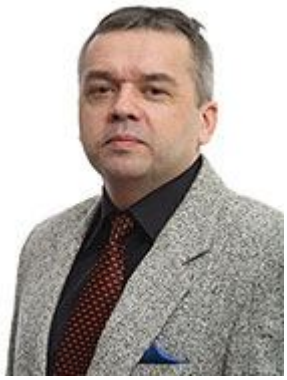
4. УПРАВЛЕНИЕ СОБЫТИЯМИ: НОВЫЙ ВЗГЛЯД ТРЕТЬЕЙ ВЕРСИИ ITIL



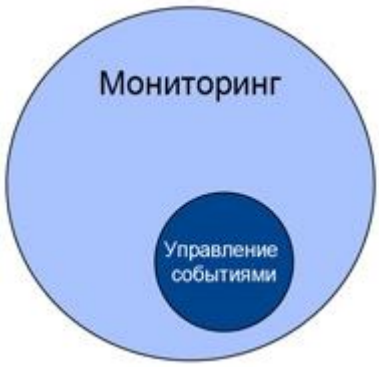
Владимир Аношин,
Ведущий тренер-консультант
IT Expert

В третьей версии ITIL появился новый процесс, который раньше отсутствовал на операционном уровне поддержки сервисов – процесс управления событиями, являющийся, согласно описанию процесса, частью общей системы мониторинга инфраструктуры. Почему авторы третьей версии посчитали необходимым выделить новый процесс? Как он связан с мониторингом? Почему нельзя просто поставить систему мониторинга?

Для начала разберемся с основными понятиями, обратившись к ITIL третьей версии.

Разница между мониторингом и управлением событиями:
Эти две области очень близки, но всё же на практике несколько различны.
Управление событиями наблюдает за событиями, связанными с изменениями в ИТ инфраструктуре и(или) оказываемых ИТ сервисах.
Мониторинг – наблюдение за состоянием, данное понятие является более широким, чем управление событиями. Например, средства контроля проверяют состояние устройства на предмет его функционирования в допустимых пределах, даже если это устройство не генерирует никаких событий.

Для большей наглядности приведем схему, характеризующую взаимоотношения между этими двумя понятиями.



Тут очень важно правильно трактовать понятие **событие,** определения которого к сожалению не было во второй версии ITIL, но, к счастью, третья версия ITIL дает нам четкое определение:

Событие – поддающееся обнаружению явление, имеющее значение для управления инфраструктурой ИТ или предоставления ИТ сервисов.
Как правило, события представлены в форме оповещений, генерируемых ИТ сервисами, конфигурационными единицами (CI) или средствами мониторинга

В связи с широким и повсеместным применением средств автоматизации в практике компаний является логичным связать средства мониторинга ИТ инфраструктуры с автоматической регистрацией инцидентов, проведением изменений, регламентных работ, оповещения персонала первой и последующих линий поддержки сервисов о других событиях, значимых для бесперебойной поддержки ИТ сервисов. По моему мнению, это и явилось одной из причин, почему в третьей версии ITIL среди процессов оперативного управления сервисами был выделен отдельный процесс управления событиями, который достаточно стройно был вписан авторами ITIL в общую схему оперативного управления сервисами.

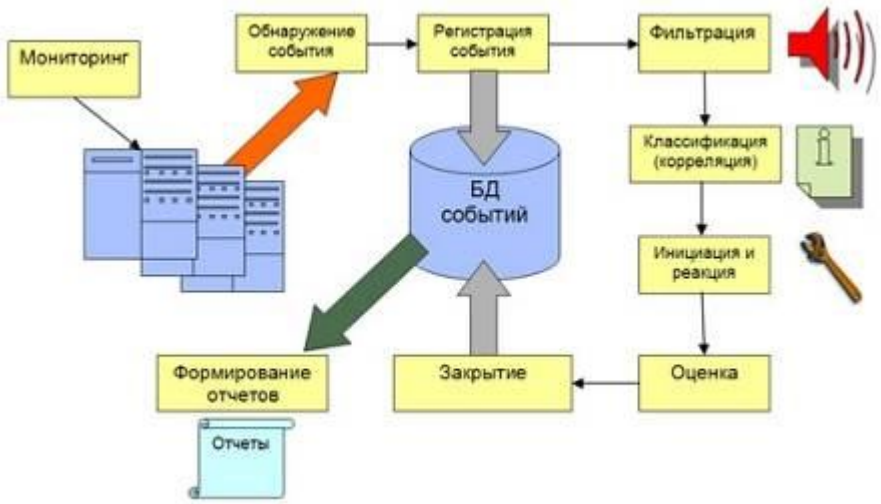
Так какую же ценность для заказчика может представлять управление событиями? В ITIL третьей версии приводятся следующие факторы:

- Раннее обнаружение инцидентов
- Повышение рациональности мониторинга автоматизированных процедур
- Раннее оповещение о необходимости обновления процедур или ресурсов
- Основа для автоматизации процедур эксплуатации

Для ознакомления с процессом управления событиями рассмотрим основные виды деятельности процесса, которые излагаются в ITIL третьей версии. Для этого рассмотрим несложную схему, отражающую жизненный цикл события, значимого для судеб ИТ поддержки:

- Итак у нас работает система мониторинга, в которой, помимо всего прочего, периодически появляются события, значимые для поддержания и(или) улучшения ИТ сервисов. Мониторинг может охватывать состояние конфигурационных единиц (контроль стабильности или изменения статуса), окружающую среду, лицензии

ПО, параметры безопасной работы, мониторинг нагрузки серверов, каналов, баз данных.



- На этапе обнаружения событий важно понимать, какого рода события подлежат мониторингу и обработке. События могут быть как ответом на опрос средствами наблюдения, так и происходить при достижении определенных условий, контролируемых внутренними средствами наблюдения

- Все события можно разделить, например, на следующие типы:
  - **информационные события** (нормальное исполнение операций) – события, не требующие каких-либо действий, например, *завершение плановой процедуры*
  - **отклонения**– события, которые могут быть расценены как триггеры для инициации инцидентов, проблем, изменений, например, *инсталляция неавторизованного ПО*
  - **предупреждения** (необычные события, не являющиеся отклонениями) – события, заставляющие насторожится, некая последовательность (сочетание) которых может привести к отклонениям, например *предпороговая нагрузка на ресурс*

- На этапе фильтрации событий целью является отобрать события, требующие реагирования. Информация об остальных событиях регистрируется и накапливается в базе данных событий без немедленной обработки. Фильтрация является первым шагом к классификации событий. Причем для некоторых КЕ фильтрация не требуется, т.к. все генерируемые оповещения о событиях важны и должны быть обработаны.

- На этапе классификации (correlation) решаются две задачи:
  - Определение категории (значимости) события – информационное событие, предупреждение или отклонение
  - Событие пропускается через заранее настроенный механизм корреляции событий (correlation engine). В нем прописывается способ реагирования на

событие, например: что делаем при первом, втором и последующих проявлениях данного предупреждающего события, при сочетании или последовательности ряда событий-отклонений, одиночном, но имеющем очень серьезные для заказчика последствия, отклонении.

- При инициации реагирования возможны следующие варианты действий (триггеры), например:
  - Генерация записи об инциденте
  - Регистрация запроса на изменение
  - Эскалация (оповещение) заинтересованных лиц
  - Запуск скрипта, управляющего компонентами инфраструктуры

- Реакция на событие может включать в себя:
  - Регистрацию произошедшего события
  - Автоматическое исполнения процедур, например регламентных работ
  - Оповещение и инициация вмешательства живого персонала
  - Запуск процедур других процессов эксплуатации, например процесса управления инцидентами

- Оценка действий по всем событиям невозможна, отбираются самые важные. Оценка дает информацию для процессов непрерывного улучшения, описанных в третьей версии ITIL, а также развития самого процесса управления событиями.

- Этап закрытие возможен не для всех событий. Если к данному событию может быть применен статус “закрыто”, то обычно закрытие этого события происходит после закрытия вызванного им инцидента, проблемы или изменения

Таким образом, мы видим, что третья версия ITIL даем нам четкий и верный взгляд на управление событиями, который достаточно хорошо соответствует современным реалиям и позволяет нам с еще большим успехом внедрять принципы ITSM в повседневную практику управления ИТ.

Подробнее эта тема обсуждается на следующих курсах:

- Основы ITIL v3 (ITIL v3 Foundation)
- ITIL v3 Operational Support and Analysis: поддержка сервисов

Схожие вопросы затрагивались в следующих проектах:

- Построение системы мониторинга и управления инфраструктурой (СМиУ) на Бурейской ГЭС

Данная заметка отражает мнение автора, которое может не совпадать с уважаемыми первоисточниками (ITIL v2, ITIL v3, COBIT, MOF и проч.). Комментарии и предложения темы для следующей заметки можно отправлять на items@itexpert.ru.