Безопасность сервисов

Дмитрий Истомин,
директор по развитию
Уральского центра систем безопасности

Неконференция 2011
*aaS предпринимателей

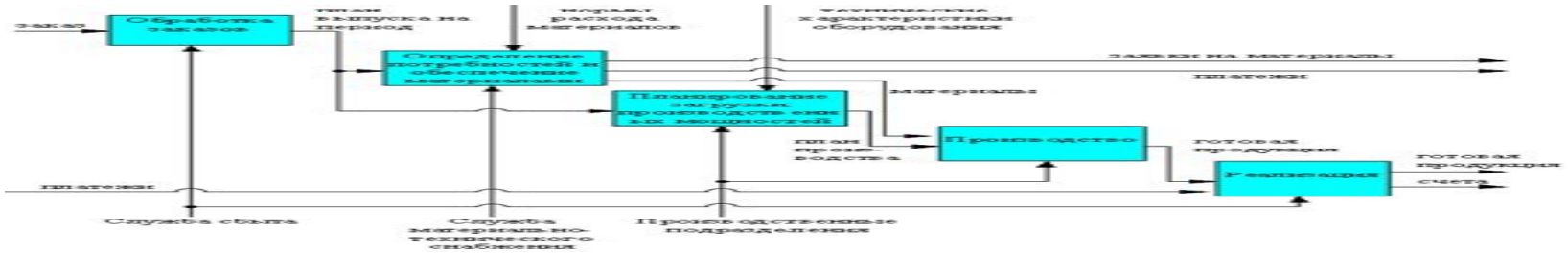
Содержание

- Какой он – безопасный сервис?
  Бизнес-процессы, показатели, безопасное состояние.
- Когда и зачем думать про безопасность?

- Как сделать сервис безопасным с минимумом затрат?
  Никак! SDL. Цикл разработки
  Оценка рисков
- Как сделать так, чтобы мне поверили?
- Безопасность на уровне требований и проектирования.
-

  Пример оформления ссылки | Дополнительная ссылка

Какой он – безопасный сервис?



Сервис – это автоматизация бизнес-процесса.

Безопасный сервис – это **безопасная** автоматизация бизнес-процесса.

Безопасный сервис – это **безопасная** автоматизация **безопасного** бизнес-процесса.

Безопасно = риски приемлемы VS **Безопасно** = функционально!

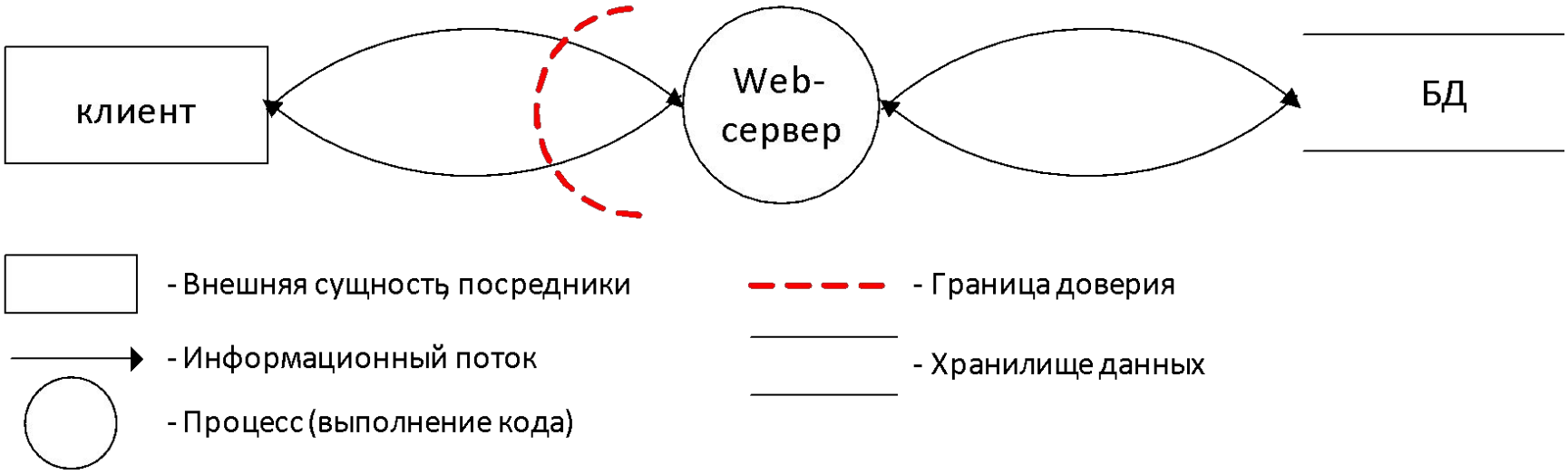
Безопасно для кого? **Владелец или пользователь?**

Когда нужно думать о безопасности?

Как сделать безопасный сервис без затрат?

Никак

Модель сервиса



Структурные элементы: хранилища данных, посредники, процессы и границы доверия

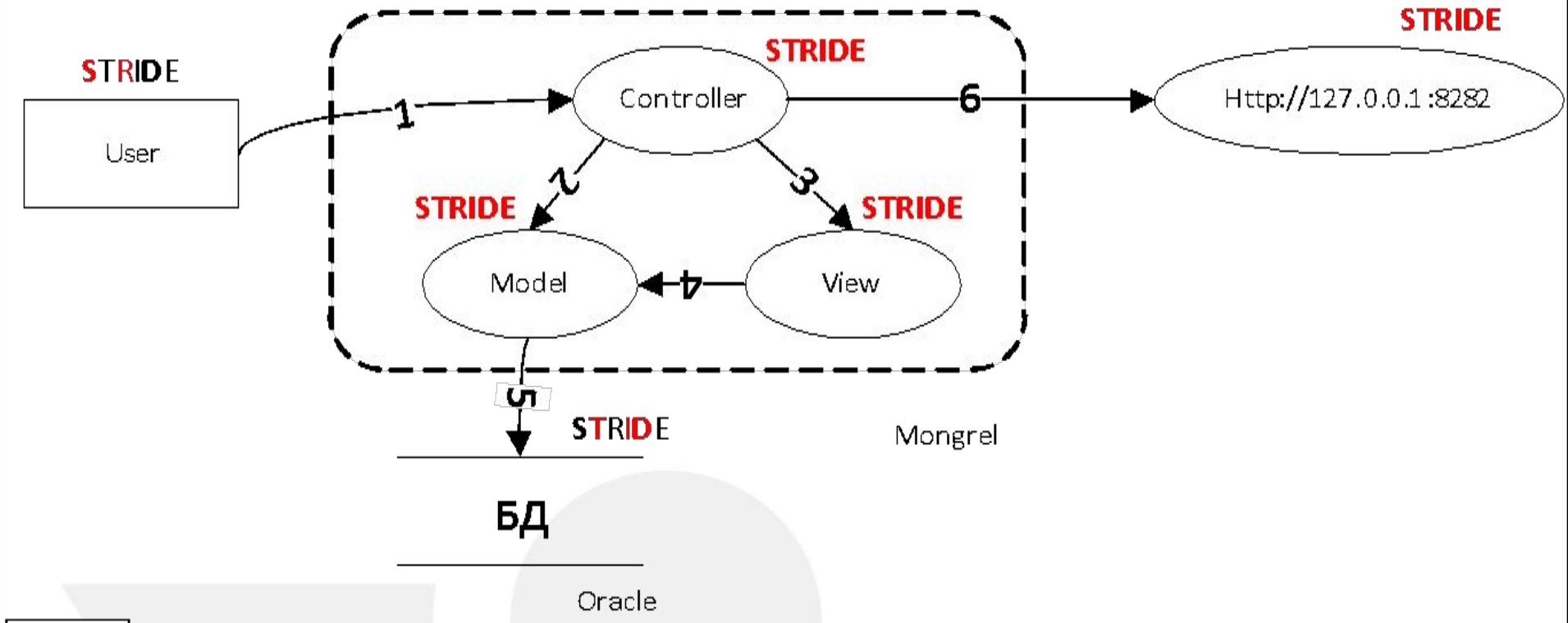
Информационные потоки

Модель угроз

STRIDE model:

- **S -** Spoofing of Identity – подмена идентификатора.
- **T -** Tampering with Data – случайное/преднамеренное искажение данных
- **R -** Repudiation – отказ от авторства
- **I -** Information Disclosure – утечка информации
- **D -** Denial of Service – блокирование доступа
- **E -** Elevation of Privilege – првышение прав доступа

Модель угроз



Как сделать сервис безопасным?

Пример методики разработки: **Secure Development Lifecycle**

Стадии:
1. Формирование требований (Reqiurements)
2. Проектирование (Design)
3. Реализация (Implementation)
4. Проверка (Verification)
5. Выпуск (Release)
6. Поддержка (Response)

У меня все безопасно. Как мне поверят?

Пользователь хочет быть уверен в том, что:

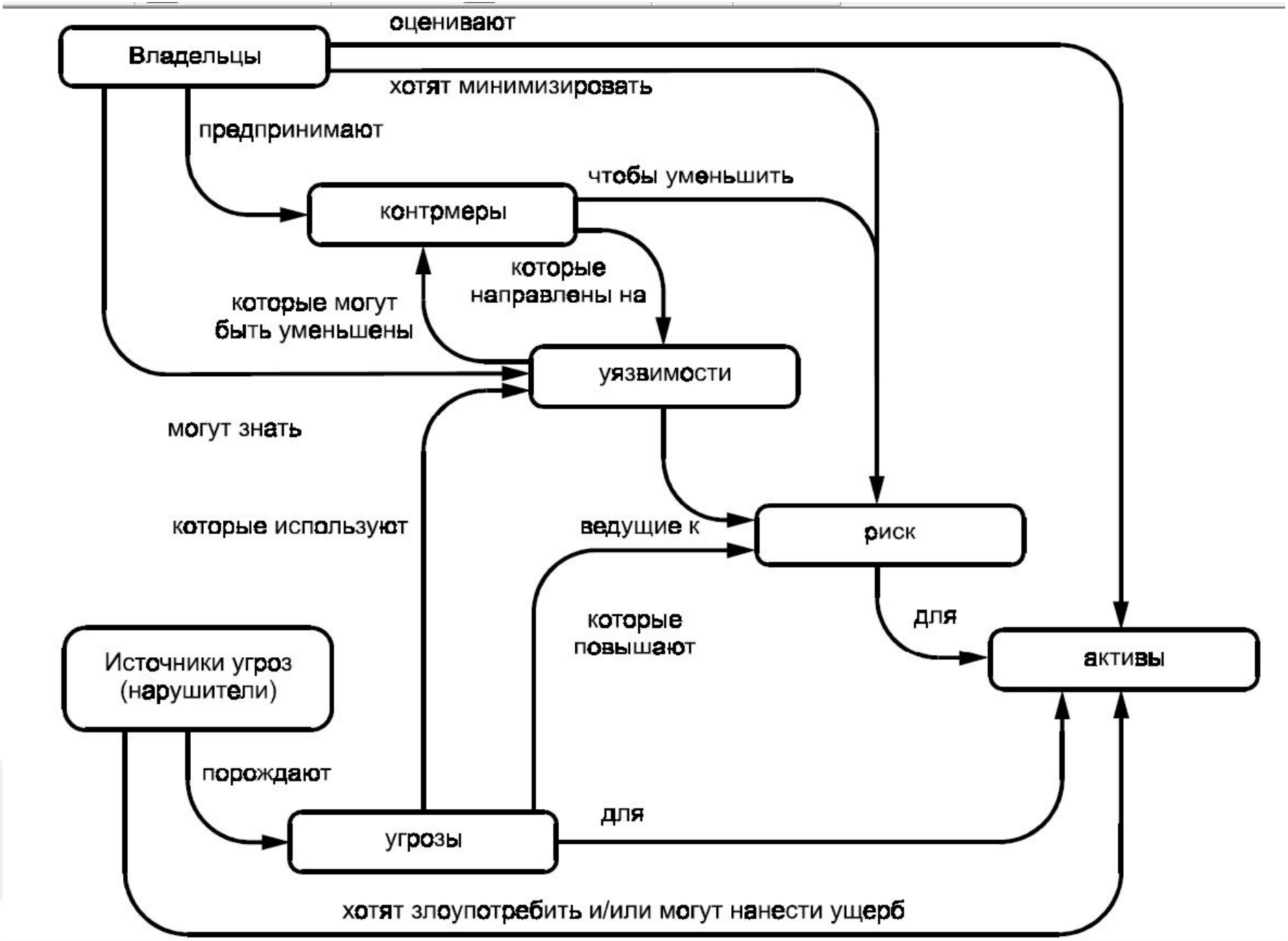
1. Архитектура безопасна (функциональные требования)
2. Реализация заслуживает доверия (требования доверия)

Что влияет:

1. Личный опыт и опыт близкого круга людей
2. Экспертная оценка

ISO 15408 Common Criteria

Часть	Потребитель	Разработчик	Оценщик
1	Общие сведения по применению. Руководство по структуре профилей защиты	Общие сведения и справочное руководство по разработке требований и формулированию спецификаций безопасности для объектов оценки	Общие сведения и руководство по применению. Руководство по структуре профилей защиты и заданий по безопасности
2	Руководство и справочник по формулированию требований к функциям безопасности	Справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки	Критерии оценки, используемые при определении эффективности выполнения объектом оценки заявленных функций безопасности
3	Руководство по определению требуемого уровня доверия	Справочник по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки	Критерии оценки, используемые при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности


оценивают
Владельцы
хотят минимизировать
предпринимают
чтобы уменьшить
контрмеры
которые
направлены на
которые могут
быть уменьшены
уязвимости
могут знать
которые используют
ведущие к
риск
для
которые
повышают
активы
Источники угроз
(нарушители)
порождают
для
угрозы
хотят злоупотребить и/или могут нанести ущерб

Требования безопасности

Функциональные требования налагаются на те функции, которые предназначены для поддержания безопасности и определяют желательный безопасный режим функционирования.

Примеры функциональных требований: требования к идентификации, аутентификации, аудиту безопасности, неотказуемости источника

Требования доверия налагаются на действия разработчика и оценщика.

Примеры требований доверия: требования к строгости процесса разработки, по поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Требования безопасности

Класс – наиболее общее группирование требований безопасности. Все составляющие класса имеют общую направленность.

Составляющие класса называются семействами. ***Семейство*** – это группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью.

Составляющие семейства называются компонентами. ***Компонент*** описывает набор требований безопасности, который является наименьшим выбираемым набором требований безопасности.

Компоненты составлены из отдельных элементов. **Элемент** - это выражение требований безопасности на самом нижнем уровне. Он является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

Требования безопасности. Пример

Класс FIA – требования к функциям установления и верификации заявленного идентификатора пользователя

Семейство FIA_SOS – требования к механизмам, которые реализуют определенную метрику качества для предоставляемых секретов и генерируют секреты, удовлетворяющие определенной метрике.

Компоненты:

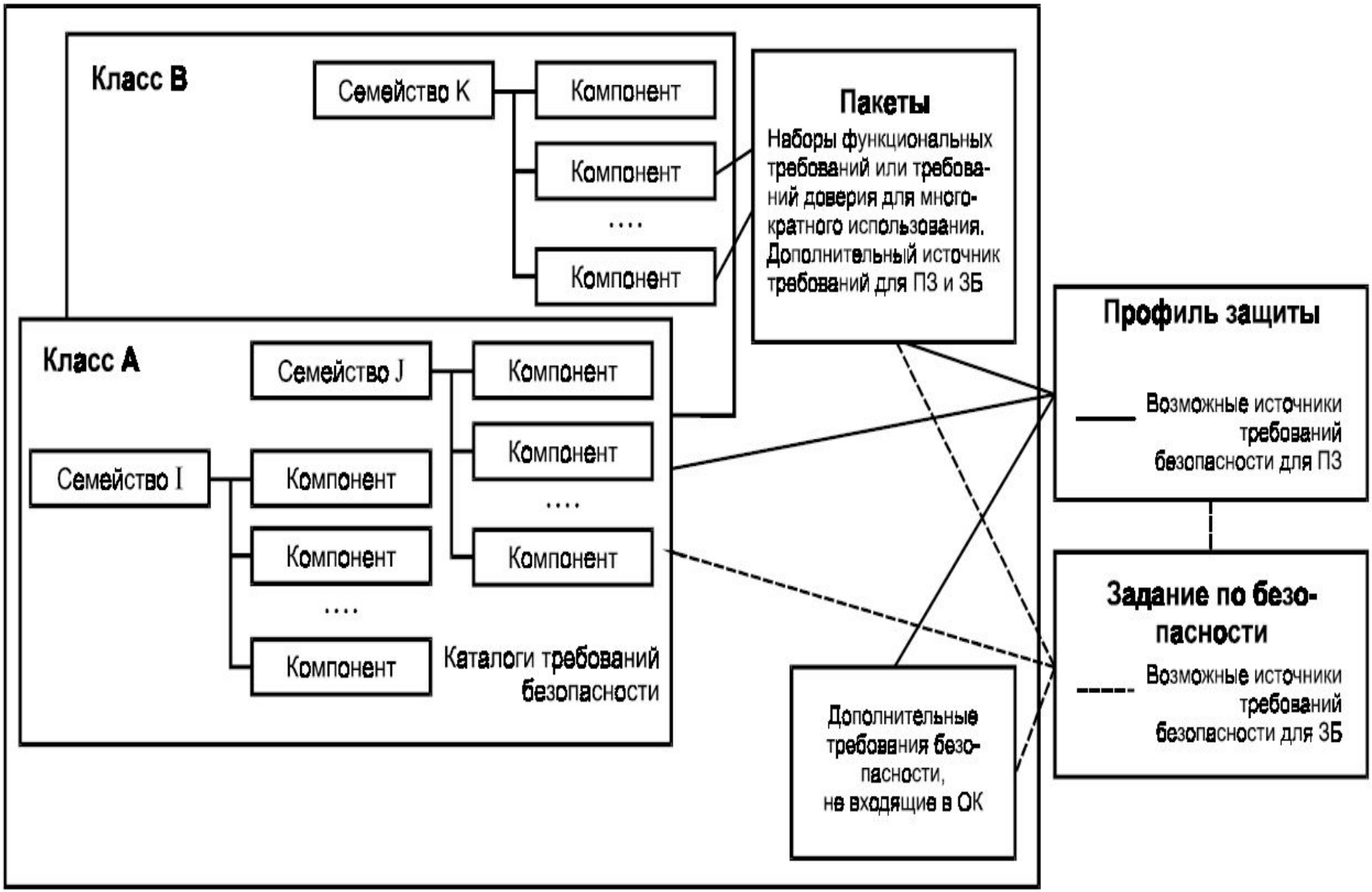
FIA_SOS.1 "Верификация секретов" содержит требование, чтобы ФБО верифицировали, отвечают ли секреты определенной метрике качества.

FIA_SOS.2 "Генерация секретов ФБО" содержит требование, чтобы ФБО были способны генерировать секреты, отвечающие определенной метрики качества.

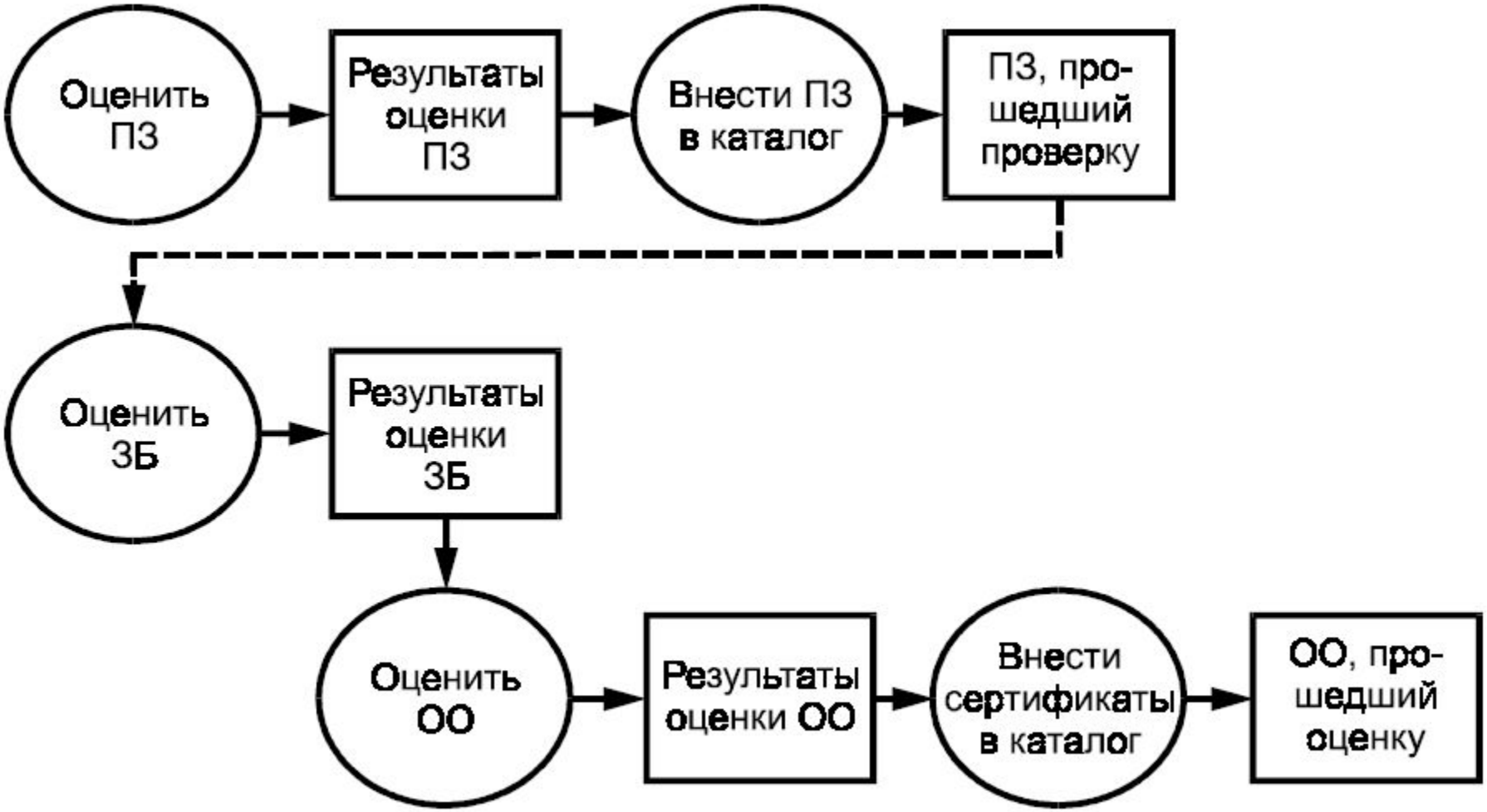
ОУД

Оценочные уровни доверия (ОУД) - это предопределенные пакеты требований доверия. ОУД является базовым набором требований доверия для оценки. Каждый ОУД определяет непротиворечивый набор требований доверия. Совместно ОУД формируют упорядоченное множество, которое является предопределенной в ОК шкалой доверия

«ОК» устанавливает ряд гарантированных уровней соответствия Оценочный уровень доверия (**ОУД**), используемых при оценке продуктов. Профили защиты для уровней ОУД1–ОУД4 являются общими для всех стран, поддерживающих стандарт ОК. Для высших уровней ОУД5–ОУД7 профили защиты индивидуально разрабатываются каждой страной для учета национальных особенностей защиты государственных секретов.



Итоговая оценка



Спасибо за внимание!

Неконференция 2011
*aaS предпринимателей