Диагноз для ИТ

Автор: **Жилкина Наталья**
Опубликовано 24 июня 2009 года

Говорят, все пользователи ИТ делятся на тех, кто уже потерпел аварию винчестера, и тех, которому это событие только предстоит. Перефразируя это утверждение, можно условно поделить всех ИТ-директоров на две категории — тех, кто пережил отказ сервисов, и тех, кто застраховал себя от этих неприятностей. Пополнение инструментария для страховки начинается с системы мониторинга.

Основной критерий, по которому оценивают работу ИТ подразделения, — это непрерывность и доступность работы критичных бизнес -систем. Увы, безотказных систем не бывает: оборудование может выйти из строя, производительность работы сети и приложений оказывается ниже ожидаемой. Причин неполадок множество: неправильная конфигурация сетевых и программных средств, внесение в ИТ-инфраструктуру изменений, приводящих к непредсказуемым последствиям, комбинация действий различных пользователей, дисбаланс нагрузки в отдельных сетевых сегментах и многое другое… Понять, что происходит в системе, иногда непросто, особенно если это филиал, удаленный от центрального офиса на большое расстояние.
Скорость работы сети, уровень загруженности каналов, коэффициент использования портов, время отклика программных приложений — все это требует непрерывного наблюдения и контроля. На рынке имеется большое разнообразие инструментов для исследования «здоровья» ИТ-инфраструктуры — от разрозненных утилит для мониторинга оборудования, каналов, приложений до комплексных платформ, позволяющих из единой консоли в режиме реального времени отслеживать состояние ИТ-инфраструктуры, в том числе в удаленном режиме.

Функции надзора

Повышение отказоустойчивости критичных бизнес-приложений — это первоочередная задача ИТ-директора, которая решается с помощью системы проактивного мониторинга. «Если система вышла из строя и клиенты не могут получить требуемый сервис — за это накажут гораздо серьезнее, чем за плохое масштабирование и неоптимальное использование ресурсов», — подчеркивает Константин Троицкий, руководитель технического отдела компании «Поликом Про».
Один из основополагающих принципов обеспечения надежности ИТ-инфраструктуры — это проактивное отслеживание и вероятностное прогнозирование тенденции событий, происходящих в ИТ-инфраструктуре. А не реакция на случившееся — когда работа приложения останавливается из-за нехватки ресурсов, и в результате нарушается производственный ритм всего предприятия.

«Проактивный мониторинг позволяет осуществлять плановое развитие сети и предотвращать возникновение нештатных ситуаций в будущем», — говорит Олег Михайлов, системный архитектор департамента корпоративных решений. — У ИТ-персонала появляется возможность определить, где именно необходимо увеличить производительность системы с учетом прогнозируемого спроса и где инфраструктурные инвестиции дадут наибольший эффект».
Еще один важный принцип касается самого объекта мониторинга. «В последнее время фокус этого процесса заметно сместился: ИТ-инфраструктура предоставляет пользователю уже не ИТ-, а бизнес-сервисы — резюмирует Артур Гиоев, начальник отдела подготовки технических решений HP Software. — Поэтому современные средства мониторинга должны в большей степени отслеживать качество бизнес-сервисов с точки зрения конечного пользователя».
Уже более 10 лет инструменты мониторинга HP используют сервисный подход: от мониторинга отдельных компонентов инфраструктуры (сетевые устройства, серверные платформы или приложения) — к мониторингу ИТ-услуг. Сервисно-ресурсная модель используется в основе ключевой системы мониторинга HP Operation Manager Software. (Еще один продукт мониторинга — HP SiteScope — реализован на основе безагентской технологии.)
К основным задачам мониторинга, связанным с выявлением потенциальной угрозы неработоспособности оборудования, каналов связи и сервисов, Олег Михайлов, системный архитектор департамента корпоративных решений Alcatel-Lucent, относит постоянное отслеживание уровня качества предоставляемых услуг.
Для надежного мониторинга аппаратного обеспечения, приложений и сервисов требуется введение метрик, за которыми должен следить администратор. «Для различных систем и приложений можно подготовить наборы метрик, которые уже оттестированы самими производителями, — говорит Андрей Москвин, технический специалист Symantec в России и СНГ. — Их можно создать самостоятельно, приобрести или обменяться с коллегами на форумах».
Вячеслав Ан, специалист по технологиям департамента SMB компании Microsoft, отмечает, что все Management Pack от Microsoft доступны для свободного скачивания:
— Некоторые партнеры раздают Management Pack под свои решения бесплатно, некоторые — продают. В основном коммерческие Management Pack предназначены для специфических приложений. Например, для типовых антивирусов.
Внедрение активного мониторинга заметно сокращает среднее время простоя и повышает уровень защищенности информационных систем. В частности, это достигается мониторингом событий безопасности. Это инструмент позволяет держать всю отчетность в журнальных файлах, не позволяя администраторам локально на местах пытаться скрыть следы происшествий путем удаления записей. «Это косвенный способ предотвратить возможные нарушения в работе внутренних сотрудников», — отмечает Константин Троицкий.
«Следствием внедрения системы мониторинга на предприятии становится уменьшение штата обслуживающего персонала», — добавляет Андрей Москвин.

Единая консоль

Количество систем мониторинга, которые можно и сегодня встретить на предприятии, бывает довольно велико. Распространена ситуация, когда каждая система — будь то приложение, каналы, сервисы — мониторится своей утилитой. В итоге, как отмечает Олег Михайлов, разрозненные утилиты мониторинга не консолидируют своих отчетов в одном месте, а необходимость переключения между ними создает неудобство и добавляет накладные расходы при администрировании, управлении и настройках.
На рынке обозначилась тенденция к интеграции средств мониторинга с другими системами и к предоставлению пользователю инструмента управления всей ИТ-инфраструктурой из единой консоли. Так, например, единая конфигурационная база данных HP Universal CMDB является хранилищем актуальной информации о состоянии ИТ-инфраструктуры. Системы мониторинга HP тесно интегрируются с uCMDB, что позволяет получать в режиме реального времени данные от системы сетевого мониторинга, системы мониторинга серверов, приложений и отслеживать изменения в ИТ-инфраструктуре. Логичным завершением построения системы мониторинга может стать веб-портал с множеством удобных закладок, представляющих в графической форме информацию о текущем состоянии ИТ-инфраструктуры на основе ролевой модели. В зависимости от потребностей заказчика каждый модуль, включая компоненты мониторинга, может быть установлен отдельно либо совмещен с другими системами.
Стремление собрать все элементы управления на единой платформе демонстрирует и компания Symantec. Все показатели по мониторингу отображаются на единой консоли управления: на других вкладках этой же консоли можно увидеть, например, инвентарные данные сервера, с которого система мониторинга снимает показатели. В случае нарушения работоспособности системы администратор может воспользоваться на консоли вкладкой для запуска системы восстановления с резервной копии Backgr Exec System Recovery или для старта задачи развертывания серверной платформы с помощью Deployment Solution.
Евгений Диденко, начальник отдела систем управления и операционной поддержки компании «АМТ-ГРУП», считает, что не стоит преувеличивать дополнительные накладные расходы на поддержку нескольких систем, поскольку пока не существует унифицированной системы, способной мониторить абсолютно все возможные элементы ИТ-инфраструктуры и полностью заменить системы, предлагаемые производителями оборудования и ПО.
«Единая система мониторинга необходима тогда, когда из ее применения можно извлечь реальную пользу, — говорит Диденко. — При этом она не обязательно должна замещать существующие системы; скорее — объединять их». По его мнению, экономию за счет замещения единой системой всех существующих можно рассматривать как некую дополнительную выгоду, но вряд ли как самоцель. Реальная выгода достигается за счет консолидированной обработки разрозненных данных, возможности реализации сервис-ориентированного подхода и сокращения требуемых интеграционных связей.

Гарантия качества

Олег Михайлов отмечает, что в последние годы произошел сдвиг парадигмы мониторинга в сторону сервисов: «Появилось большое количество операторов услуг, которые предоставляют своим клиентам не просто каналы, а расширенный набор сервисов с заданным SLA, за который пользователи и платят большие деньги. Если компания не выдерживает заданных параметров, это влечет за собой очень большие штрафные санкции».
Константин Троицкий подчеркивает, что обязательно должен быть сформулирован критерий того, что является пределом нормального функционирования системы. Формулировка этого критерия необходима для нахождения общего языка с бизнесом. Например, за норму может быть принят останов системы раз в месяц хотя бы на час для проведения профилактических работ, установки патчей и т. д.
— Часто систему оценивают лишь с точки зрения понесенных убытков, причем только в момент конфликта, - разъясняет Троицкий. — А когда конфликт исчерпан — об этом забывают. Чтобы систему оценивать с точки зрения полезности для бизнеса, по каждому из сервисов должно быть понимание, с каким уровнем доступности вы можете их предоставить. Наличие формальных отношений между ИТ и бизнесом позволяет обосновывать бюджет. Без формулировки критериев это сделать нереально.
Как правило, SLA с ИТ-подразделением в нашей стране подписывается редко. При этом руководитель ИТ-подразделения не может отказаться от ответственности за непрерывность сервисов. В таком случае, говорит Троицкий, нужно предоставить руководству прогноз, основанный на конкретных цифрах: какой уровень доступа бизнес-критичных систем и приложений при текущей инфраструктуре может быть обеспечен? Как часто могут случаться простои? Какой механизм даст возможность оценить надежность вашей инфраструктуры и дать такое предсказание? Как это сделать?
Возможность оперировать не ощущениями, а цифрами дает объективная статистика. А собрать и подготовить эту базу поможет система мониторинга, обеспечивающая диагностику корпоративной ИТ-инфраструктуры.

Рынок предлагает

«В контур систем мониторинга должны быть включены инструменты для мониторинга состояния систем с точки зрения конечного пользователя», — считает Артур Гиоев. Такие решения компания HP объединила общим названием HP End User Monitoring. В нем используется три подхода. В первом случае, когда происходит обращение к системе, фиксируется время ее отклика, эти параметры сохраняются и предоставляются на специальном портале. Второй вариант связан с записью транзакции в системе на уровне сетевых протоколов. Этот способ позволяет из любой точки инфраструктуры выполнить транзакцию пользователя (типовые действия пользователя в системе), причем это можно сделать без установки и использования клиентских мест той или иной системы. Третий метод применяется, когда системы используют веб-технологии, и весь обмен информацией осуществляется на основе HTTP или HTTPs: трафик параллельно выводится для анализа за рамки продуктивной среды в систему мониторинга, что позволяет получить информацию вплоть до времени открытия конкретного окна пользователя, а также в случае ошибки увидеть то, что видит на своем экране пользователь.
В настоящее время технологии HP позволяют применять как мониторинг на основе установки агентов мониторинга, так и без их использования. Подход к мониторингу без агентов реализован в продукте HP SiteScope. «Каждый подход имеет свои плюсы и минусы, — поясняет Артур Гиоев. — При наличии агента все действия выполняются на стороне сервера, на котором установлен агент, и сбор информации осуществляется гарантированно. Безагентская технология не нагружает компьютер, не вмешивается в его работу, но может создавать нагрузку на сетевую инфраструктуру и при отсутствии сетевого подключения не работает».
Комплекс VitalSuite разработан компанией Alcatel-Lucent для управления производительностью сетевой инфраструктуры и приложений. VitalSuite отслеживает эффективность взаимодействия сетевых, прикладных и бизнес-процессов как на уровне сети, так и на уровне отдельных сервисов и сетевых приложений. VitalSuite анализирует состояние устройств, каналов связи, дифференцирует различные типы трафика в сети, позволяет отслеживать SLA, сервисы. Аналитические функции VitalSuite осуществляют сравнение реальной ситуации в сети с интеллектуальными порогами, заданными и приоритизированными администратором, и в том случае, если значения выходят за пределы заданных границ или замечена неблагоприятная тенденция, немедленно идентифицируют и диагностируют сетевые ресурсы, не отвечающие заданным сервисным параметрам.

Помимо поддержки сетевого оборудования, от которого информация собирается по протоколу SNMP, система мониторинга Vital Suite поддерживает некоторые специфические протоколы для обмена данными с call-центрами или телефонными станциями, которые выступают коллекторами событий для Vital Suite. Кроме того, в комплекс VitalSuite встроен программный клиент VitalAgent. Этот агент устанавливается на ПК, ноутбуках и серверах и передает данные от корпоративных серверов и пользовательских ПК непосредственно в систему управления VitalSuite каждый раз, как только обнаружено какое-либо событие производительности — например, отказ электронной почты или существенное ухудшение производительности приложения.
Продукт для мониторинга Altiris Monitor Solution в скором времени, вероятно, будет переименован в Symantec Monitor Solution — это решение входит в пакет для управления серверными платформами Server Management Suite. В свою очередь Server Management Suite — это часть истории Endpoint Management. В настоящее время Symantec выделили у себя направление Endpoint Management, которое включает Client Management, Server Management, Asset Management. Заказчик может выбрать отдельно мониторинг — по разным причинам: у него уже может не быть потребности в иных представленных решениях, может отсутствовать финансирование. Altiris Monitor Solution поддерживает два режима мониторинга: с помощью агентской и безагентской технологии. Версия с участием агента отслеживает работоспособность приложений и ОС, когда требуется собрать информацию в журнальных файлах, следить за показателями. Являясь единым универсальным агентом Altiris, он может еще и инициировать выполнение какой-либо задачи на конечной станции, дабы устранить обнаруженные неисправности. Без участия агента мониторинг осуществляется на основе протокола SNMP, который позволяет вести сбор данных не только с серверных платформ, но и с сетевых устройств.

Спасатели бьют тревогу

Довольно часто администраторы ИТ-инфраструктуры, использующие систему мониторинга, сталкиваются с проблемой большого числа тревожных сообщений. Например, в предыдущих версиях, до выхода Microsoft System Center Operation Manager 2007, на администратора обрушивалось огромное количество различных событий: ошибки, предупреждения серверов из журнальных и конфигурационных файлов, из настроек. Из-за того что не существовало единой консолидированной системы, которая могла бы представить всю инфраструктуру в виде законченной диаграммы сервисов, администратор часто не понимал, с чего надо начинать решать проблему.

— Ключевое изменение в версии System Center Operation Manager 2007 — это внедрение Service Definition Module, позволяющего построить такую модель, — рассказывает Вячеслав Ан. — Построенная диаграмма в итоге даст возможность представлять всю консолидированную инфраструктуру для поддержки этого сервиса. Модель определения сервисов, которая появилась в Microsoft Windows 2007, позволяет перейти от модели конкретных серверов и приложений к модели предоставляемых сервисов. И администратору теперь нет необходимости разбираться со всем огромным количеством событий, которые валятся в журналы.
Как поясняет Олег Михайлов, для более фокусного реагирования на оповещения системы мониторинга любые тревожные сообщения можно ранжировать по уровню критичности. Как правило, все это гибко настраивается под требования заказчика. «То, какое количество сообщений выводить на администраторскую консоль и какой уровень для каждого события задавать, — это вопрос настроек и вопрос бизнеса компании, — говорит Михайлов. — Сервис, критичный для компании, где используется передача голоса по IP, может оказаться не очень важным для тех, кто использует этот протокол для доступа в Интернет».

Взаимодействие с Service Desk

Решение проблемы часто передается в автоматизированную службу Service Desk, поэтому нередко система мониторинга интегрируется с этой службой.
Комплексный пакет управления содержит в себе базу знаний с рекомендацией действий по устранению возникающих ошибок. База знаний — это ресурс, который постоянно пополняется, в том числе службой технической поддержки. По последовательности из некоторых событий (например, при нарушении порогового значения) пользователю, столкнувшемуся с тревожной или аварийной ситуацией, будет представлено решение проблемы. Специалисты службы поддержки могут описать свою методику решения проблемы, и каждый, кто впоследствии столкнется с такой проблемой, уже будет снабжен квалифицированной рекомендацией по исправлению ситуации. «Этих решений в блогах Интернета вы просто не найдете, — утверждает Вячеслав Ан. — К тому же на форуме ответственность за подобные рекомендации никто не несет, в отличие от службы поддержки. В соответствии с ITIL ответственность несет тот человек, кто рекомендует те или иные действия для исправления ситуации».

При интеграции Symantec Server Management Suite со службой автоматизации Service Desk в нее перенаправляются уведомления о нарушениях, запускается процесс Incident Management — регистрация тревожных сигналов (alert) и их обработка. Одним из возможных следствий такого уведомления может стать назначение задания на соответствующую группу сотрудников для разрешения инцидента. Если в течение определенного промежутка времени повторяется один и тот же инцидент от одного сервера — есть все основания для запуска процедуры поиска причины возникновения инцидента (Problem Management). Заказчику предоставляются большие возможности для настройки логики работы системы мониторинга. «В компаниях, где непрерывность предоставления сервисов критична для бизнеса, обычно работают ITSM- и ITIL-консультанты, — поясняет Андрей Москвин. — В случае периодического возникновения одинаковых инцидентов необходимо запускать процедуру Problem Management. Решение проблемы может быть переключено на того, кто отвечает за Problem Management, отслеживает все инциденты и далее регистрирует одну проблему. Либо это может быть автоматическая реакция системы, которая периодически делает выборки по одинаковым инцидентам и заводит проблему самостоятельно. Я бы второй способ не рекомендовал. Анализ с привлечением человеческого интеллекта всегда более эффективен».
Для обработки инцидентов, выявленных на стадии функционирования HP Operation Manager Software, управление также может быть передано в диспетчерскую службу, построенную на основе HP Service Manager. Эта система, помимо автоматизации повседневной деятельности, позволяет создать промышленную базу знаний — в ней накапливается, сортируется, ранжируется по весовым коэффициентам и публикуется в разных срезах для разных пользователей весь опыт по разрешению инцидентов, проблем и проведению изменений.
— Современные системы мониторинга уже давно вышли за пределы просто мониторинга и управления ИТ-системами, — считает Артур Гиоев. — Активно предоставляя ИТ-услуги и бизнес-сервисы, такие системы начинают участвовать не только в регистрации инцидентов, но и в управлении конфигурациями, изменениями и даже знаниями.

Евгений Диденко считает, что интеграция системы мониторинга с Service Desk не только имеет своей целью поддержку процессов, связанных с устранением проблем, но и служит инструментом оценки показателей их эффективности. Если соответствующие процессы до внедрения или модернизации системы мониторинга были измеряемыми, это позволит в том числе и оценить выгоду от внедрения. Наличие Configuration Management System, внедрение которой должно предшествовать внедрению системы мониторинга, обеспечивает процесс необходимыми данными, способствует поиску корневой причины, позволяет оценить влияние сбоя в ИТ-инфраструктуре на бизнес, обеспечивает приоритизацию и принятие обоснованных решений. Непосредственная связь современных систем мониторинга и Configuration Management позволяет первым автоматизировать перечисленные выше задачи.

Мнение эксперта

Евгений Диденко, начальник отдела систем управления и операционной поддержки компании «АМТ-ГРУП»

Мониторинг ИТ-инфраструктуры решает множество задач. Их перечень в каждом внедрении зависит от различных факторов, определяется приоритетами заказчика, степенью зрелости ИТ. А конечной целью мониторинга является обеспечение должного уровня сервиса.
Можно выделить тенденцию к поэтапному подходу, дающему бОльшую гибкость и позволяющему адекватно оценивать результаты. Как правило, в первую очередь решаются задачи мониторинга доступности и работоспособности сети и компонентов ИТ-инфраструктуры. При этом мониторинг, даже не будучи проактивным, позволяет сократить время простоя за счет своевременного обнаружения отказов, а наличие в системах мониторинга средств корреляции и определения корневой причины позволяет уменьшить время локализации неисправности. Показатель среднего времени простоя относится к доступности, то есть к одному из показателей уровня сервиса. Это лишь одна из целей, но достигаемая, как правило, в числе первых и с наименьшими сложностями.
Основным свойством проактивного мониторинга является способность предсказать проблему до ее появления. Неочевидно, кто именно должен предсказывать появление проблемы: система мониторинга или человек, оперирующий предоставляемыми отчетами. Многие системы могут проактивно извещать о возможных проблемах на основании анализа изменений параметров. Существуют и системы, обладающие интеллектом в части мониторинга определенного оборудования или приложений. Многие системы мониторинга являются модульными, с отдельно лицензируемым функционалом, в том числе и в части проактивности.
К задачам планирования и прогнозирования, тесно связанным с мониторингом производительности, как правило, обращаются чуть позже: ИТ-подразделения в первую очередь стремятся обеспечить именно доступность, откладывая задачи оптимизации использования ресурсов и снижения капитальных затрат. В определенной степени такой порядок действий является оправданным, но без накопления и должного анализа данных о поведении ИТ-инфраструктуры во времени мониторинг не сможет стать проактивным.
Нельзя не отметить, что существенно вырос интерес заказчиков к решениям, позволяющим производить глубокий анализ использования сетевой инфраструктуры пользователями и приложениями, выявлять реальные потребности в емкостях, что является следствием экономической ситуации и стремлением адекватно снизить затраты на инфраструктуру.
Обеспечение надлежащего уровня сервиса, представляющееся «конечной сверхзадачей», требует на практике кропотливой работы по идентификации сервисов и их составляющих, формированию SLA и их параметров, определению технических решений по мониторингу, источников актуальной информации о технической реализации сервисов, взаимосвязи их компонентов, механизмов поддержания данной информации в актуальном состоянии, управления изменениями. Сложной не значит недостижимой, и роль интегратора заключается еще и в том, чтобы соотнести желаемое и возможное, выявить риски, сформировать последовательность этапов и критерии оценки их успешности.
При внедрении системы мониторинга, как и других систем, огромное значение имеет надлежащая организация бизнес-процессов эксплуатации и инструментальных средств их поддержки, четкого распределения ответственности, наличия должностных инструкций, регламентов. В противном случае существует риск, что внедрение не принесет желаемого эффекта.

Мнение эксперта

Алексей Николаев, руководитель отдела систем управления компании «Инфосистемы Джет»

Создание и использование систем мониторинга ИТ в России и мире имеет большую историю. Как и 10 лет назад, основное назначение подобных систем — сокращение времени простоев ИТ-систем, поддерживающих бизнес компании.
Достигается это в первую очередь за счет сокращения времени на выявление и диагностику проблемных ситуаций. Не менее важную роль играет возможность проактивного, аналитического мониторинга, позволяющего предсказывать потенциальные проблемы, выявлять отклонения от типичного сценария работы ИТ.
Практика создания систем мониторинга ИТ показывает, что успешность, эффективность подобных систем зависит не только от выбора программных продуктов, но и от ряда других факторов. Вот лишь некоторые из них.
1. Эффективная система мониторинга должна обеспечивать контроль всей ИТ-инфраструктуры, причем не только «изнутри», с точки зрения администратора, но и «извне», с точки зрения конечного пользователя услуги. Необходимо учитывать особенности и структуру взаимодействия различных ИТ-ресурсов в рамках предоставления услуг бизнесу.
2. При создании эффективной системы мониторинга должны учитываться потребности различных групп и персоналий — системных и сетевых администраторов, групп поддержки прикладного ПО, руководителей подразделений и ИТ в целом, представителей бизнеса. Каждый из потенциальных пользователей предъявляет свои требования к полноте, детализации, структуре представления информации мониторинга. Важно учесть возможности системы мониторинга в части обеспечения процессов управления ИТ, таких как управление инцидентами, управление проблемами, управление мощностями, управление уровнем сервиса.
3. Должны быть систематизированы подходы к мониторингу компонентов ИТ, определены «модели здоровья» компонентов и правила их пересмотра. При определении подобных моделей значительную помощь, помимо анализа собственной практики, могут оказать рекомендации вендоров, использование мировых практик, систематизированных, например, Microsoft Operation Framework.

4. Важно определить процессы эксплуатации системы мониторинга, в том числе регламент обслуживания системы, включение системы мониторинга в процессы управления конфигурациями и управления изменениями. Без учета изменений, происходящих в этом мире, система мониторинга перестает быть полезной, становится ненужной, а иногда и вредной — балластом.
5. Необходимо реализовывать механизмы «повышения полезности» информации мониторинга. Современные решения предоставляют большой набор подобных возможностей: выявление корневой причины сбоя, корреляционный анализ трендов и событий, факторный анализ. Использование подобных технологий позволяет существенно повысить эффективность локализации и диагностики проблем.
В части выбора архитектуры системы, конкретных программных решений практика обнаруживает невозможность использовать готовые рецепты. Общая практика показывает эффективность комплексного, интеграционного подхода к созданию систем мониторинга. Особенностью является использование на уровне сбора информации о работоспособности и производительности систем, ориентированных на управление конкретными компонентами ИТ (пример — решение Sun Management Center для управления серверами и системами хранения). Задачи комплексной аналитики информации мониторинга, предоставления ее в различных разрезах, решаются за счет внедрения промышленных средств мониторинга и управления (решения компаний BMC Software, CA, Hewlett-Packard, IBM, Microsoft и др.). Важным этапом такого проекта является интеграция подобных решений с развернутыми средствами управления компонентами ИТ.
Выбор промышленных, готовых решений, в противовес собственной разработке, позволяет существенно сократить сроки и стоимость внедрения, учесть существующий опыт и наработки.
Хотелось бы отметить, что приведены лишь основные практические рекомендации. Требуется также и учет особенностей, опыта, наработок конкретной компании при создании и эксплуатации систем мониторинга ИТ.