Канадские критерии безопасности

Созданы в 1993г

Цель разработки

- Единая шкала критериев
- Основа для разработки спецификаций безопасных компьютерных систем
- Средства для описания характеристик безопасных компьютерных систем

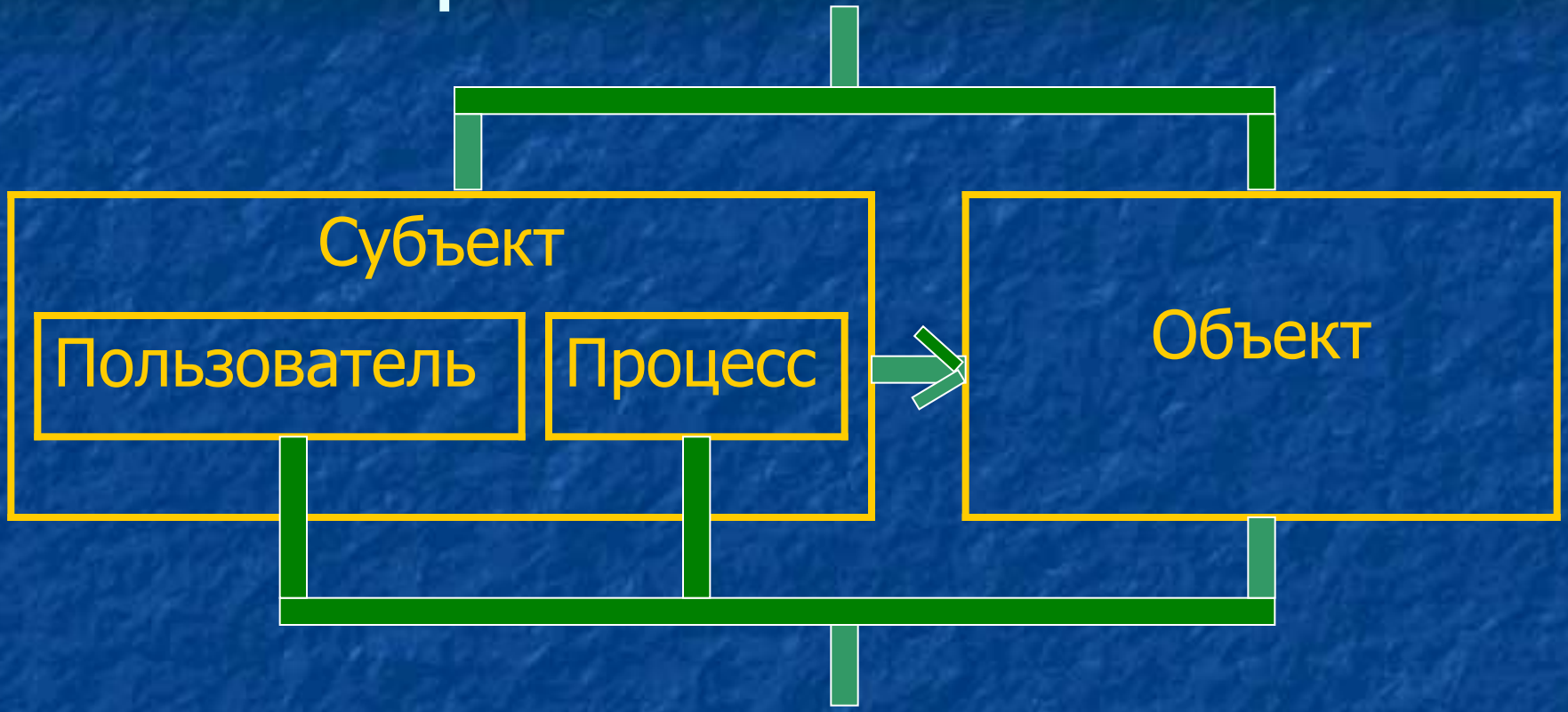
Все компоненты системы, находящиеся под управлением ТСВ называются **объектами**.

Пользователь - физическое лицо, взаимодействующее с системой

Процесс— программа, выполнение которой инициировано пользователем.

Объект **-** пассивный элемент, над которым выполняют действия ***пользователи*** и ***процессы.***

Оранжевая книга



Канадские критерии

Соответствие «Оранжевой книги» и «Канадских критериев безопасности»

Основные положения и структура "Канадских критериев"

Требования безопасности представлены в виде:

- функциональных требований к средствам защиты
- требований к адекватности их реализации.

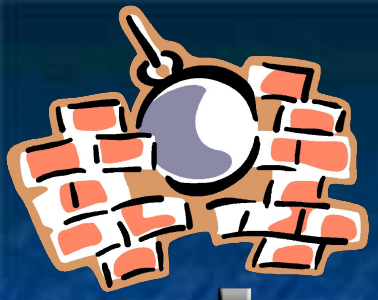
Функциональные критерии

- Критерии конфиденциальности
- Критерии целостности
- Критерии работоспособности
- Критерии аудита



Критерии конфиденциальности

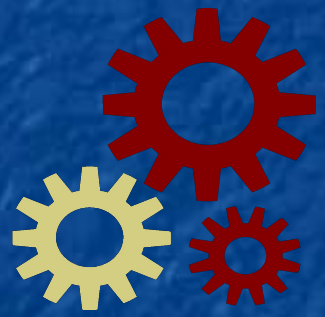
- Контроль скрытых каналов
- Произвольное управление доступом
- Нормативное управление доступом
- Повторное использование объектов



Критерии целостности

- Домены целостности
- Произвольное управление целостностью
- Нормативное управление целостностью
- Физическая целостность
- Возможность осуществления отката
- Разделение ролей
- Самотестирование

Критерии работоспособности



- Контроль за распределением ресурсов
- Устойчивость к отказам и сбоям
- Живучесть
- Восстановление

Критерии аудита

- Регистрация и учет событий в системе
- Идентификация и аутентификация
- Прямое взаимодействие с ТСВ.

- Внутри каждой группы функциональных критериев определены уровни безопасности, отражающие возможности средств защиты по решению задач данного раздела.
- Уровни с большим номером обеспечивают более высокую степень безопасности.



- Критерии адекватности определяют требования к процессу проектирования и разработки компьютерной системы.
- Рассматриваются без разделения на подгруппы.
- Уровень адекватность присваивается всей системе в целом.
- Более высокий уровень означает более полную и корректную реализацию политики безопасности.

Критерии адекватности

- Архитектура системы
- Среда разработки
- Контроль процесса разработки
- Поставка и сопровождение
- Документация
- Тестирование безопасности

Приложения к «Канадским критериям» включают в себя

- описание предложенной концепции
- руководства по применению критериев
- набор стандартных профилей защиты
- ранжированный перечень функциональных критериев и критериев адекватности

Выводы

- Впервые отделены функциональные требования от требований адекватности
- Используется независимое ранжирование требований по каждому разделу.
- Уровень адекватности характеризует качество всей системы в целом.

Конец лекции 8

Единые критерии безопасности

1999г

Цель разработки:

Объединить основные положения «Европейских критериев», «Федеральных критериев» и «Канадских критериев» безопасности компьютерных систем".

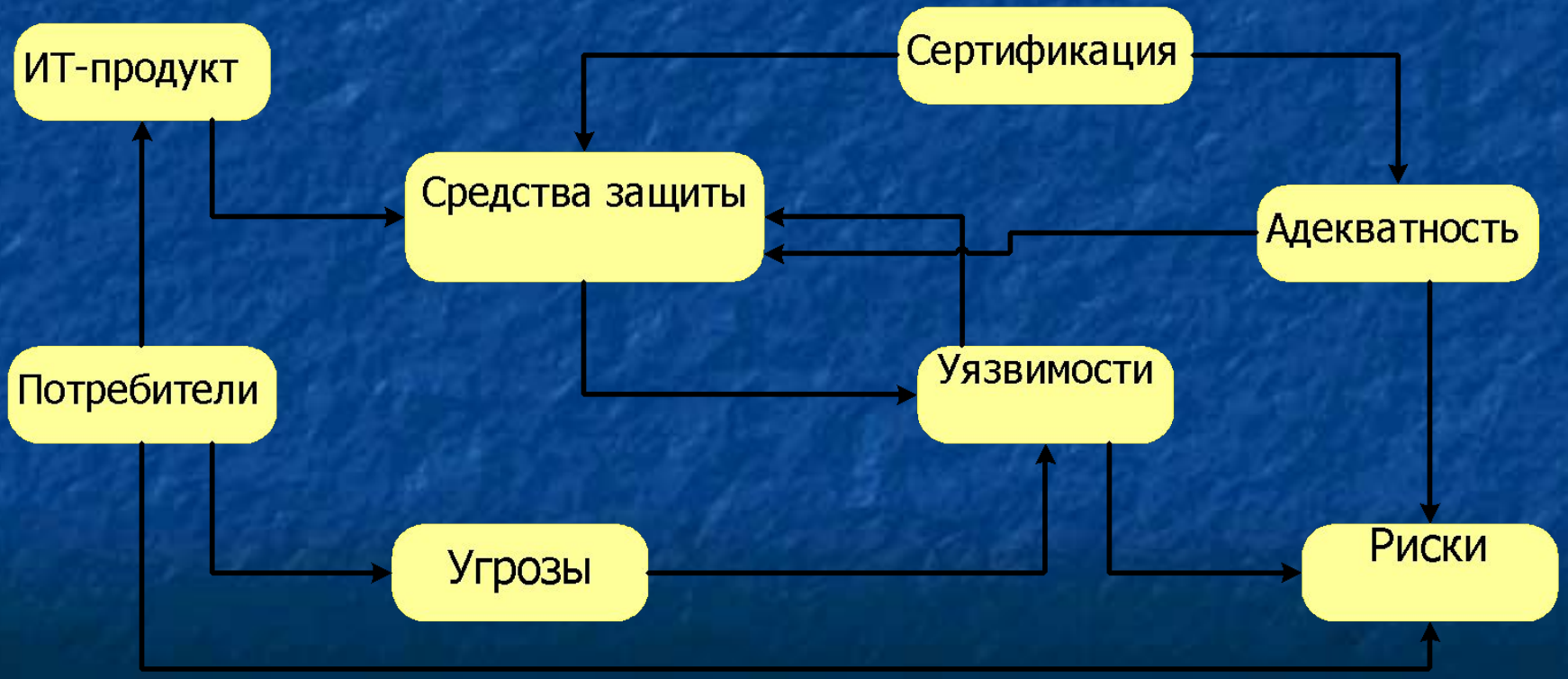
«Единые критерии» удовлетворяют запросы трех групп специалистов:

- потребителей продуктов ИТ

- Производителей

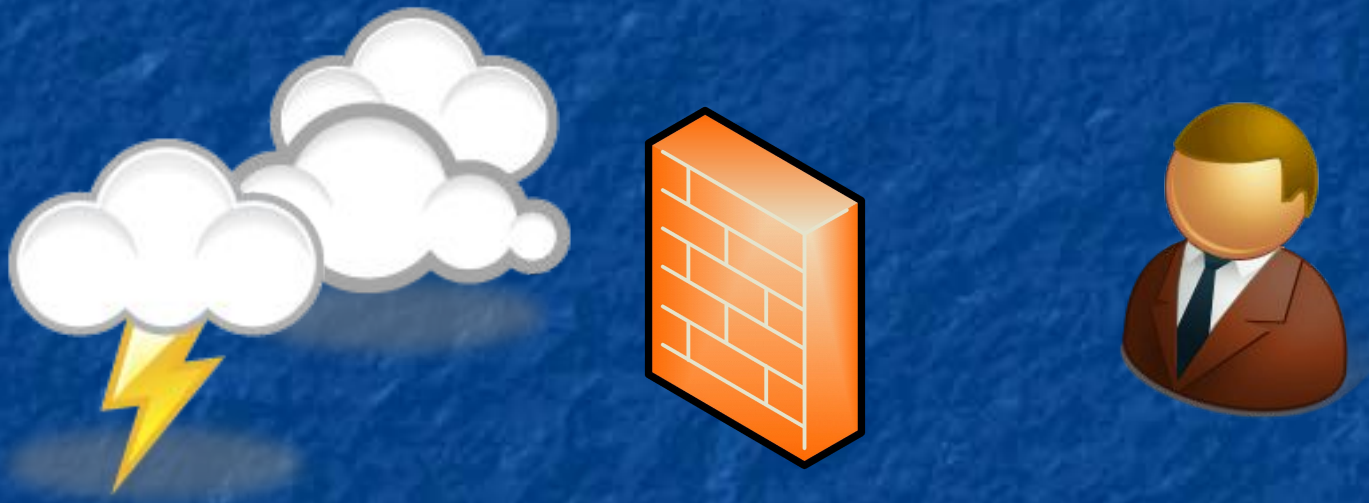
- экспертов по квалификации уровня их безопасности

В концепцию "Единых критериев" входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.



Основные положения

Задачи защиты — *выражает потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности*



Профиль защиты — специальный нормативный документ, представляющий собой совокупность:

- Задач защиты,
- функциональных требований,
- требований адекватности

и их обоснования.

Служит руководством для разработчика ИТ продукта при создании Проекта защиты.

Проект защиты — специальный нормативный документ, представляющий собой совокупность:

- Задач защиты,
- функциональных требований,
- требований адекватности,
- общих спецификаций средств защиты

и их обоснования.

В ходе квалификационного анализа служит в качестве описания ИТ-продукта.

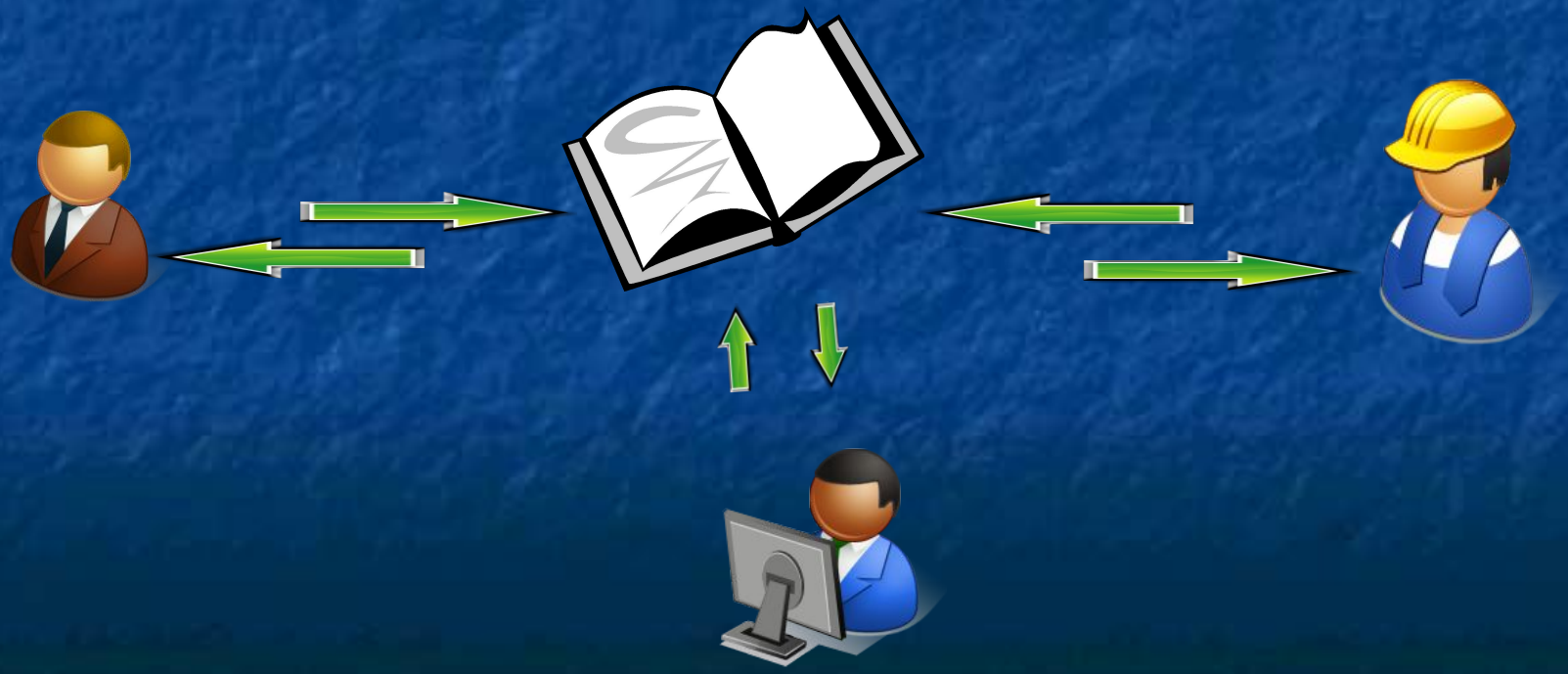
Профиль защиты и спецификации средств защиты составляют Проект защиты, который и представляет ИТ-продукт в ходе квалификационного анализа.

Для проведения квалификационного анализа разработчик продукта должен представить:

- Профиль защиты;
- Проект защиты;
- обоснования и подтверждения свойств и возможностей ИТ-продукта;
- ИТ-продукт;
- дополнительные сведения, полученные путем проведения независимых экспертиз.

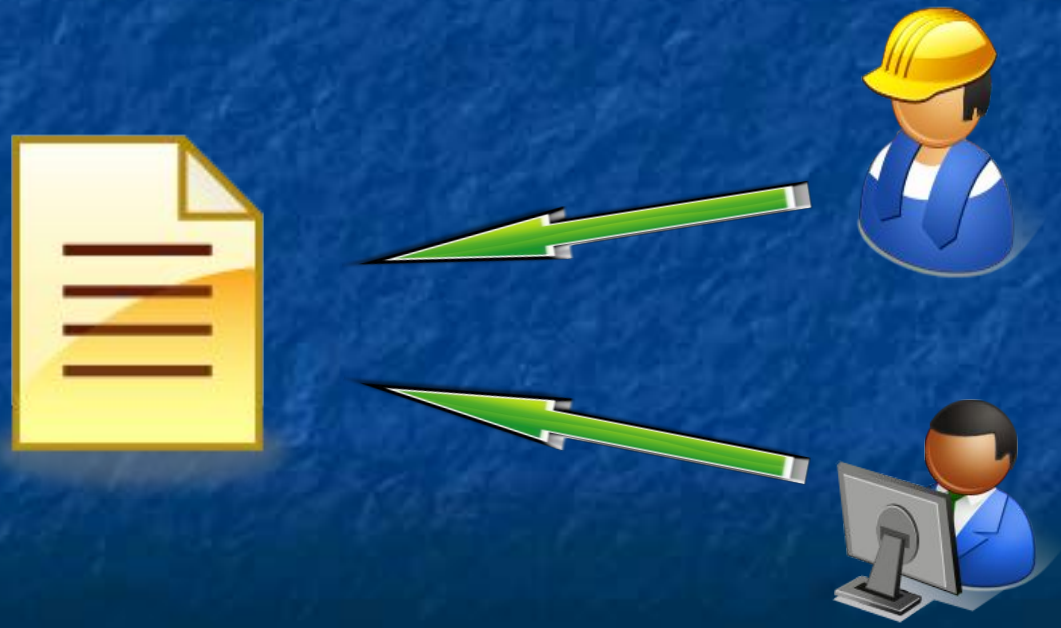
Процесс квалификационного анализа включает три стадии:

- Анализ Профиля защиты
- Анализ Проекта защиты.
- Анализ ИТ-продукта на предмет соответствия Проекту защиты.



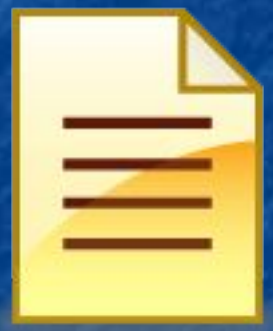
Результат квалификационного анализа –

заключение о том, что ИТ-продукт соответствует представленному Проекту защиты.



Профиль защиты

Определяет требования безопасности к определенной категории ИТ-продуктов



Основные понятия

- ***Введение*** - информация, необходимая для поиска профиля защиты
- ***Идентификатор*** - уникальное имя профиля
- ***Условия эксплуатации*** - ограничения на условия его применения

Основные требования

- *Функциональные требования*
- *Требования адекватности*
- *Требования к среде эксплуатации*

Конец лекции 9