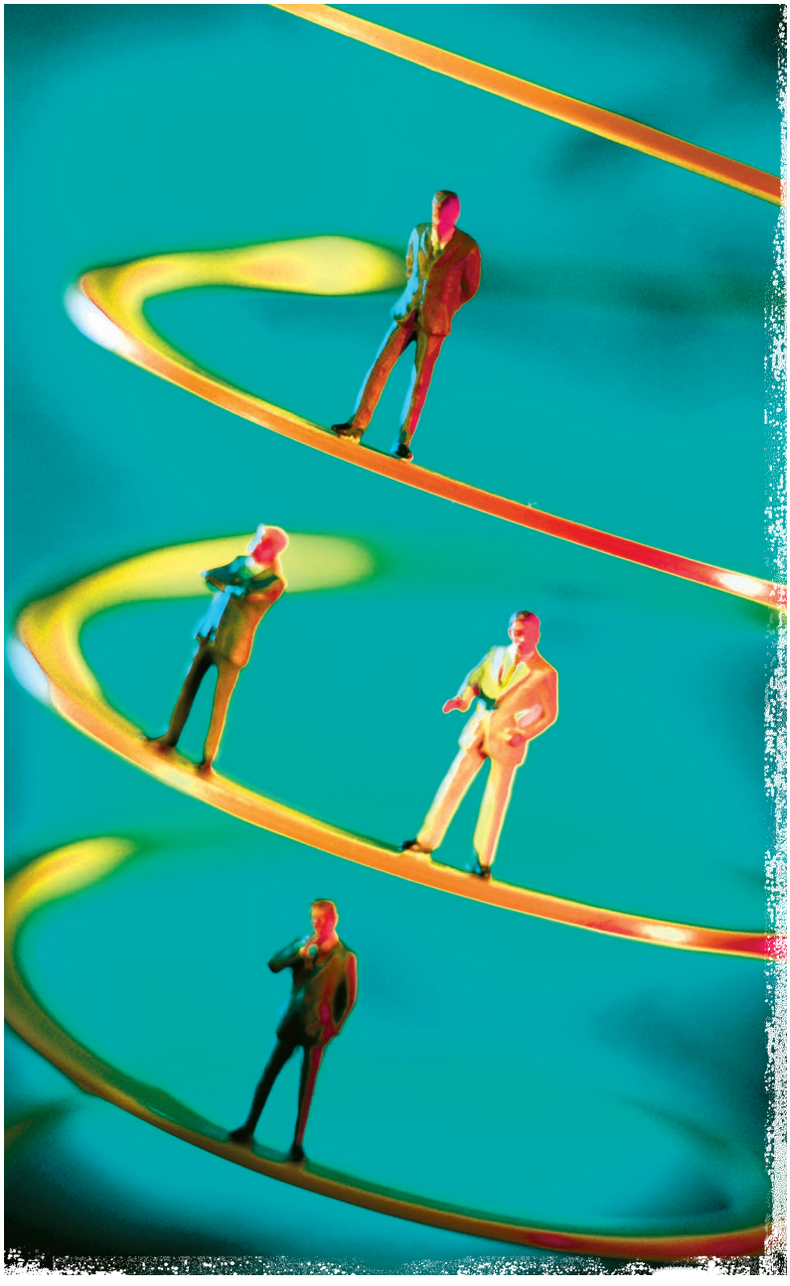
ОБЕСПЕЧЕНИЕ непрерывности бизнеса



Вопросы обеспечения непрерывности бизнеса встают перед руководителем практически каждой компании. Большинство современных руководителей в данном вопросе принимают стратегию страуса, откладывая решение этой проблемы до лучших времен: всегда остается надежда, что законы природы обойдут нас стороной, что бутерброд упадет маслом вверх...

– **ВИКТОР ГАЛАКТИОНОВ**

Однако законы неумолимы, бутерброды падают маслом вниз,

неприятности непременно случаются, а важные данные обязательно пропадают. Поэтому постановка вопроса «Пропадут ли данные?» некорректна. Более правильно ставить вопрос «Когда эта беда произойдет, будем ли мы к ней готовы?» В этой статье автор делает очередную попытку обратить внимание на проблему восстановления бизнеса в случае, если возникнет чрезвычайная ситуация. Современные руководители, ответственные за действия в условиях чрезвычайных ситуаций, способных нанести ущерб бизнесу, должны быть соответствующим образом подготовлены. При этом, с одной стороны, чем больше компания, тем больше убытков она несет в результате наступления чрезвычайной ситуации. В небольшой компании эти убытки, очевидно, меньше. С другой стороны, риск угрозы бизнеса в целом для крупной компании в силу диверсификации бизнеса и наличия территориально рас-

пределенной структуры существенно ниже, чем в малой, специализированной компании. Поэтому затронутые здесь вопросы касаются в равной степени как крупных, так и мелких компаний.

С советских времен многим руководителям знакомы внутренние распоряжения, издаваемые, как правило, перед очередными праздниками, примерно следующего содержания: «1. На период праздников назначаются следующие дежурные: (далее идет перечисление ответственных лиц достаточно высокого ранга и даты их дежурств). 2. В случае наступления чрезвычайных ситуаций действовать по обстоятельствам и принимать все возможные меры по их ликвидации...» Странность в том, что такая особая забота проявляется исключительно по праздникам. Разве в обычные дни не нужно выключать чайники из сети? Может быть, стихийные бедствия и землетрясения происходят исключительно по праздникам? Или, может быть, в будни мы всегда знаем, что нужно делать, и поэтому это особой тревоги не вызывает? А что такое «чрезвычайные ситуации» — обесточивание здания, прорыв канализации, землетрясение? Что значит «принимать неотложные меры по их ликвидации»? Как может вице-президент пусть даже очень крупной компании ликвидировать землетрясение? Как определить степень неотложности принимаемых мер, их адекватность уровню критичности возникшей ситуации?

Первый шаг к снижению уязвимости компании от потенциальных катастроф — документированная система управления рисками и реагирования в чрезвычайных обстоятельствах. План обеспечения непрерывности описывает мероприятия, необходимые для непрерывного обслуживания клиентов в таких случаях. Иными словами, это последовательность действий, которую должна выполнить организация, чтобы подготовиться к/отреагировать на/справиться с/ликвидировать последствия разрушительных событий и вернуться к штатному режиму ведения бизнеса.

Главная цель плана обеспечения непрерывности — поддержка работы ключевых подразделений компании. Поэтому часто его называют «планом продолжения бизнеса». Если на план смотрят с точки зрения событий, несущих существенную угрозу и приводящих к остановке части или всего бизнеса компании, то употребляют термин «план восстановления бизнеса». Аварийные планы, сфокусированные на преодолении повреждений или разрушений оборудования в результате наводнений, пожаров и других стихийных бедствий, известны как «аварийно-восстановительные планы». Встречаются и другие названия: аварийный план (crash plan), чрезвычайный план (disaster plan), план продолжения (contingency plan), план восстановления (recovery plan). Как правило, чтобы подчеркнуть важность решаемых планом задач, в его названии фигурирует слово «бизнес». Термин же «план обеспечения непрерывности бизнеса» является наиболее общим и более всего соответствует конечным целям — целям непрерывности и сохранения бизнеса при наступлении чрезвычайных ситуаций, а также восстановления бизнеса после выхода из чрезвычайной ситуации.

Пожалуй, наиболее типичной ошибкой даже крупных компаний является сужение задач непрерывности бизнеса до задач обеспечения непрерывности работы программно-технических средств. Эта ошибка сопровождается, с одной стороны, неоправданно высокими ожиданиями и требованиями к безотказности информационных технологий компании, что влечет значительное увеличение расходов на них, а с другой стороны, значительным риском потери клиентов и бизнеса в чрезвычайных ситуациях при сохранении непрерывности информационного обеспечения. Вопросы непрерывности информационного обслуживания должны входить составной частью в план обеспечения непрерывности бизнеса компании в целом, но не подменять его. Такие планы необходимы для всех бизнес-функций, всех подразделений и работников, которые зависят от информационного обслуживания бизнеса. Наиболее типичной ошибкой является сужение понятия непрерывности ведения бизнеса до непрерывности информационного обслуживания, которое в свою очередь зачастую рассматривается как необходимость приобретения дополнительных серверов, резервирования каналов связи, ревизии систем пожаротушения и видеонаблюдения и т.д.

План продолжения бизнеса — подробный перечень возможных сценариев развития чрезвычайных ситуаций и действий, которые должны быть выполнены администрацией и персоналом компании при наступлении чрезвычайной ситуации с целью непрерывного обслуживания клиентов и ведения бизнеса, а также последующего восстановления полной работоспособности компании и возврата ее в штатный режим ведения бизнеса

Кто составляет план обеспечения непрерывности бизнеса?

Руководители бизнес-подразделений должны координировать разработку планов обеспечения непрерывности бизнеса для каждой бизнес-функции. В отдельную категорию попадают функции, исполнение которых предусматривает использование информационных служб и ресурсов; эти планы должны быть подготовлены и максимально тщательно протестированы теми, кто впоследствии будет их выполнять.

Проекты таких планов должны быть переданы руководству компании, а также внутренним заказчикам и поставщикам, для того чтобы учесть все точки зрения. В некоторых случаях их следует предоставить внешним заказчикам и поставщикам (при этом, однако, необходимо решить определенные юридические вопросы). Руководство, например, может посчитать, что при нарушении функционирования автоматизированной системы опреде-

День «ИКС»

Рассмотрим один из возможных сценариев внедрения системы расчетов в банке. (Случай этот вымышленный, и многое в нем показано излишне выпукло, для того чтобы выделить те моменты, на которые следует обратить особое внимание.) Поскольку система была предварительно тщательно протестирована, никакого плана обеспечения непрерывности бизнеса не разрабатывалось. Клиентов о возможных технических перерывах в обслуживании не предупреждали, банк осуществлял переход в обычный рабочий день (это и «понятно»: в воскресенье не работают ни внешние системы, ни клиенты). В запланированный день «Икс» система расчетов была запущена в боевую эксплуатацию. Вначале все находилось под контролем, функционируя в полном соответствии с бизнес-требованиями. Однако из-за ошибок, не выявленных на этапе тестирования и опытной эксплуатации, во второй половине дня (за полчаса до закрытия третьего рейса) система расчетов остановилась. Платежные документы, вводимые во фронт-офисе банка, не ушли во внешнюю систему расчетов. Пока технологи и разработчики занимались локализацией проблемы, центр расчетов вводил платежи вручную. Система работала с производительностью, близкой к простою. (Кстати, такая ситуация может возникнуть и по ряду других, более прозаических причин, совершенно не обязательно в день запуска системы). Очереди исходящих платежных документов начали расти. Встал вопрос: откатываться назад или продолжать дальше? Разработчик точно знает, что устранение проблемы может быть проведено только ночью, когда все бизнес-процессы будут остановлены. Службе сопровождения известно: для того, чтобы откатиться назад, нужно один час и сорок три минуты. Руководитель проекта в момент принятия решения об откате должен иметь четкое представление, будут ли обработаны очереди платежных документов до 8 часов вечера при сложившейся производительности или нет. Кроме того, руководитель проекта должен иметь все полномочия, чтобы приостановить работу не только центра расчетов, но и фронтальных бизнес-подразделений на этот срок. Однако

ленные операции не следует делать вручную (даже если это возможно), с тем чтобы персонал мог подключиться к работе других подразделений, продолжение нормальной работы которых более приоритетно. Поставщики и заказчики должны видеть, какие действия планируются в их отношении, а ИТ-подразделения должны понимать и учитывать их планы. Итеративный процесс подготовки плана гарантирует, что планируемые действия будут «лучшим, что можно предпринять» в случае наступления чрезвычайных ситуаций, в частности в случае неполадок в информационной системе.

С чего начать?

В планах продолжения бизнеса нет ничего нового. Большинству исполнителей хорошо известно, что надо делать, если приложение становится недоступным на достаточно короткий период. Иногда эти процедуры хорошо документированы и могут служить отправной точкой для построения плана. Иногда они достаточно очевидны; в таком случае построение плана следует начать с документирования существующих процедур обработки краткосрочных отказов. Затем план следует расширить, включив в него процедуры обработки более продолжительных отказов, а также другие возможные сценарии чрезвычайной ситуации, критерии, приоритеты и процедуры оповещения.

Каждую бизнес-функцию следует рассмотреть с позиции перечисленных ниже аспектов.

- **Упрощенное обслуживание.** Можно ли упростить процессы обслуживания? Позволит ли это поддержать обслуживание на достаточном функциональном уровне?
- **Новые приемы работы.** Поможет ли распределение клиентов между большим количеством обслуживающего персонала существенно снизить объем выполняемой каждым ручной работы и таким образом продолжить обслуживание клиентов?
- **«Зажатие» входного потока.** Можно ли «зажать» (ограничить) входной поток клиентских заявок с целью снижения его интенсивности? Можно ли провести ранжирование заявок по важности и срочности? Можно ли провести ранжирование услуг/операций с целью продолжения реализации услуг, не затронутых чрезвычайной ситуацией? Можно ли отложить обслуживание части заявок? На основании какого критерия? Можно ли провести ранжирование клиентов по степени важности для организации с учетом реальной угрозы потери клиентов? Каких клиентов нужно сохранить ценой потери других?
- **Тренировка.** В какой подготовке нуждается персонал, чтобы выполнить ручные процедуры?
- **Тестирование.** Как протестировать ручные процедуры?
- **Альтернативные поставщики.** Существуют ли альтернативные поставщики услуг, на которых можно оперативно переключиться в случае возникновения проблем у основных поставщиков?
- **Пиковые нагрузки.** Существуют ли пиковые нагрузки в графике обслуживания, которые не позволят выполнять процесс вручную? Не будет ли лучше вообще прекратить обслуживание либо сократить спектр предоставляемых услуг?
- **Бланки.** Существуют ли в достаточном количестве необходимые для ручной работы бланки, формы, конверты и т. п.?
- **Диагностика.** Требуется ли персоналу специальная диагностика приложений при выполнении ручных процедур?
- **Переработки.** Потребуются ли переработка или изменение графика работы для выполнения ручных процедур? Достаточно ли персонала необходимой квалификации для укомплектования всех смен?
- **Дополнительные ресурсы.** В тех случаях когда для выполнения ручных процедур потребуется дополнительный персонал, будут ли нужны дополнительные столы, телефоны и прочее конторское оборудование? Следует ли дополнительное оборудование подготовить заранее?
- **Переводы.** Потребуется ли перевод персонала в другие подразделения для выполнения (вручную) высокоприоритетных процедур обслуживания?
- **Отсутствие персонала.** Каковы действия в случае отсутствия ключевых работников по болезни или иным причинам?

таких полномочий и оповещения нет. В результате, хотя часть внутренних бизнес-процессов приостановлена, «фронты» и дополнительные офисы продолжают в штатном режиме принимать платежные документы, совершать сделки, заключать договоры по «межбанку». При этом банк уже не может дать гарантий, что принятый платеж сегодня же будет исполнен. В теории управления при выходе из строя одного из звеньев системы остальные должны или перестроиться, чтобы локализовать и устранить сбойный элемент, продолжив затем функционирование в штатном режиме, или принудительно понизить интенсивность входного потока хотя бы с частичным отказом в обслуживании отдельным категориям входящих заявок, чтобы не остановить работоспособность всей системы в целом. В нашем примере банку лучше отказать среднестатистическому клиенту в обслуживании (клиент поворчит и придет завтра), не выполнить мелкие платежи, не разместить средства, недополучить прибыль, чем завтра платить многомиллионные штрафы. Однако эти вопросы уже выходят за рамки компетенции руководителя центра расчетов.

Здесь и возникают общие вопросы: кто, когда, на основании чего примет решение о «зажиме» входящего потока, каким образом и кого известит об этом? Какие операции относятся к низкоприоритетным и должны «зажиматься» в первую очередь? Какие — во вторую очередь? После устранения первопричин и возврата системы в штатный режим работы нужно, чтобы и бизнес начал функционировать. Кто должен будет впоследствии отдать приказы для возврата банка в штатный режим взаимодействия с клиентами и контрагентами? Формально бизнес не подчиняется ИТ, поэтому даже директор информационной службы не уполномочен давать таких указаний. Хотя, безусловно, информационные технологии принимают в этом самое непосредственное участие.

Вывод таков. Наступление чрезвычайной ситуации в одном из подразделений компании должно приводить к адекватной перестройке работы других подразделений для локализации чрезвычайной ситуации и сохранения бизнеса компании в целом. Серьезной ошибкой является сведение задачи обеспечения непрерывности бизнеса исключительно к задаче обеспечения непрерывности ИТ-обслуживания. Это наглядный пример того, что задача сохранения непрерывности бизнеса в большей степени является задачей бизнеса — удержать бизнес при временной недоступности ИТ-служб.

- **Системы клиентов и поставщиков.** Взаимодействуете ли вы с системами клиентов или поставщиков? Можно ли что-то предпринять сейчас, чтобы продолжить обслуживание в случае, когда ваша система будет работать, а у клиента (поставщика) нет? Обсуждали ли вы с клиентами (поставщиками) свои планы продолжения бизнеса? Правильно ли они их понимают? Предоставлены ли вам планы продолжения бизнеса ваших клиентов и поставщиков? Помните, что непрямые, последовательные и каскадные аварии могут привести к ситуациям, которые вы не в силах предусмотреть.
- **Иное оборудование.** Используется ли оборудование, которое невозможно протестировать в полной мере (например, кассовые аппараты, смарт-карты и т. п.)? Будут ли без этих устройств работать приложения? Будет ли оборудование работать без приложений?
- **Настольные приложения.** Такие приложения, как электронная почта, электронные таблицы, локальные базы данных, текстовые процессоры (вместе с документами, индексами, таблицами и т. д.) могут стать недоступными; настольный компьютер может оказаться отключен от сети или возникнут проблемы с сетью. Помните, что большинство рабочих файлов расположено на сетевых устройствах, а большинство принтеров — это сетевые принтеры. Должно ли быть предусмотрено копирование критических файлов на локальные диски? Проблемы с сетью лишат возможности что-либо распечатать даже при исправном компьютере и принтере.
- **Компоненты собственной разработки.** Где используются неформально разработанные программные компоненты? Насколько они критичны для бизнеса? Смогут ли разработчики подобных программ совмещать их исправление с ручным выполнением процедур? Что важнее — скорейшее исправление программы или выполнение аналогичных операций вручную?
- **Восстановление.** После того как приложение вновь стало доступным, какие процедуры необходимо выполнить, чтобы проверить и интегрировать в общую базу вручную введенные данные? Требуется ли тщательная проверка данных, которые не были разрушены в результате локального сбоя? Нужно ли снизить рабочую нагрузку на период восстановления? Есть ли потребность в дополнительном персонале для поддержания уровня рабочей нагрузки на период восстановления? Понадобится ли ограничение доступа к обновляемым (восстанавливаемым) базам данных? Есть ли для этого средства, существует ли необходимость перенастроить контроль доступа?

Сценарии чрезвычайных ситуаций

На непрерывность бизнеса оказывают влияние два типа угроз.

К первому типу относятся постоянные угрозы, которые могут возникнуть в любой момент штатного режима ведения бизнеса. Это угрозы стихийных бедствий, угроза потери административного контроля над зданием (территорией), угроза пожара/затопления, угроза потери связи с другими офисами и филиалами, угроза выхода из строя серверного или сетевого оборудования, угроза сбоя программного обеспечения и т. д.

Главная цель плана обеспечения непрерывности — поддержка работы ключевых подразделений компании

Ко второму типу относятся угрозы, возникающие в определенные промежутки времени. Их правильнее называть рисками. Например, риск неудачи при переходе с одной информационной системы на другую, внедрении новой системы, реинжиниринге определенного бизнес-процесса, преобразовании организационной структуры, риск неготовности персонала к изменениям. Эти угрозы реальны и подлежат анализу, который должен быть осуществлен в рамках соответствующего проекта. Проектные риски и разрабатываемые в рамках проекта превентивные мероприятия носят временный характер и утрачивают актуальность после успешного завершения проекта.

Угрозы второй категории значительно сложнее учитывать и зачастую невозможно решить в рамках одного проекта, в том случае если в компании ведется целая программа из нескольких взаимозависимых проектов. Проекты, связанные с ИТ, зачастую имеют сильный технический уклон. Безусловно, необходимо разрабо-

тать превентивные меры: скажем, продублировать канал информационного взаимодействия, разработать процедуры копирования критической информации на внешние носители и передачи этого носителя в смежное подразделение через курьера, а также предусмотреть процесс перехода с выделенных каналов связи на коммутируемые с многократной потерей скорости передачи данных. Но зачастую в ходе отдельного ИТ-проекта не удается найти ответы на более общие вопросы:

- Насколько уменьшится производительность (пропускная способность) бизнес-подразделения в связи с «выходом из строя» основного программного комплекса и переходом на резервные механизмы?
- Останется ли после перехода на резервные механизмы уровень производительности бизнес-подразделения достаточным для того, чтобы продолжать бизнес в штатном режиме или упадет ниже критической отметки и возникнет необходимость ввода в действие соответствующего аварийного плана?
- Насколько сильно повлияет падение производительности отдельно взятого конкретного подразделения на бизнес других подразделений? Продолжать ли им работу в штатном режиме или же действовать согласно аварийному плану?

Руководители бизнес-подразделений должны координировать разработку планов обеспечения непрерывности бизнеса для каждой бизнес-функции

- Кто, на основании каких критериев и каким образом принимает решение о вводе в действие аварийного плана, какие из смежных бизнес-подразделений необходимо оповестить о его вводе в отдельном подразделении, как происходит это оповещение и какие изменения нужно внести в работу смежных бизнес-подразделений, чтобы отреагировать адекватно сложившейся ситуации?

Содержание планов обеспечения непрерывности

Прежде всего, планы обеспечения непрерывности должны идентифицировать подразделения и кратко описывать бизнес-функции с указанием соответствующей клиентуры, циклов и ключевых событий. В планах должна содержаться информация, позволяющая установить приоритеты обслуживания сведений, а также уточняющие их область применения.

План должен содержать критерий (обычно связанный с серьезностью аварии), являющийся основанием для принятия решения о вводе в действие отдельных частей плана, указания на то, кто именно будет принимать решение, а также меры и средства оповещения клиентов.

Планы включают в себя описания выполняемых вручную процедур, позволяющих предоставить клиентам некоторое количество услуг. Возможны варианты: полное прекращение обслуживания, предоставление части услуг, отложенная обработка, предоставление предварительных данных с последующим подтверждением либо предоставление тем или иным образом полного спектра услуг. В случаях, когда одновременное выполнение нескольких приложений невозможно или персонал временно откомандировывается в другие подразделения, должны быть указаны приоритеты функций обслуживания. Необходимо также указать ожидаемую продолжительность задержек обслуживания (особенно при множественных или каскадных авариях). Наконец, план должен регламентировать процедуры восстановления режима полного обслуживания.

В нем должны содержаться детализированные процедуры реализации основных функций предприятия в случае сбоев и последующего возвращения в штатный режим.

Отдельные разделы плана обеспечения непрерывности бизнеса разрабатываются пользователями, специалистами по коммуникациям, персоналом вычислительного центра, другими сотрудниками ИТ-подразделений. Вместе с тем все планы в части обеспечения информационного обслуживания должны содержать процедурный и проблемно-ориентированный разделы.

Процедурный раздел, детализирующий планы по управлению подготовкой системы, тесно связан с так называемым приоритетным управлением. Он готовится проектировщиками системы, операторами и персоналом поддержки при консультационном участии пользователей и содержит процедуры, выполняемые ими в случае возникновения ожидаемых проблем. Примером такого рода проблем может служить ситуация, когда в коде подсистемы обнаружены серьезные ошибки, которые в силу имеющихся временных ограничений и установленных приоритетов не могут быть устранены в полном объеме.

Проблемно-ориентированный раздел имеет дело с управлением операционными рисками. Он готовится пользователями системы при консультационном участии проектировщиков системы, операторов и персонала поддержки. Раздел содержит процедуры, которые должны быть выполнены пользователями системы непосредственно до, во время и сразу после отработки определенной проблемы. Это могут быть сбои питания, аварии системы, несовместимые данные, потеря коммуникаций и т. п.

Оба раздела должны быть тщательно скоординированы. Планы необходимо довести до всех пользователей системы, а также до администраторов других систем, с ней взаимодействующих.

Заключение

В журнальной статье невозможно исчерпывающе рассмотреть все вопросы обеспечения непрерывности бизнеса. Тем более невозможно дать универсальный ответ: разработка плана обеспечения непрерывности бизнеса носит исключительно индивидуальный характер. Его нельзя «списать у соседа».

Каждой компании необходимо планомерно и методично заниматься этой проблемой. Но и после разработки его нельзя поставить на полку. Поддержание актуальности плана, соответствующей текущему состоянию бизнеса компании, и тестирование плана является не менее важной работой, чем разработка штатных процедур и правил, которая требует определенных ресурсов. Но это уже тема отдельной статьи. CIO.ru

Виктор Галактионов — вице-президент, главный системный архитектор ОАО «Альфа-банк», *vgalax@mail.ru*