Статьи → Управление изменениями в системе управления ИБ

автор: sereg777 | 25 мая 2008 | Просмотров: 2512

Одним из важных процессов в системах управления ИТ-деятельностью является управление изменениями, оказывающих непосредственное влияние на стабильность работы ИТ-системы. Особенно это заметно в условиях увеличения масштаба и функционала ИТ-систем. В статье приведены основные положения о связи процесса управления изменениями с функциями системы управления информационной безопасности.

В первую очередь необходимо понять место процес-са управления изменениями в системе управления информационной безопасностью (СУИБ). Сам процесс управления изменениями связан со многими другими процессами, например, управлением рисками, мониторингом/аудитом, управлением инцидентами, управлением доступом, управлением непрерывностью и т. д. Следует отметить, что управление изменениями является основополагающим процессом в СУИБ, своеобразным «мотором» жизненного цикла системы безопасности.

Если проводить аналогию с системами управления ИТ-услугами, процесс управления изменениями является основой для подсистемы принятия решений и оказывает управляющее воздействие на подсистему управления процессами жизненного цикла СУИБ. Без тщательно выстроенного процесса управления изменениями даже хорошо спроектированная и продуманная СУИБ «сломается» спустя некоторое время после ввода в эксплуатацию.

Требования к управлению изменениями прописаны во многих международных и национальных стандартах, например в ISO 27001, п. А 10.1.2 (в целях и мерах контроля). Более того, в стандарте ГОСТ 13335-1-2006 («Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий») неконтролируемые изменения систем являются по определению инцидентами ИБ, а «любое изменение активов, угроз, уязвимостей или защитных мер может оказать значительное влияние на риск». Любые изменения способны создать новые уязвимости системы, которые должны быть проанализированы и оценены и либо снижены, либо приняты. Если анализировать жизненный цикл систем ИБ, то контроль над управлением изменениями появляется на этапе цикла «эксплуатация и поддержка».

Таким образом, возникает необходимость в методах контроля изменений в политике безопасности (да и в системе ИБ в целом). \\connect.ru