однопроходное резервное копирование образа диска дает необходимую гибкость и контроль для восстановления данных приложения без необходимости восстанавливать весь диск или том. Это ускоряет процесс восстановления наиболее важных данных, за которым следует восстановление частей с большими сроками RTO.

Существуют другие технологии нового поколения, уменьшающие RTO. Одной из них является Acronis Active Restore. Эта функция позволяет возобновить работу системы сразу же после запуска восстановления. Система загружается из **резервной копии**, после чего машина готова к работе и предоставлению необходимых сервисов. Данные, которые требуются для обработки входящих запросов, восстанавливаются с наивысшим приоритетом; все остальное восстанавливается в фоновом режиме. Это уменьшает время простоя и позволяет сотрудникам продолжать работу с наиболее важными данными.

Руководители ИТ-отделов должны не только найти решения, подходящие для текущей среды. Они должны проанализировать данные, выбрать наиболее важные и найти лучшее решение, удовлетворяющее конкретным требованиям каждого подразделения, одновременно сократив издержки.

Факт №7

Гибкость имеет значение



▲
Факт №6

Почти
50%

ИТ-компаний
имеют виртуальную,
физическую
и облачную
инфраструктуру

Всем нравятся
решения, которые
«сидят как влитые»

Факт №7

Гибкость имеет значение

Всем нравятся решения, которые «сидят как влитые».

ИТ-специалисты хотят иметь все необходимые функции, не переплачивая за ненужные усложнения. С традиционными решениями для защиты данных компаниям приходилось выбирать между доступными, но неполными узкоспециализированными продуктами и многофункциональными, но сложными и дорогими платформами. С современными решениями ИТ-специалисты получают лучшее от обоих вариантов: высококлассные отдельные продукты, которые легко объединяются в простое, полное и безопасное решение.

Возьмем ИТ-администраторов, отвечающих за корпоративный сервер Exchange. Им необходимо решение, оптимизированное для Exchange, которое обеспечивало бы несколько вариантов восстановления, от отдельного сообщения или почтового ящика пользователя до сервера целиком.

Или возьмем системных администраторов, отвечающих за виртуальную среду компании. Им необходимо решение, оптимизированное для конкретных гипервизоров, используемых в компании, например VMware, Microsoft, Citrix, Red Hat или др. Администраторам нужно решение для резервного копирования как виртуальных машин, так и физического сервера, на котором они расположены.

Решения для защиты данных нового поколения позволяют покупать только то, что необходимо. В частности, это относится к специалистам, отвечающим за отдельный рабочий процесс. Кроме того, решения нового поколения позволяют расширять ИТ-инфраструктуру без предварительных вложений в дорогую и сложную в обращении платформу. Таким образом ИТ-администраторы, управляющие рядом различных рабочих процессов, могут использовать унифицированную консоль управления для выполнения всех своих задач. Даже если среда расширяется и усложняется, стратегия защиты данных остается простой и всеобъемлющей.

Факт №8

Слишком сложное не будет работать

▲
Факт №7

Самая большая проблема — это **сложность резервного копирования**

Рабочим специалистам нужна **простота использования**

Факт №8

Слишком сложное не будет работать

Данные крайне важны для компании, но давайте посмотрим правде в глаза:

ИТ-специалисты — занятые люди, у них нет времени возиться с системами резервного копирования и восстановления, да они и не должны этого делать. Более того, у многих мелких компаний нет выделенного ИТ-персонала, и резервным копированием, помимо прочих обязанностей, занимаются обычные сотрудники.

В каждой из этих ситуаций компаниям требуется простое и надежное решение, работающее с первого раза, чтобы избежать чрезмерной потери времени и дорогостоящих ошибок с критически важными данными.

В качестве примера можно привести одного из клиентов Acronis, компанию Ashby Cross Company, которая производит оборудование для распределения жидкостей и клеящих веществ. Их генеральный директор, имеющий большой опыт в области техники, выполняет обязанности главы ИТ-отдела в компании со штатом 20 человек.

Защита данных должна быть простой и быстрой, чтобы он мог тратить время на управление работой компании, а не файлами и приложениями. И эта защита должна работать. Любые сложности или ошибки в процессе резервного копирования впоследствии могут помешать успешному восстановлению.

“ Как правило, процесс восстановления — это сильный стресс для ИТ-специалистов. Ставки высоки, работа под угрозой, а тут еще руководители в панике спрашивают, почему не работает корпоративная почта или почему исчезла важная финансовая информация.

Кроме того, невозможно предугадать, когда произойдет авария. Если это случается посреди ночи, ИТ-администратора, отвечающего за восстановление, вытаскивают из постели, чтобы немедленно поднять систему для сотрудников, которые не могут закончить работу где-то на другой стороне планеты.

В таких ситуациях самое важное — простота.

”

Сергей Кандауров, топ-менеджер, отвечающий за выпуск продуктов Acronis.

Для успешного восстановления данных ИТ-специалистам необходимы технологии, обеспечивающие простое выполнение сложных задач. Решения также должны включать краткие и понятные инструкции по управлению процессом восстановления, чтобы в критической ситуации непрофессионал мог справиться не хуже опытного специалиста. Методы защиты данных, не удовлетворяющие этим условиям, просто не будут работать. А если они не будут работать, то данные — и потенциально вся компания — окажутся под угрозой.

Acronis

О компании Acronis

Acronis устанавливает стандарты защиты данных нового поколения в своих решениях для резервного копирования, аварийного восстановления и защищенного доступа. Основанные на системе AnyData и отличающиеся своей технологией создания образов, решения Acronis обеспечивают простое, полное и безопасное резервное копирование всех файлов, приложений и операционных систем в любых средах — виртуальных, физических, облачных и мобильных.

Компания Acronis была основана в 2002 году, сейчас решения Acronis защищают данные более 5 миллионов пользователей и 300 000 компаний в 130 странах. Используя более 100 патентов, продукты Acronis были названы продуктом года по версии Network Computing, TechTarget и IT Professional и предоставляют целый ряд функций, включая миграцию, клонирование и репликацию.

Дополнительную информацию см. на сайте www.acronis.ru.

Подпишитесь на Acronis в Твиттере: http://twitter.com/acronis_russia.

© Acronis International GmbH, 2002–2014. Все права защищены.

Наименование Acronis и логотип Acronis являются товарными знаками компании Acronis International GmbH.

Другие упомянутые здесь наименования могут являться товарными знаками или зарегистрированными товарными знаками их владельцев и должны рассматриваться соответствующим образом. Возможны технические изменения и отличия от иллюстраций; ошибки исключены. 2014-07