

# Начинаем применять ISO 27001 «в лоб»

- **ISO 27001 требует применение анализа рисков.** Какую методику анализа рисков выбрать? Сложные методики непонятны для руководства организаций и требуют высокой квалификации службы ИБ. Простые методики субъективны, не обеспечивают повторяемости результатов и независимости от конкретного исполнителя, а также воспринимаются как «шаманство», то есть, являются больше искусством, чем наукой.
- **Не начинайте с анализа рисков, начните с «отправной точки».** ISO 27002, ранее известный как ISO 17799, вводит очень удачное понятие «starting point». Отправная точка ИБ – это состояние системы управления ИБ, при котором внедрены самые важные средства управления ИБ, и организация готова к внедрению управления рисками
- **«Отправная точка» во многом созвучна понятию «базовая безопасность».** Однако термин *baseline security* концентрируется на конфигурации инфраструктуры, часто упуская из виду управленческие процессы. Ликвидировать угрозы всегда выгоднее, рассматривая их корневые причины. А такой причиной, вне зависимости от вида угрозы, всегда является пресловутый человеческий фактор.

