Игорь Афонин

Непрерывность бизнеса и финансовые последствия простоев

Информационные технологии (IT) всё больше проникают во все аспекты нашей жизни и общества. При постоянно растущей зависимости предприятий от их информационных систем и хранящихся в электронном виде данных потенциальные издержки, возникающие вследствие простоев из-за отказов в IT-системе и неспособности обезопасить свои данные, могут быть огромными.

С целью выполнения оценки рисков и экстраполяции потенциальных убытков для бизнеса от различного вида простоев в целом и от простоя информационной системы в частности можно обратиться в специализированные консалтинговые компании, которые проведут экспертизу и дадут рекомендации. Но весьма часто многие компании не обладают достаточным бюджетом для проведения такой экспертизы, а IT-менеджеры и специалисты компании в большинстве случаев не имеют средств и опыта для оценки реальных рисков, пересчёта их в денежный эквивалент и донесения результатов до руководства и владельцев компании.

Поэтому, как показывают опросы, большинство IT-руководителей организаций не располагают информацией о стоимости простоя компании и вследствие этого не могут обосновать необходимость принятия мер для обеспечения бесперебойного функционирования IT-системы. Можно считать, что обеспечение высокой доступности информации является страховкой бизнеса компании от последствий, связанных с простоем IT-системы.

Основные понятия доступности информации

У большинства организаций определение понятия доступности информации лежит где-то в диапазоне между множеством часов простоя с существенной потерей данных и безотказной работой в режиме 24/7 с нулевой потерей данных. На самом деле определение необходимого уровня доступности информации будет зависеть от потребностей бизнеса, требований к данным и приложениям и организационной структуры компании. Цель должна заключаться в том, чтобы не позволить последствиям неизбежного простоя ИТ-системы повлиять на бизнес-процессы.

Рис. 1. Доступность информации/непрерывность бизнеса

Для начала определимся с понятиями: что такое послеаварийное восстановление, высокая доступность, непрерывные операции, непрерывная доступность и непрерывность бизнеса (рис. 1).

Аварийное восстановление (Disaster Recovery), или, точнее, послеаварийное восстановление – это полное восстановление после сбоев, проведение восстановительных работ для возобновления работы. Практически сводится к восстановлению работы оборудования из комплектов ЗИП, а информации – из резервной копии. Это понятие применимо для внеплановых простоев.

Высокая доступность (High Availability) – это способность устранения сбоев и отказов приложений с минимальным ущербом для бизнеса. Можно сказать, что высокая доступность является одним из уровней аварийного восстановления. Используется для критически важных операций, когда восстановление с помощью ЗИП и резервных копий неприемлемо. Для обеспечения высокой доступности используется принцип избыточности, когда рабочая нагрузка с отказавшего компонента может быть быстро перенесена на резервный без остановки работы системы, операции и восстановления после сбоев сервера. Используется при плановых и внеплановых простоях.

Непрерывность операций (Continuous Operations) – это способность выполнения техобслуживания приложений и серверов, а также резервного копирования с минимальным ущербом для поддерживаемых бизнес-функций. Ориентирована исключительно на устранение простоев, связанных с плановыми событиями.

Непрерывная доступность (Continuous Availability) означает непрерывную доступность важнейших бизнес-функций. Она ориентирована на устранение плановых и внеплановых простоев, а также на защиту серверов, отдельных офисов и площадок организации и компании в целом.

Непрерывность бизнеса (Business Continuity) ориентирована не только на устранение рисков простоя IT-активов, она включает в себя людей и процессы для обработки внеплановых событий, влияющих на весь бизнес или регион, в котором работает компания. Обеспечение непрерывности бизнеса включает в себя IT-активы, а также запланированные процессы для оповещения работников и клиентов об аварийной ситуации, подготовку и тестирование планов готовности к аварийным ситуациям, а также проверку этих процессов для обеспечения эффективности.

Следует отметить, что надёжность (*Reliability*) и доступность (*Availability*) не являются синонимами (рис. 2). Надёжность относится к промежутку времени между отказами (MTBF) аппа-

Рис. 2. Взаимосвязи доступности

ратной части системы. Доступность означает, что данные и приложения доступны пользователям при необходимости, без учёта того, что может привести к их недоступности. Следовательно, надёжность является частью доступности. За счёт использования специальных технических решений, таких как резервирование компонентов, мониторинг и диагностика состояния системы, а также специального высоконагруженного тестирования при производстве компонентов и изделий, можно считать, что большинство аппаратных средств в настоящее время очень надёжны, об этой проблеме можно практически не беспокоиться. Главной проблемой остаётся именно обеспечение доступности.

Решение проблемы доступности предполагает также решение проблемы надёжности, но только в качестве составляющей более важных вопросов. Значительное улучшение аппаратных средств и надёжности программного обеспечения лишь немного снизит общее количество часов простоя в течение года, потому что по сравнению с другими факторами, такими как техническое обслуживание аппаратных средств, программного обеспечения и баз данных, ненадёжные системы являются причиной лишь небольшого процента простоя. Значительное улучшение доступности возможно только путём устранения всех причин недоступности и включает повышение надёжности.

Доступность информации

Доступность информации охватывает все стороны IT-системы, включая приложения, данные, серверы, операционные системы, процессы и инфраструктуру (рис. 3), и предусматривает последовательный предсказуемый доступ к любым данным или приложениям, вне зависимости от того, откуда, когда и как пользователи запрашивают их.

Доступность информации не означает доступности IT-системы в течение 100% времени. Например, организации, которым не нужны их системы с полуночи и до 6 часов утра, не будут беспокоиться о простое в течение этих часов. Тем не менее, достижение уровня оптимальной доступности информации, который подходит для бизнеса, означает, что данные и приложения, определённые как крайне важные, будут доступны в течение заранее определённых часов, что может означать 24/7, 24/5, 20/7, 12/6 или любое сочетание часов и рабочих дней, которое соответствует бизнес-целям организации.

Некоторые организации беспокоятся лишь о потере данных и используют резервное копирование для их защиты. Такое решение будет неполным, так как данные нужно не только сохранять, но и обрабатывать: получать из них информацию, необходимую для бизнес-процессов, то есть необходима защита от сбоев и данных, и приложений. Конкретные требования будут определяться бизнес-стратегиями и целями организации. Например, интернет-магазин, вероятно, не захочет потерять какие-либо данные, так как это может означать потери продаж и резко отрицательное отношение со стороны клиентов. В то же время логистическая компания или производитель, работающий в три смены, и высококомпьютеризированное производство будут больше беспокоиться о потере доступа к приложениям.

Исходя из сказанного, можно утверждать, что особое значение принимает планирование информационной доступности, которая обеспечивает системный и целостный подход ко всей информационной инфраструктуре предприятия. План предназначен для оценки уязвимых мест доступности, оценки масштаба и вероятности угроз, а также выявления и внедрения решений, обеспечивающих окупаемость инвестиций.

Системный подход необходим, потому что в любом бизнесе сегодня, особенно в малом и среднем, больше неприемлема или недостаточна постоянная доступность только одного приложения или защита комплексного плана аварийного восстановления. Необходимо учитывать данные и сети, которые интегрируются с этим приложением, а также зависимость приложения от других факторов.

Целостный подход необходим, потому что отказ какого-либо одного элемента может послужить причиной отказа всего оборудования. Поэтому концентрация внимания только на одном компоненте, например только на жёстких дисках, блоке питания или процессорах, лишь незначительно улучшит доступность. Возможно, приложения не будут работать без данных и объектов, и наоборот. Для определения общесистемных требований к доступности в процессе планирования должны рассматриваться все данные и приложения по предприятию в целом. В этом контексте данные не означают просто бизнес-данные. Они включают в себя все данные по безопасности, данные промежуточной области связующего ПО, очереди данных и другие системные данные, требуемые для поддержки приложений в рабочем состоянии в соответствии со спецификациями.

Простой определяется как любое прерывание IT-процессов, когда пользователи не могут получить доступ к данным, приложениям или сетям или использовать их. Существует два типа простоев.

- *Внеплановый простой* – непредсказуемое событие, которое служит причиной остановки работы; обычно такой простой связан с производственной аварией (прорыв водопровода или отопления, отключение электроэнергии или короткое замыкание и перегрузка в системе электропитания), со стихийным бедствием или ошибкой, вызванной человеческим фактором (рис. 4). На долю таких простоев, как правило, приходится не более 10%.
- *Плановый простой* происходит, когда IT-персонал намеренно останавливает системы, базы данных, приложения или

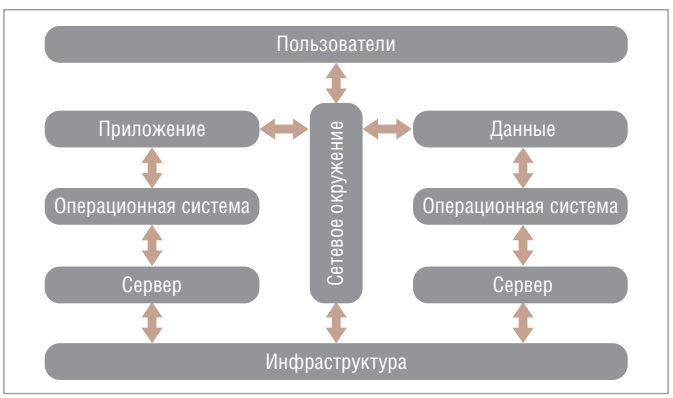

Рис. 3. Двухточечное представление IT-системы

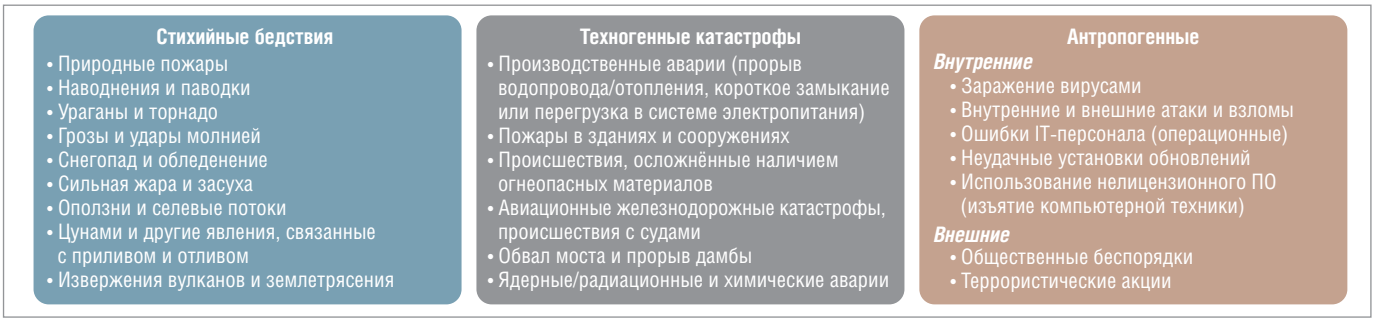

Рис. 4. Внеплановые простои

сети для выполнения технического обслуживания или резервного копирования, включая ежедневные/еженедельные сохранения, пакетную работу, реорганизацию баз данных, обновления приложений и систем, обслуживание системы, настройку производительности и другие виды операций.

Большинство простоев, с которыми сталкивается обычный пользователь, являются плановыми простоями. В то время как внеплановые события, как правило, привлекают к себе наибольшее внимание, на самом деле плановый простой представляет собой бóльшую проблему для конкурентоспособности бизнеса. Регулярные ежедневные/еженедельные операции по резервному копированию и обслуживанию баз данных, приложений или систем могут повлечь за собой прерывание услуг.

Плановые простои

Плановый простой представляет для IT-подразделения более сложную задачу, так как происходит довольно часто. Причём, если внеплановые события, как правило, привлекают к себе наибольшее внимание, на самом деле плановый простой представляет собой бóльшую проблему для конкурентоспособности бизнеса. Регулярные ежедневные/еженедельные операции по техобслуживанию баз данных, приложений или систем влекут за собой прерывание услуг. Исследования показывают, что обновления системы, настройка производительности и работа в пакетном режиме создают более 70–90 процентов простоев.

Резервное копирование

Одной из проблем для современных IT-систем, связанных с большими объёмами информации, многочисленными приложениями и географически распределённой организационной структурой, является выполнение резервного копирования приложений, баз данных и серверов на регулярной основе. Тема резервного копирования весьма обширна и требует отдельного повествования. Здесь только будут упомянуты основные понятия резервного копирования.

Прежде всего необходимо обратить внимание на то, что, с одной стороны, наличие RAID-массивов в организации ни в коем случае не отменяет резервное копирование, а с другой, несмотря на то что подавляющее большинство организаций выполняют резервное копирование и архивацию для защиты своих данных, эти копии не могут восстановить данные, которые были потеряны между сохранениями.

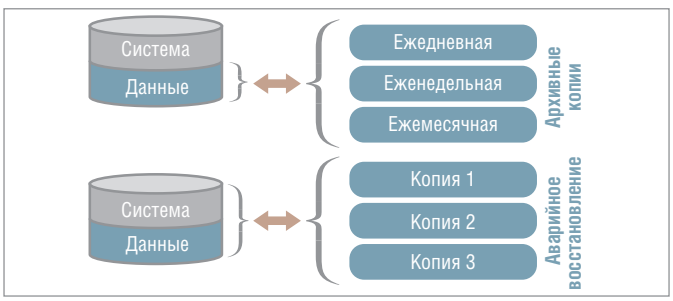

Рис. 5. Основные типы копирования данных

Существуют две основные задачи резервного копирования – создание архивных копий данных и резервных копий для аварийного восстановления (рис. 5).

1. Архивация предполагает ведение архива данных для выполнения требований законодательства и регуляторов, с одной стороны, и, что не менее важно, с другой стороны, для последующего обеспечения доступа к данным за предыдущие периоды с целью восстановления информации, которая была потеряна или искажена в результате операционной деятельности. Примером может служить периодическая – ежедневная, еженедельная и ежемесячная выгрузка базы данных с последующим хранением на кассетах или оптических дисках.
2. Создание резервной копии для восстановления инфраструктуры при сбоях (Disaster Recovery). Основной целью выполнения резервного копирования является возможность восстановления. Резервное копирование, как правило, ориентировано на систему. В случае сбоя сервера весь сервер и его приложения должны быть восстановлены одновременно, независимо от того, имеет ли приложение решающее значение для бизнеса или нет. Если резервное копирование будет сложным и ненадёжным, то это полностью лишает смысла его выполнение.

IT-отделы сталкиваются с проблемой выполнения нескольких типов резервного копирования. Большой пул резервных копий может создать проблемы при извлечении данных из резервных копий. При восстановлении присутствуют некоторые риски. Поэтому необходимо на постоянной основе проверять возможность восстановления.

Обслуживание

Техническое обслуживание оборудования, баз данных и приложений, заключающееся в поддержании исправного состояния и актуальных версий программного продукта, имеет важное значение для обеспечения отлаженной IT-среды. Часто модификация серверов и приложений многократно откладывается на потом, пока не получается выбрать подходящее время для выполнения технического обслуживания. И, как правило, проведение технического обслуживания обычно выпадает на внеурочное время, на выходные или праздничные дни, что, во-первых, ограничивает доступ к службе поддержки поставщика оборудования и программного обеспечения и, во-вторых, влечёт за собой расходы на сверхурочную работу. Способность выполнять модификации в соответствии с требованиями времени является важным условием для получения наилучшей поддержки поставщиков ОС и приложений.

Аналогичным образом очень важно, чтобы компания выполняла плановое профилактическое техобслуживание сервера и приложений для поддержания производительности сервера. Реорганизации баз данных и другие рутинные операции

должны выполняться на регулярной основе. При том, что последние версии ОС помогают снизить необходимость выполнения частого технического обслуживания, его нельзя полностью избежать. К сожалению, для выполнения техобслуживания серверов и приложений требуется остановка некоторых сервисов, что всегда является тяжёлой ситуацией для бизнеса.

Анализ угроз простоя

Перед тем, как начинать рассчитывать стоимость простоя, необходимо определить его источники. И не все из них представляют собой проблемные моменты, связанные с IT. Для начала нужно понять, какие существуют для конкретной организации внутренние и внешние угрозы простоя, стихийные, техногенные и вызванные человеческим фактором (рис. 3). В чём состоит потенциальная возможность угрозы, способной остановить и даже разрушить бизнес? Угрозы для бизнеса могут включать в себя природные явления, а также антропогенные бедствия, – «погода и провода». Необходимо поразмыслить о том, что может на самом деле произойти, и составить соответствующий план действий. Это могут быть случайные или же плановые события, способные вызвать или повлечь за собой простой систем и деловой активности – внеплановый и плановый соответственно. Некоторые события могут быть в зоне контроля и влияния на них, а другие нет. О некоторых событиях, таких как, например, ураганы или регламентное отключение в энергосетях, будет заблаговременно известно; а такие события, как выход из строя источника питания сервера или RAID-контроллера, случаются внезапно, и может не хватить времени, чтобы среагировать. К сожалению, необходимо учитывать экстремальные внешние события, включая терроризм или региональные бедствия, такие как отключение электроснабжения или обрушение основного моста в районе метро. Подобные события могут повлиять на наличие персонала и его безопасность, наличие электроснабжения и доступности линии передачи данных и т.д.

После того как составлен список всех событий и установлены условия, которые могут повлиять на функционирование компании, необходимо определить порядок действий для оперативного контроля и сбора информации о внешних угрозах. Такие действия могут включать в себя простую подписку на получение электронных писем или уведомлений от местных метеорологических станций, чтобы знать о надвигающихся погодных явлениях, а также от властей, муниципальных и других организаций, чтобы знать о ситуации в регионе, в частности, о перекрытиях дорог и отключениях электроэнергии и водоснабжения. Для некоторых типов событий нужно будет точно определить их вероятность, а также потенциальную степень сложности для того, чтобы должным образом составить план действий.

Кроме того, необходимо продумать и спланировать, что произойдёт потом, в ближайшие дни и недели после события. Например, если возникнет необходимость изменить местоположение при возникновении аварии, нужно обязательно спланировать, как создать и поддерживать надлежащий уровень безопасности для пользователей или устройств, присоединённых к новому серверу на время устранения последствий.

Результатом этого должен быть **лист анализа угроз простоев**.

1. Угрозы:
   - природные, техногенные, технологические или политические катастрофы;
   - случайные и преднамеренные;
   - внутренние и внешние;
   - контролируемые и вне контроля организации;
   - события с предварительным уведомлением и внезапные.
2. Вероятность событий:
   - создание методов сбора информации по каждому событию;
   - определение источников информации;
   - оценка и определение фактора доверия к каждому источнику информации;
   - разработка подходящего метода оценки вероятности с приемлемой степенью сложности.
3. Ключевые вопросы/проблемы, связанные с выполнением каких-либо требований безопасности, законов, поставленных задач.
4. Стоимость, связанная с каждым вопросом/проблемой.
5. Процессы для выполнения пересмотра угроз простоев в оперативном порядке.

Анализ последствий для бизнеса

Анализ последствий для бизнеса (Business Impact Analysis, BIA) является хорошей основой для оценки и расчёта стоимости простоя. Основная задача состоит в том, чтобы определить важнейшие бизнес-функции, основанные на целостности данных или приложений, а также степень зависимости каждой функции от времени простоя.

Прежде всего необходимо определить максимальное время простоя, в течение которого каждый вид деятельности, обеспечивающий основные продукты и услуги, может быть прерван без каких-либо негативных последствий для бизнеса, не превышена мера терпения (Maximum Tolerable Period of Disruption; MTPOD). Далее, определение последствий, как долгосрочных, так и краткосрочных простоев, поможет установить целевую точку (Recovery Point Objective, RPO) и целевой срок восстановления (Recovery Time Objective, RTO) для каждого вида деятельности (рис. 6). Затем необходимо определить приоритеты восстановления, ресурсы и возможные решения для уменьшения степени воздействия простоя на основную деятельность (рис. 7).

После того как будут выявлены уязвимые места при простое, легче определить расходы, понесённые вследствие этого простоя, а также общее его воздействие на бизнес. Располагая такой информацией, будет проще установить финансовый ре-

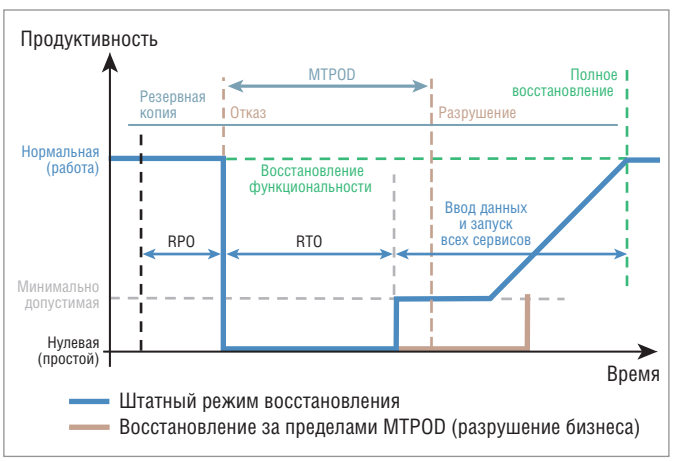

Рис. 6 Расчётное и полное время восстановления

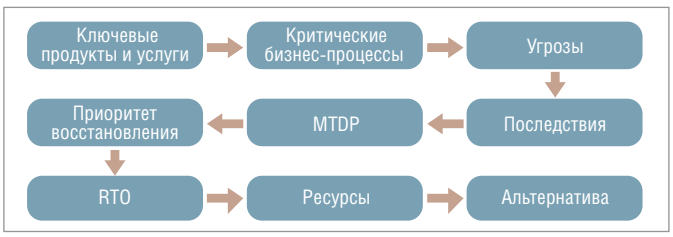

Рис. 7. Основные этапы анализа последствий для бизнеса

зультат различных решений или действий, необходимых для сокращения расходов, понесённых во время простоя бизнес-функции, или, что предпочтительно, избежать их вообще.

Чем основательнее будут исследованы уязвимые места при простое, тем лучше будет понятна ценность управления плановыми простоями и пути устранения внеплановых.

Для лучшего согласования бизнес-стратегий с информационными технологиями необходимо оценить стоимость и последствия, обусловленные простоями в IT-процессах.

Стоимость простоев

Стоимость простоев варьируется по отраслям и масштабам бизнес-операций. Для среднего бизнеса точная почасовая стоимость может быть ниже, но влияние на сам бизнес может быть намного больше. Остановка IT-систем, плановая или внеплановая, может запустить цепочку расходов – последствий, прямых и косвенных, материальных и нематериальных, краткосрочных и долгосрочных, немедленных и далеко идущих.

Прямые расходы легко посчитать, так как они всегда имеют количественное (материальное) выражение.

Для расчёта косвенных расходов необходимо использовать статистические и оценочные методы.

Несмотря на то что точно рассчитать окончательную стоимость простоя очень трудно, можно придерживаться следующих рекомендаций для выполнения максимально точной оценки.

Оценка текущей надёжности системы

Один из способов спрогнозировать количество часов, в течение которых система внезапно будет простаивать каждый год, – это оценить надёжность системы. Оценка заключается в расчёте надёжности системы по показателям MTBF компонентов, полученных от производителей оборудования. Следует отметить, что показатель вероятности зависит от комбинации аппаратных, программных и сетевых компонентов, резервирования (дублирования) компонентов и каналов связи.

В целом необходимо оценить надёжность всех компонентов системы и устранить точки отказов:

- источники питания;
- системные блоки (серверы и клиентские системы);
- операционные системы;
- жёсткие диски сервера;
- система управления базами данных;
- прикладное программное обеспечение;
- устройства коммутации сети и маршрутизации;
- сетевые соединения.

Планирование доступности информации и приложений

Несмотря на то что внезапные отказы и связанные с ними внеплановые простои могут иметь значительные последствия для бизнес-процессов, зачастую до 90% простоев являются плановыми и связаны с резервным копированием системы, техническим обслуживанием, модернизацией и т.д.

Клиентам будет всё равно, насколько надёжна IT-система компании, если они не смогут получить необходимый сервис, когда им нужно, поэтому важным моментом обеспечения бесперебойной работы является определение количества плановых простоев. Обеспечение отказоустойчивости клиентских приложений требует активного контроля за плановыми и внеплановыми простоями в полном объёме.

Оценки ежегодных плановых простоев, как правило, более точны, чем оценки внеплановых простоев, так как работы по техническому обслуживанию, как правило, выполняются в соответствии с установленными графиками и периодичностью в расчёте на год и достаточно предсказуемы.

Первым шагом к получению оценки плановых простоев является выполнение строгого аудита всех обычных операций по техническому обслуживанию, таких как резервное копирование и реорганизация баз данных. Для каждой операции умножьте фактическое среднее значение простоя с поправкой на любые тенденции роста, на количество раз в год, когда выполняются такие операции. Сроки проведения других плановых мероприятий, таких как обновление аппаратного и программного обеспечения, менее упорядочены, но фактическое среднее значение обеспечивает достаточную информацию о периодичности и продолжительности требуемого времени простоя. Эти фактические средние значения могут быть скорректированы для включения сведений о предстоящих обновлениях.

Оценка стоимости простоя

Несмотря на невозможность точно предсказать потери от простоя, важно вывести их оценку, приближенную к реальной. Только тогда можно подсчитать экономически необходимый уровень инвестиций в области программных решений по восстановлению данных или доступности информации.

Потери в области оплаты труда, в получении дохода и оплаты услуг входят в общую стоимость простоя. Хорошей отправной точкой для оценки этих факторов является сбор статистических данных, как по продолжительности, так и по сопутствующим затратам предыдущего простоя в соответствии с данными бухгалтерии. К ним относятся многочисленные материальные и нематериальные факторы (рис. 8).

Потерянный доход

Прогнозирование потенциальных потерь доходов от простоев проще всего выполнить, используя отношение валового годового дохода к количеству рабочих часов в год.

Расчёт выполняется по следующей формуле:

$$R_{loss} = R_{gross} / T_{gross} \cdot I \cdot T \quad (1)$$

Здесь R_{loss} – потерянный доход; R_{gross} – валовой доход в год; T_{gross} – общее годовое рабочее время; I – степень воздействия в процентах; T – время простоя.

Степень воздействия в процентах определяет способность организации восстанавливать коммерческие потери при простое и потери клиентов, которые перешли к конкурентам.

Потеря производительности труда

Повышение производительности труда каждого работника всегда было и остаётся приоритетом для большинства компаний, так как является одним из ключевых моментов обеспечения конкурентоспособности. Значительный прорыв в этой области всегда достигается за счёт совершенствования бизнес-процессов, что, в свою очередь, невозможно без глубокой интеграции в них информационных технологий и делает их заложниками ИТ-системы, а точнее, её работоспособности.

Сотрудники организации в целом всегда продолжают получать полную оплату, когда находятся на рабочем месте, в то время как неработающая ИТ-система или её компонент не позволяет им выполнять функциональные обязанности и наносит урон их производительности. Это самый простой компонент расчёта, так как все данные для него легко получить из бухгалтерии и отдела кадров организации.

Для прогнозирования потерянного рабочего времени можно использовать как статистический анализ при наличии исторических данных о простоях, так и синтетический анализ,

Рис. 8. Структура стоимости простоя

основанный на данных о штатном расписании, организационной структуре и должностных обязанностях сотрудников.

Некоторые сотрудники могут продолжать выполнять определённые производственные работы во время простоя системы, в то время как другие будут простаивать. Следует разделить сотрудников на группы и оценить снижение производительности каждой группы работников в процентах от их производительности в нормальном режиме функционирования организации.

Далее надо оценить стоимость часа потери производительности. Подходящей единицей измерения является общая средняя заработная плата, надбавка к окладу и накладные расходы для вынужденно простаивающей группы работников. Отдел кадров обычно может предоставить эти данные. Так как компании стараются заработать прибыль, то экономическая отдача, вносимая работниками, как правило, больше, чем оплата их труда. Поэтому при использовании показателей заработной платы, надбавок и накладных расходов для оценки снижения производительности получаем анализ затрат/прибыли с запасом.

Следующее уравнение можно использовать для расчёта средней стоимости рабочей силы при простое. Так как затраты на рабочую силу и последствия простоев различаются, для достижения высокой степени точности это уравнение следует применять непосредственно для каждого отдела и группы работников.

$$C_E = P \cdot E \cdot W \cdot T \quad (2)$$

Здесь C_E – стоимость потерь производительности; P – число вынужденно простаивающих работников; E – средний процент простаивающих работников; W – средняя стоимость труда работника в час; T – количество часов простоя.

При определении времени простоя следует иметь в виду, что восстановление полноценной работоспособности сотрудника происходит не сразу же после восстановления работоспособности системы, а постепенно, в течение некоторого времени, в силу психофизиологических особенностей человека.

Стоимость восстановления

Стоимость восстановления определяется временем, которое необходимо затратить сотрудникам IT-отдела для восстановления системы, и напрямую зависит от числа занятых в этом процессе специалистов и их квалификации.

$$C_{rec} = W \cdot E_{rec} \cdot T_{rec} \quad (3)$$

Здесь C_{rec} – стоимость восстановления; W – средняя стоимость труда работника в час; E_{rec} – количество сотрудников, занятых в ИТ-операциях; T_{rec} – время, необходимое сотруднику для того, чтобы восстановить отказавшие системы и вернуться к исполнению своих обычных обязанностей.

Сверхурочная работа

Расходы на обслуживание простоев редко равны нулю. Вследствие простоев компании сталкиваются с каскадом связанных с ними издержек. Такие расходы, как оплата сверхурочных работ, в том числе в выходные и праздничные дни, связанных с восстановлением объёма производства, выполнением договорных обязательств, устранением брака и другими последствиями простоя, понесённые во время или после предыдущего простоя, может помочь выявить бухгалтерия. Общая сумма этих расходов должна быть разделена на общее количество часов, когда система не функционировала, чтобы определить стоимость в час.

$$C_{ot} = W \cdot E_{ot} \cdot T_{ot} \quad (4)$$

Здесь C_{ot} – стоимость сверхурочных работ; W – средняя стоимость труда работника в час; E_{ot} – количество сотрудников, занятых на сверхурочных работах; T_{ot} – время, затраченное на сверхурочные работы.

Потребительская лояльность

Потеря дохода R_{loss}, определённая в формуле (1), не включает в себя ценность клиентской лояльности. Для более точной оценки общих потерь в сумме продаж следует учесть потерю клиентов, которые перешли к конкурентам. Если большой процент клиентов, как правило, становится лояльным после совершения благополучной покупки, то фактор воздействия простоя может быть весьма значителен. Поскольку для определения пожизненной ценности клиентов требуется предоставление долгой истории данных и предполагается, зачастую неправильно, что будущие продажи будут повторять прошлые, то обоснованного предположения будет достаточно.

$$P_{loss} = R_{loss} \cdot R \quad (5)$$

Здесь P_{loss} – прогнозируемая потеря дохода из-за утраты потребительской лояльности; R – средняя частота повторения продажи.

Показатель определяется на основе статистических данных и будет тем точнее, чем больший объём данных имеется в распоряжении.

Потеря репутации

Негативное освещение в СМИ проблем компании, связанных с частыми и (или) длительными простоями системы (или просто слухи) и очернение имиджа организации в сознании потребителей может привести к потере дохода из-за утраты потребительской лояльности:

$$P_{rev} = R_{loss} \cdot R' \quad (6)$$

Здесь P_{rev} – прогнозируемая потеря дохода из-за утраты потребительской лояльности; R' – процент от продаж потенциальным заказчикам, не обратившимся в организацию из-за её негативной репутации.

Финансовые показатели и прочие затраты

Эта категория охватывает некоторые из нематериальных затрат при простое и прочие расходы, которые не попадают ни

в одну из перечисленных категорий. Вопросы, которые необходимо учитывать, включают:

- штрафы за невыполнение договорных обязательств и срыв поставок;
- штрафы за загрязнение окружающей среды;
- штрафы за несвоевременную сдачу отчётности;
- негативное влияние на котировки акций компании;
- необходимость планирования и проведения мероприятий для разъяснения и принесения извинений за отсутствие сервиса.

Определение истинного воздействия простоя требует тщательного рассмотрения каждой операционной зоны бизнеса. Можно также добавить моральный фактор: не только клиенты компании, но и сами сотрудники всегда испытывают негативные ощущения, если система неисправна и нарушаются бизнес-процессы.

Поскольку внеплановый простой может произойти в любое время, единственный способ рассчитать его почасовую стоимость – это использовать среднее значение всех почасовых затрат в целом по неделе. Но поскольку некоторые проблемы являются результатом перегрузки системы, которая происходит в самые экономически эффективные часы, более консервативным подходом будет использовать среднее значение именно для этого периода времени.

В отличие от внеплановых простоев плановые могут быть намечены на наиболее экономически неэффективное время. Однако при проведении технического обслуживания ночью или в выходные дни последует оплата сверхурочной работы и/или надбавки за работу во вторую или третью смену, поэтому такие расходы должны учитываться в расчётах.

Предоставление информации и заключений руководству компании

Суммирование всех перечисленных затрат обеспечивает разумный прогноз ожидаемых потерь[1] от часа простоя для конкретной системы. Для расчёта ожидаемой общей годовой стоимости нужно умножить эту цифру на количество ожидаемых часов простоя за год. При рассмотрении всех факторов потенциальные потери от простоев вызывают шок у большинства людей, которые впервые рассчитали их общую стоимость.

Конечной целью работы по определению источников простоя и расчёту их стоимости является понимание ситуации, а затем предоставление полученной информации на рассмотрение лицам, ответственным за принятие решений.

Необходимо представлять организационную структуру компании и хорошо понимать, какие лица отвечают за принятие решений. У каждого менеджера, вице-президента и генерального директора есть перед кем отчитываться.

Фактически устранение простоев является одной из основных возможностей для достижения реальных, ощутимых результатов, с точки зрения финансовой стоимости и рыночных преимуществ.

Прежде всего, нужно стремиться к устранению плановых простоев, источники и причины которых окончательно задокументированы. Необходимо предоставить все расчёты и обоснования, описанные ранее: затраты на рабочую силу, эксплуатационные расходы, стоимость невосстановимых доходов от бизнеса или потери по причине отложенных продаж и т.д.

После того как будет задокументирована прочная основа материальных затрат, описываются нематериальные издержки (репутация на рынке, правовые риски согласно правилам и т.д.), а также позитивные факторы доступности информации, такие как повышение производительности IT, а также усовершенствованное денежное обращение и точность управленческих отчётов. Необходимо отметить, что система резервного копирования может использоваться для получения срочных отчётов для руководства на основе больших объёмов оперативных данных.

Завершающим штрихом является то, что инвестиции в устранение плановых простоев и «предсказуемых» внеплановых простоев обеспечивают не только минимизацию финансовых потерь, но и положительные рыночные преимущества без каких-либо дополнительных затрат.

Учитывая ориентацию компании на работу с конечным потребителем, можно убедительно сформулировать аргументы в пользу обеспечения высокой доступности информации для бизнеса.

Внедрение улучшенной доступности информации является умной инвестицией в бизнес с оправданным финансовым результатом, как в краткосрочной перспективе, для восстановления капитальных вложений, так и в долгосрочной перспективе, так как компания будет продолжать получать прибыль постоянно. ●

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

[1]Расходы будут варьироваться в зависимости от характера приложения, поэтому данный расчёт должен выполняться для каждой системы.

НОВОСТИ НОВОСТИ НОВОСТИ

Газ – в моторы! FASTWEL – на заправки!

Введена в строй крупнейшая АГНКС в России и Европе. АСУ ТП станции выполнена на базе российских модульных контроллеров и распределённой периферии FASTWEL I/O.

В ноябре 2017 года в Москве состоялся торжественный ввод в эксплуатацию самой большой в России и в Европе автомобильной газонаполнительной компрессорной станции «Газпрома». Её проектная мощность почти 30 млн м^3 природного газа в год. Современное надёжное оборудование станции, состоящее преимущественно из отечественных комплектующих, позволяет ежедневно обслуживать около 2000 единиц техники.

Новая АГНКС на ул. Левобережной оборудована четырьмя компрессорными установками производительностью 1200 м^3/ч каждая. На станции расположено 12 заправочных постов и колонка для наполнения передвижных автогазозаправщиков. Газомоторным топливом могут заправиться автобусы, грузовые и легковые машины, а также коммунальная и дорожно-строительная техника.

Вся работа технологического оборудования полностью автоматизирована и не требует вмешательства оператора при штатной работе. Общестанционная АСУ ТП выполнена на базе российских ПЛК FASTWEL I/O и предназначена для:

- автоматизации основных операций технологического процесса;
- обеспечения централизованного оперативно-диспетчерского контроля работы оборудования;
- своевременного обнаружения и ликвидации отклонений параметров работы от заданных технологических режимов и предупреждения аварийных ситуаций;
- осуществления учёта энергетических ресурсов, контроля за их использованием.

В настоящее время на территории Москвы и Московской области действуют две АГНКС «Газпрома» (с учётом станции на ул. Левобережной), ещё четыре новые станции будут запущены в столице к чемпионату мира по футболу 2018 года. ●