

Как интернет-провайдеру увеличить прибыль на 10% или сага о резервном копировании

Почему только на 10%, спросите вы? Потому что увеличить на 100% во многих случаях невозможно - уже подключен максимум клиентов, заняты все каналы, и резкий рост прибыли возможен только при переходе на новый уровень, а на это может не быть ни воли, ни денег.

Статья написана в предположении, что провайдер зарабатывает на среднем и малом бизнесе, так что если вы Ростелеком или Газком, или ваши клиенты крупны, как Сбербанк, ваш опыт может отличаться. Если вы зарабатываете на физ.лицах - считайте, что все, описанное в статье, и к вашим клиентам относится, только они еще более беспечны и скупы, чем малый бизнес.

Хочет ли интернет-провайдер развивать сопутствующие услуги?

Большинство провайдеров это делает. Чаще других услуг встречаются цифровое телевидение, всякого рода антивирусная защита, виртуальные телефонные номера, несколько реже - услуга видеонаблюдения. Стало быть, даже если не хочет - жизнь заставляет.

Резервное копирование: обзор ситуации на российском рынке

Может ли такой сопутствующей услугой быть резервное копирование? Важный комментарий: современное резервное копирование в идеале должно быть полностью автоматическим, совершенно безопасным, абсолютно надежным, быстрым и простым и в создании резервной копии, и в ее переносе в хранилище, и в восстановлении.

Резервное копирование может быть выгодной услугой, хотя директора некоторых провайдеров интернет в Петербурге в личных беседах говорили мне, что не считают эту услугу коммерчески привлекательной: клиенты хотят платить как можно меньше, а затраты на ввод услуги в строй и поддержку значительные. Ниже я покажу, что оба сомнения напрасны: и клиенты готовы платить, и затраты можно уменьшить почти до нуля.

Кто в России уже предлагает резервное копирование?

В основном - хостинг-провайдеры и дата-центры (ЦОД). Я не планирую здесь делать детальный обзор существующих сервисов. Большинство из них не российские, и их обзор сделан достаточно давно, и обновляется, например, в Википедии, а для технических спецов есть и поучительная дискуссия на Хабре .

Главным конкурентом любой компании, взявшейся зарабатывать на резервном копировании в России, являются бесплатные или цинично недорогие западные службы: mozy.com, Dropbox, Amazon - из известных западных, Rackspace - из малоизвестных в России, но известных на западе.

Однако у любой западной службы есть два, а то и все три недостатка из самых частых трех:

1. скорость доступа к службе невысока (либо при передаче данных на ее серверы, либо при скачивании их оттуда, либо в обе стороны);
2. физически данные хранятся не в одном городе с клиентом (это хорошо, если клиент параноик, но плохо, если надо восстановить 10 Тб данных - к местному провайдеру можно съездить с трехтерабайтными дисками в портфеле, из-за рубежа придется заунивно качать данные несколько дней - и хорошо, если не недель);
3. если вам потребуется помощь в настройке, а общаться по-английски вы не привыкли, то поможет вам разве что Google Translate.

Несмотря на это, компаний, которые в России продают резервное копирование как услугу, не так и много. Быстрый поиск в Яндексe даст, пожалуй, два-три имени, среди которых в основном будут хостинг-провайдеры и дата-центры, например Selectel и Infobox.

Почему не интернет-провайдеры?

Провайдеры интернет реже предлагают услугу резервного копирования, и сходу я смог найти всего одного такого провайдера, совсем неглобального - [ТТК Калининград](#).

Конечно, клиент хостинга охотнее подпишется на резервное копирование, так как его данные и так уже доверены хостинг-провайдеру, и об их ценности он хорошо осведомлен. Однако хостинг нужен гораздо меньшему количеству людей, чем автоматические резервные копии, так что потенциал роста клиентской базы есть. Клиентами интернет-провайдеров в той или иной степени являются десятки миллионов людей в России (и сотни тысяч компаний). Хостинг нужен явно меньшему количеству клиентов - хорошо если их число перевалит за два миллиона.

Причин того, что интернет-провайдеры не предлагают резервное копирование наперебой, несколько:

1. интернет-провайдер не готов рекламировать услугу резервного копирования клиентам, считая, что многие из них не понимают ее смысла, недооценивают риски потери информации;
2. интернет-провайдер не исчерпал еще другие, более легкие для него, способы роста заработка: увеличение скорости доступа, подключение цифрового ТВ, интеграция сетей мобильной и фиксированной связи;
3. интернет-провайдер знает, что его клиенты используют свою собственную инфраструктуру для резервного копирования (например, дублируют резервные копии в иностранные офисы, купили оборудование для резервирования на месте и т.п.).

Готов ли клиент платить за такую услугу?

Не претендующий на репрезентативность опрос знакомых владельцев малого и среднего бизнеса говорит "ДА". Экспертная оценка, интернет-провайдеры и сами потенциальные клиенты говорят, что частные лица готовы платить от 50 до 100 руб. в месяц за резервное копирование своих данных, а малые и средние компании - от 1000 до 3000 руб. Естественно, это средние цифры: модный дизайнер интерьеров, работающий на дому, заплатит и 5000 руб в месяц за то, чтобы его эскизы на 200 000 руб. не пропали по глупой случайности перед сдачей заказчику.

Окупит ли спрос затраты на предложение?

Вероятно, да. Расчеты имеются в последней части статьи на примере конкретной реализации, которую мы сами сделали.

Подход разных компаний к резервному копированию

В этом разделе мы говорим о малых и средних компаниях - частные лица обычно значительно более легкомысленны (или худо осведомлены о необходимости резервного копирования).

Самый распространенный вариант - копирование на флэшки и внешние диски, подключаемые по USB.

Следующий - копирование на отдельный сервер в офисе (довольно часто он играет и другие роли в сети, например, принт-сервера или почтового сервера, а бэкап - это его неосновная нагрузка). Реже копирование делают на сервер в другом офисе, а зря: правило географического удаления резервной копии от оригинала никто не отменял!

Значительно реже резервные копии делают на внешнее устройство типа ленты или в специальное сетевое хранилище (NAS).

И наконец хит сезона - облачное хранилище (Amazon, DropBox, Google Drive, Яндекс.Диск и т.п.) Облачным хранилищам доверяет свои данные абсолютное меньшинство малых и средних компаний.

Примеры из жизни

Все примеры - совершенно реальные, я лично знаком с руководством каждой из описанных компаний, но названия не называю - компании скромные, делятся информацией на условиях анонимности. Большинство расположено в Петербурге.

1. Совсем малое предприятие: офис из пяти человек, занимаются проектированием газовых котельных для средних и крупных объектов (больницы, заводы, коттеджные поселки и проч.) В офисе 5 компьютеров, объем важных данных - десятки гигабайтов, резервное копирование не делается вообще.

Почему так? Так вышло. Офис обслуживается приходящим сисадмином, регулярно копирование делать некому, сотрудники разбираются только в том CAD'e, в котором они делают проекты, а

копированием заниматься некогда. Программ автоматического копирования они не знают. Однако важность копирования понимают, и готовы платить от 1000 до 3000 рублей в месяц тому, кто им все настроит и будет надежно хранить копии. Скорее всего, за эти деньги ждут и восстановления данных из копий, если вдруг что случится.

Это почти идеальный клиент для услуги резервного копирования: в меру мотивированный, не имеющий работающего решения из-за нехватки времени и знаний.

2. Предприятие побольше: компания, которая делает пластиковые карточки (скидочные, рекламные), а также уличные вывески.

В офисе работают человек 20, есть еще производство, но оно данные не генерирует, все задачи для производства создаются на компьютерах - в Corel Draw и CAD'ax. Данных довольно много, есть значительный по размеру архив за прошлые годы. В сумме - сотни гигабайт важной информации.

Резервное копирование делает в конце дня лично владелец компании, он же ген. директор. Данные списываются на внешний диск, диск едет в портфеле домой к директору. Там на полочке стоит еще 6 дисков - ротация. Каждый диск имеет наклейку "ПН", "ВТ", "СР" - и так далее, чтобы не перепутать.

Отчего так? Владелец - контрол-фрик, доверяет только себе, считает, что так надежнее всего. Это не худший вариант, но и не лучший: очевидные недостатки читатель может просчитать сам, я помолчу, чтоб не каркать.

3. Предприятие еще крупнее: компания, занимающаяся медицинскими исследованиями, пять офисов в разных странах, более 400 человек персонала, 200 из них - в центральном офисе. Ценных данных - десятки гигабайт, ежедневный прирост - сотни мегабайт, а то и гигабайты. Этой компании сейчас уже нет - сменила владельцев и схему копирования, вероятно, тоже, так что опишу, как там было дело в начале 2000-х.

Все данные реплицируются между офисами и по ночам пишутся на ленты в двух офисах из пяти - в разных странах. Для бэкапа используется Veritas под Windows и rsync под Linux.

Схема кажется надежной, но на самом деле она достаточно сложна и сильно зависит от человеческого фактора: если сисадмин ошибется с тем, какую ленту вставить в стриммер в очередной день, важная информация может быть перезаписана, а если не обратит внимания на сообщение об ошибке - вообще не запишется.

4. Гостиница - 5 рабочих мест.

Резервные копии пишутся на внешний USB-диск.

Почему так? Данных немного, с ними постоянно работают, сбой рабочей копии или внешнего диска заметят сразу, а вероятность одновременного сбоя и того, и другого считают низкой. Надежность решения невелика, хотя если персонал знает, что "при пожаре надо звонить 01, брать вон ту коробочку и бежать из здания", то все не так уж и плохо.

5. Большая проектировочная контора - 70 компьютеров. Бэкапы делаются автоматически на центральный сервер, выделенный для копий. Риск потери данных не убирается до нуля (особенно если выделенный сервер в том же офисе), но все же лучше, чем полное отсутствие бэкапа.

Центральный сервер, разумеется, укомплектован RAID-массивом.

Может ли интернет-провайдер заработать на резервном копировании?

Почему бы клиентам провайдера не использовать бесплатные или очень дешевые службы облачного хранения, такие как Amazon и DropBox? Подробно об этом сказано ниже, а вкратце потому, что это дольше, дальше, неудобно при серьезных авариях, сложнее настроить или плохо автоматизируется. Опять же, любой способ копирования кто-то должен посоветовать. Вы часто видите на российских улицах и в метро рекламу DropBox и Amazon? А Skynet, Megafon, Beeline, InterZet и многие другие рекламируются весьма активно - значит, можно рассказать клиентам и о копировании.

В чем смысл для провайдера предлагать услугу резервного копирования своим клиентам?

Все клиенты делятся на три категории: те, у кого копирование не делается вообще, те, кто думает, что его система копирования достаточно хороша и те, у кого она действительно хороша.

К последним часто относятся филиалы иностранных компаний, хотя и у них система может быть

неидеальна. Впрочем, им все равно предлагать копирование как услугу бессмысленно: местный офис как правило не имеет ни права, ни желания что-то менять в корпоративной политике ИТ, а головной офис считает, что у них все настроено правильно и так.

Первые две категории - это потенциальные клиенты, которые могут приносить деньги провайдеру, если решат хранить свои резервные копии у него.

Сколько денег реально собирать с клиентов? Как уже отмечено выше, провайдеры и клиенты сходятся в том, что малое и среднее по размеру юрлицо готово платить 1000 рублей в месяц (многие готовы и больше), а физлицо - максимум 100 рублей в месяц (реалистичнее - 50 рублей). Такая разница легко объяснима: физ.лицо обычно ниже ценит файлы на своем компьютере (а зря!), завышает легкость их восстановления, ошибочно полагает, что восстановить файлы можно дешево.

Кстати, восстановление данных с дохлого жесткого диска в самой лучшей из известных мне компаний по восстановлению данных - Q-Lab в Петербурге - обойдется тысяч в 10-15 рублей минимум. Сумма, подъемная для большинства даже мелких компаний, но чувствительная для большинства физлиц.

С другой стороны, физлица еще хуже разбираются в ИТ, чем руководители малых и средних компаний, а большинство из них сможет прожить день-другой без своих данных, поэтому даже грамотные пользователи могут предпочесть более дешевые хранилища, несмотря на низкую скорость доступа к хранящимся там данным и долгое восстановление.

Однако некоторые провайдеры считают, что до 10% их клиентов могли бы купить резервное копирование у них, если бы оно настойчиво предлагалось. Стоит ли за эти деньги заняться просвещением своих клиентов? Посмотрим: средний интернет-провайдер обслуживает около 10000 клиентов, допустим, что 1000 из них - юридические лица, остальные - физические. Так мы получаем для услуги резервного копирования 100 клиентов-юрлиц, 900 - физлиц. $100 \times 1000 + 900 \times 100 = 190000$ рублей. Стоит ли овчинка выделки, если доход такого провайдера от основной услуги - 2-3 миллиона рублей в месяц?

Не каждый провайдер считает, что стоит, и я бы с интересом прочел в комментариях мнение тех, кому есть что добавить к аргументам против, равно и мнения тех, кто выступает за эту идею.

Методика продажи услуги клиенту

Чтобы провайдеру было легче предлагать услугу резервного копирования клиенту, я решил собрать возражения клиентов в короткий раздел. Провайдер может и должен на них уверенно отвечать.

Чего боятся те, кто резервную копию за пределами офиса не делает?

1) Важные данные будут переданы (или проданы) конкурентам.

На самом деле данные при резервном копировании шифруются на компьютере клиента до того, как будут отправлены провайдеру; известные мне решения для резервного копирования используют сложные алгоритмы шифрования. Так, придуманное нами решение (описано в конце статьи) использует AES-256, тот самый алгоритм, которые за несколько лет не смогли взломать ни спецслужбы Бразилии, ни ФБР США.

Таким образом, даже если прямо за стенкой вашего офиса стоит устройство, копирующее все проходящие через него данные на сервер конкурентам, без знания пароля эти данные - бессмысленный набор символов. Придумайте хороший, сложный, многословный, незапоминаемый и неподбираемый пароль, запишите его на бумажку, убедитесь, что за вами нет слежки, обратитесь инкогнито к нотариусу в стране, властям которой вы доверяете, и положите эту бумажку в несгораемый сейф этого нотариуса. Можно сохранить пароль и с меньшими предосторожностями - главное, чтобы ваши недоброжелатели его не нашли.

И помните, пожалуйста: почти все серьезные утечки важной информации - результат социальной инженерии, а вовсе не хищений данных из резервных копий. Вероятность того, что вашего инженера с важной флэшкой в кармане банально ограбят на улице, напоят и обчистят в баре, соблазнят и вытянут из него важные данные, или посадят ему в компьютер троянскую программу, значительно выше, чем то, что вашего провайдера будут взламывать, чтобы добыть нужную информацию.

2) Важные данные про... скажем так, долбят, и никто и не заметит, пока не грянет гром.

Да, это возможно. Никто не может быть уверен, что замененный устаревший жесткий диск, на

котором хранилось что-то важное, будет технически грамотно уничтожен так, чтобы данные никто не смог восстановить. Однако это относится к компьютерам в офисе клиента, а не к серверам провайдера. То, что в зашифрованном виде лежит там, можно хоть в газете "Правда" опубликовать - без пароля оно не имеет никакого смысла. А пароль следует держать в секрете.

3) Данные будут украдены рейдерами, от которых нет защиты.

Ответ аналогичен ответу на первые два страха. В распоряжении рейдеров окажется зашифрованная копия, а не данные. Да, они могут схватить сисадмина компании, чьи это данные, и под пытками заставить выдать пароль. И даже сделать то же самое с генеральным директором, если пароль знает только он. Но зачем так сложно? Рейдерам такого типа проще воздействовать на директора или владельца напрямую - способы воздействия заинтересованный читатель наверняка знает из общедоступных новостей.

4) Данные вне офиса - это табу ("я всю жизнь проработал на военном заводе и так привык").

Никогда не говори "никогда", как говорил один известный киногерой из числа профессиональных разведчиков. Просто считайте частью своего офиса ту область диска на сервере провайдера, где хранится ваш зашифрованный архив.

5) А что, если провайдер неожиданно разорится и сгинет?

Ничего страшного. Если вы храните данные далеко за рубежом (например, в DropBox'e), то о его разорении вы узнаете из газет, а о том, что ваш интернет-провайдер перестал работать, вы узнаете первым - отключится доступ в интернет. К тому же, если инженеры и менеджеры провайдера - адекватные люди, есть шанс, что данные вам дадут переписать на ваши диски, даже если провайдер разорится. Опять же, следить за ситуацией в компании, которая продает вам доступ в интернет, вашей службе безопасности проще, чем за DropBox'ом.

Как провайдер может убедить клиента, что овчинка стоит выделки?

Попробуйте аргументы из наших статей.

Конкретное решение для провайдеров интернет

Мы сделали готовую систему, которая начинает приносить деньги сразу после установки. Она состоит из четырех простых компонент: хранилища, API для примитивных действий с ним (управление пользователями, проверка занятого и свободного места), примера реализации веб-сайта, который работает с этим API, и клиентского ПО, которое надо установить на те компьютеры, с которых будет выполняться резервное копирование.

Хранилище - это четное количество (минимум - два) серверов Linux с файловой системой Gluster на них. Данные зеркалируются, т.е. если у вас два сервера, на каждом из них хранится своя копия данных - для надежности.

Как это работает?

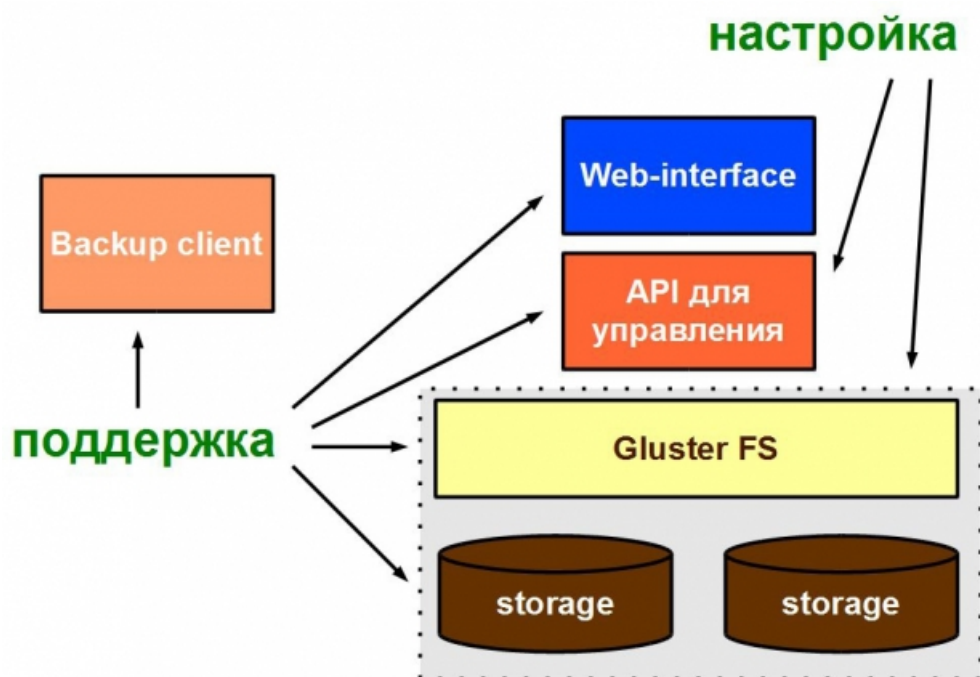
Мы бесплатно настраиваем серверы провайдера для надежного хранения данных. Клиенты провайдера нажимают кнопку "включить услугу резервного копирования" (или как-то иначе ее активируют из личного кабинета на сайте провайдера). Получают имя и пароль, скачивают клиентскую программу для Windows (или Linux), запускают ее, указывают, в каких папках у них лежат данные, подлежащие копированию, каким паролем шифровать копии, и в какое время надо запускать копирование. Все остальное программа копирования сделает сама.

Клиенты платят провайдеру по тарифу, который придумает провайдер, провайдер платит нам за обслуживание серверов, где хранятся копии.

Вот простая таблица:

что делает провайдер	что делает Semonix
----------------------	--------------------

что делает провайдер	что делает Semonix
находит 2 сервера находит среди своих клиентов тех, кто готов платить за резервное копирование предлагает клиентам услугу резервного копирования (ориентировочно: частным лицам — от 50 до 100 руб. в месяц, юр. лицам — от 1000 до 3000 руб. в месяц) собирает деньги с клиентов и платит Semonix за обслуживание серверов и клиентского ПО	настраивает на этих серверах Linux + Gluster передает провайдеру клиентское ПО для резервного копирования в автоматическом режиме устанавливает сверхлегкий веб-сервер у провайдера для того чтобы провайдер мог управлять пользователями и ресурсами файловой системы Gluster через API обслуживает ПО серверов (обновления, безопасность) и отвечает на вопросы по клиентскому ПО



Сколько это все стоит? Настройку для первых заказчиков делаем бесплатно, обслуживание стоит 20 000 рублей в месяц за два сервера, подробности - на сайте.

Клиентская программа Semonix Backup Client сделана на основе Duplicati, это ПО с открытым исходным кодом, желающие могут скачать код из Сети и скомпилировать у себя. Лицензия GPLv2.

Выводы

Спрос на услуги резервного копирования со стороны малого бизнеса и частных лиц будет расти, и так считают как хостинг-провайдеры, уже вложившие немалые деньги в создание своих собственного программного обеспечения для копирования, так и некоторые провайдеры интернет. Среди хостинг-провайдеров назовем еще раз Инфобокс, а среди дата-центров - Селектел. У них довольно приличная репутация и вряд ли их стоит подозревать в бессмысленном транжирстве.

Для создания полноценной системы автоматизированного резервного копирования в любом случае требуются те независимые компоненты, которые мы собрали в свою собственную систему: хранилище с резервированием (избыточностью), веб-интерфейс к нему, программа резервного копирования для клиентов.

Инфобокс и Селектел разработали свои решения с нуля, другие провайдеры имеют возможность либо повторить их путь (а это сотни тысяч рублей вложений и месяцы разработки и тестирования), либо заказать готовое решение. Был бы рад предложить для сравнения не только наше решение, но другого такого продукта просто не знаю. Вероятно, многие провайдеры таких услуг делают свои собственные версии, что в современном мире трудно считать лучшим выходом: быстрее и дешевле

использовать созданное другими, чем все делать самим с нуля.

Итак, вы согласны, что сможете заработать на резервном копировании? Найдите минимум 20 клиентов на эту услугу среди тех, что у вас уже есть - и можно начинать считать шуршащую в вашем кармане выгоду.