



Качество в IT индустрии. CMMI. Стандарт ISO 27000 и информационная безопасность для различных отраслей бизнеса

Горбунов А.В.

**независимый эксперт по менеджменту качества,
«Практический менеджмент качества он-лайн», г. Москва**

**XIV международная научно-практическая конференция
«Качество – стратегия XXI века»**

10 – 11 декабря 2009 года, г. Томск



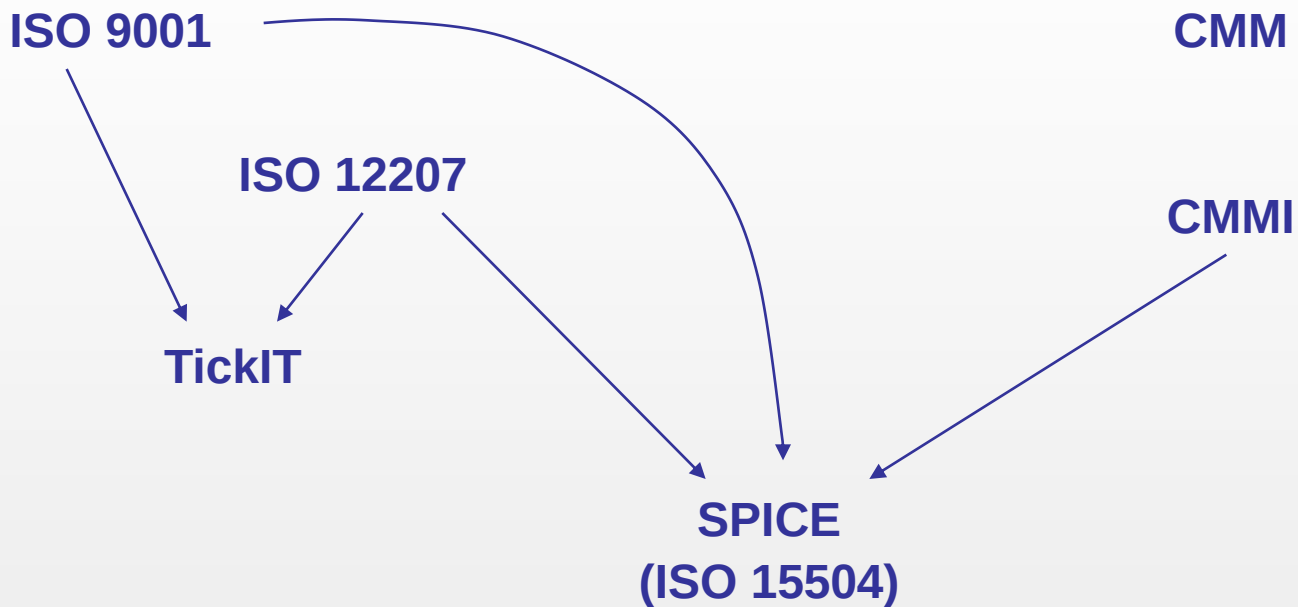
Качество в IT индустрии. Модель СММИ



Качество в ИТ

Европа

США



Цель: обеспечить гарантированное высокое качество программных средств.



Capability Maturity Model Integration (Модель зрелости процессов)

1990-е годы – разработка Software Engineering Institute (SEI) моделей CMM

2000-е годы – объединение в CMMI

Тип модели	Уровни зрелости/возможностей*					
	0	1	2	3	4	5
Product and service development (CMMI for Development model)						
Service establishment, management, and delivery (CMMI for Services model)						
Product and service acquisition (CMMI for Acquisition model)						

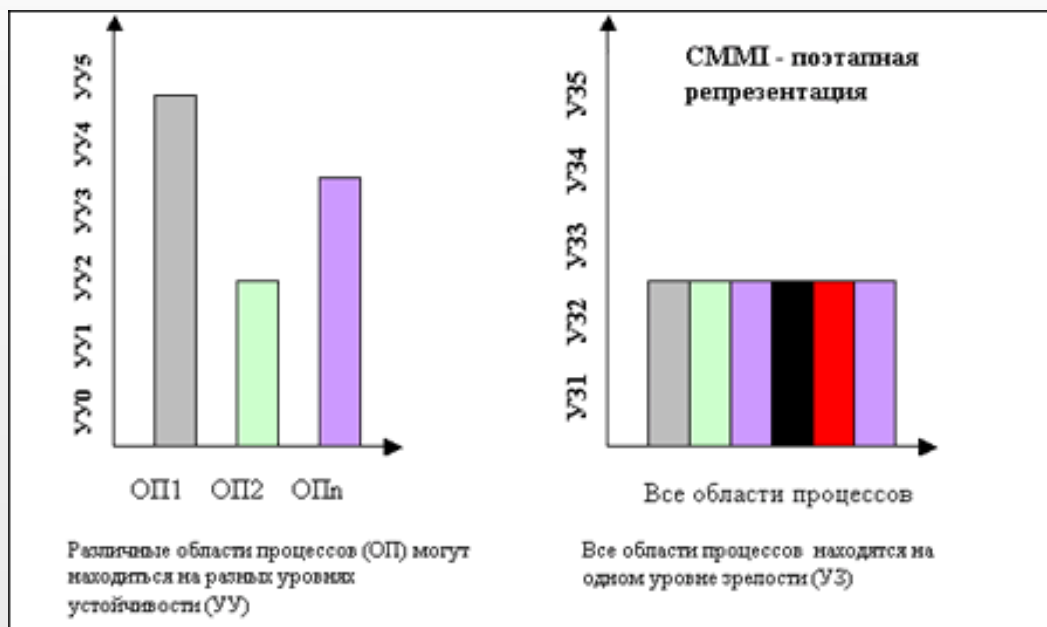
* Для представления Staged – 5 уровней зрелости, для представления Continuous – 6 уровней возможностей процесса.



CMMI

Представление Staged – все процессы должны быть одного уровня.

Представление Continuous – уровень зрелости достигается в рамках выбранной процессной области.

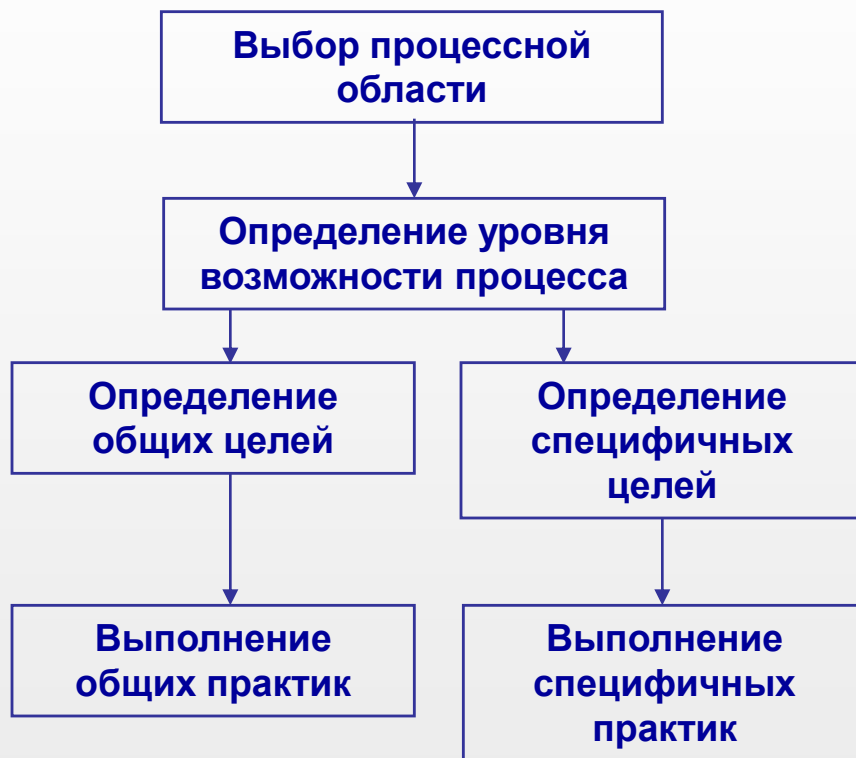




Представление Staged



Представление Continuous





Модель CMMI:

- не является стандартом,
- ориентирована на специфику отрасли,
- предполагает выполнение определенных практик (5 уровень зрелости – 435),
- не предполагает сертификации, но возможна оценка организации на соответствие определенному уровню (с 2007 года введено ограничение действия оценки – 3 года).
Результат оценки не оформляется отдельным документом, подтверждение достигнутого уровня для заинтересованных лиц через ссылку на сайт SEI,
- в России пока только один Lead Appraiser, но без права проводить оценку на 4-5 уровень.

В России только одна организация (Luxoft) имеет 5 уровень CMMI. Около десятка имеют 3-й уровень.

Когда имеет смысл внедрять CMMI? Если у компании есть значимые заказчики из США и они выдвигают условие наличия оценки по CMMI.



Стандарт ISO 27000 и информационная безопасность для различных отраслей бизнеса



Глобальная информатизация





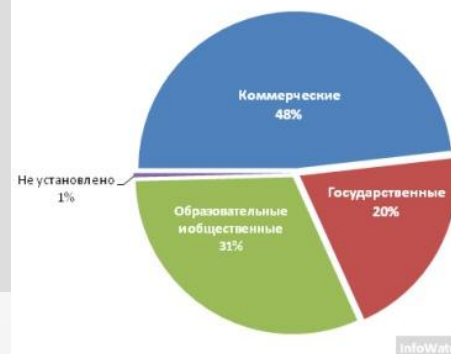
Глобальная информатизация

Проблема: утечка информации

InfoWatch: утечки информации в 2008 году затронули интересы более 100 млн. человек. Почти половина утечек пришлась на коммерческие организации. Организация CERT, опросившая более 800 компаний, установила, что каждая вторая компания хотя бы раз в течение года пострадала от утечки чувствительных сведений

CNews: утечки информации приводят к ухудшению имиджа компании, снижению ее репутации. Анализ годовых финансовых отчетов тех компаний, которые зафиксировали громкие утечки, показывает, что ухудшение имиджа может привести к снижению чистой прибыли на 20-30% в результате недополученного дохода.

Распределение утечек по типу организации (9 мес. 2008)



Последствия утечек информации в России. InfoWatch, 2007 г



Предпосылки

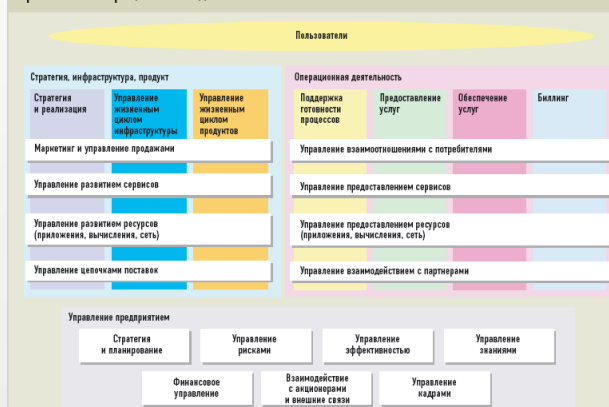
Вывод: информационной безопасностью надо управлять

Цель: обеспечить непрерывность бизнеса

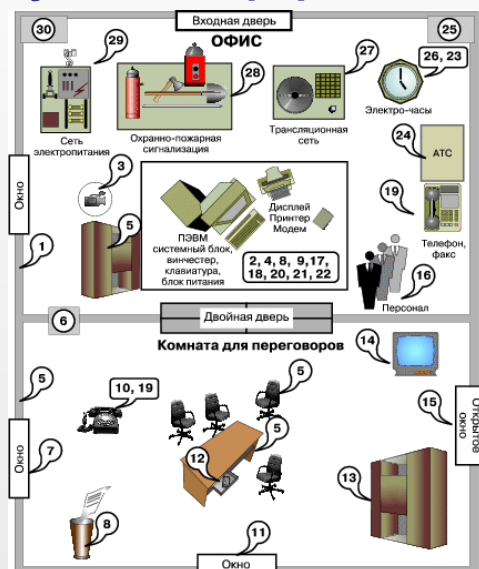
Факторы:

Многофункциональность бизнеса

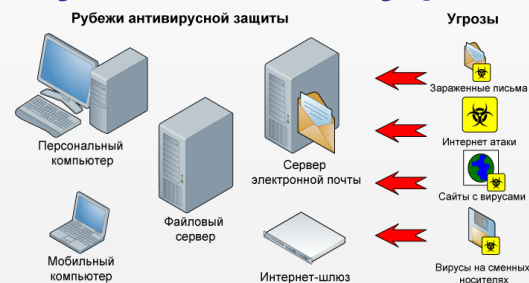
Карта бизнес-процессов модели eTOM



Множество каналов утечки информации



Множество уязвимостей и угроз



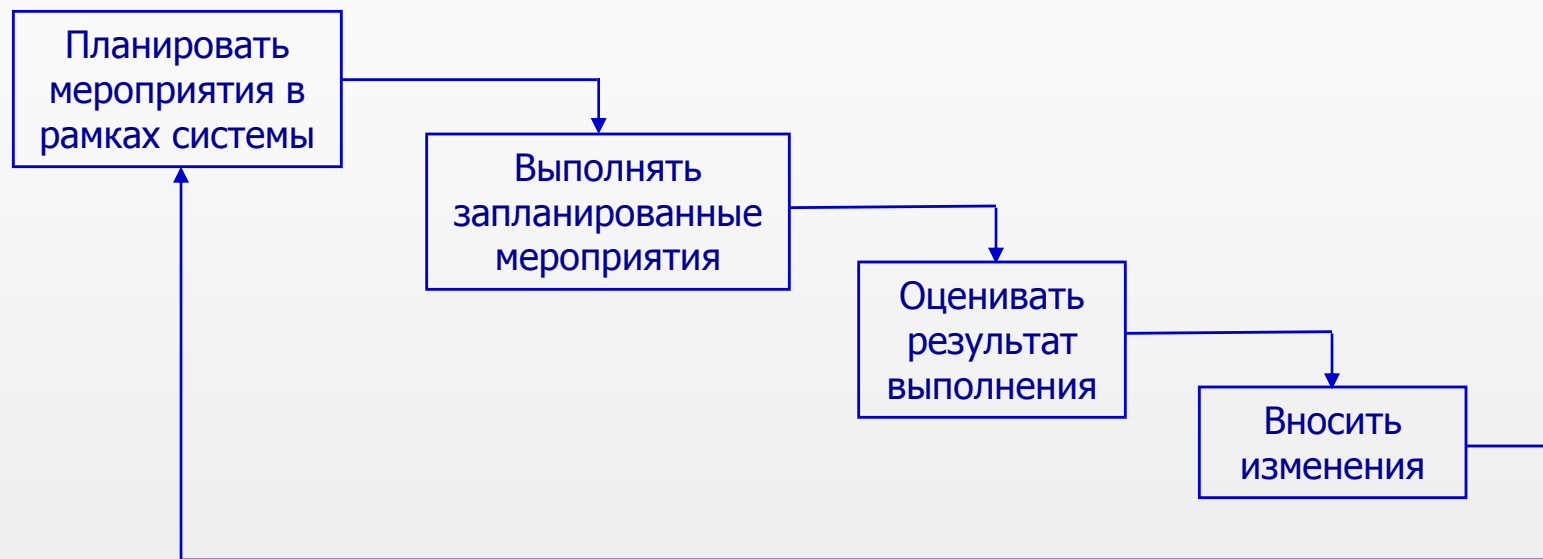
Решение должно быть комплексным:

система менеджмента информационной безопасности



ISO 27001: требования к системе менеджмента информационной безопасности

Стандарт предполагает построение и функционирование СМИБ в соответствии с циклом PDCA (Plan-Do-Check-Act – цикл Деминга)



Цикл Деминга обеспечивает постоянное улучшение системы.



ISO 27001: принципы построения СМИБ

Выделить область применения

Определить, в рамках какого бизнес-процесса будет действовать СМИБ

Выделить объекты управления

Составить перечень активов (т.е. всего, что имеет ценность для бизнеса организации с точки зрения информационной защиты)

Оценить риски

Определить уязвимости и угрозы для каждого актива, а также степень риска.

Определить способы управления

Для каждого актива выбрать способ разрешения риска, а также соответствующие методы управления (контроли).

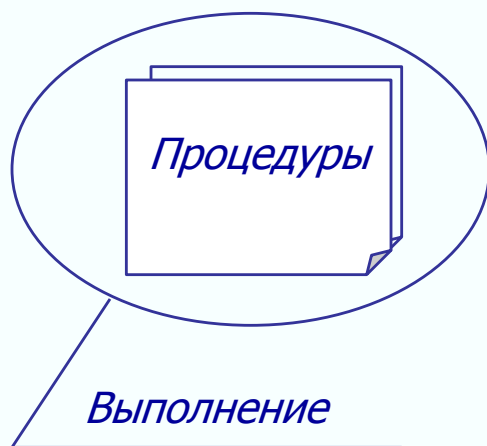


Система менеджмента информационной безопасности

Plan



Do



Check

Результативность:

- степень соответствия результатов целям

Пригодность:

- соответствие политики целям,
- степень соответствия контролей и процедур политикам

Исполнимость:

- степень выполнения процедур

Act

Корректирующие действия:

- определить причину,
- определить действия по ее устранению,
- выполнить действия,
- проверить результативность действий