УНИФИКАЦИЯ ПРОЦЕССА ПОСТРОЕНИЯ БЕЗОПАСНЫХ ВСТРОЕННЫХ СИСТЕМ

Десницкий В.А., Чечулин А.А.,

Учреждение Российской академии наук
Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто-2011, 30 марта – 2 апреля 2011 г.

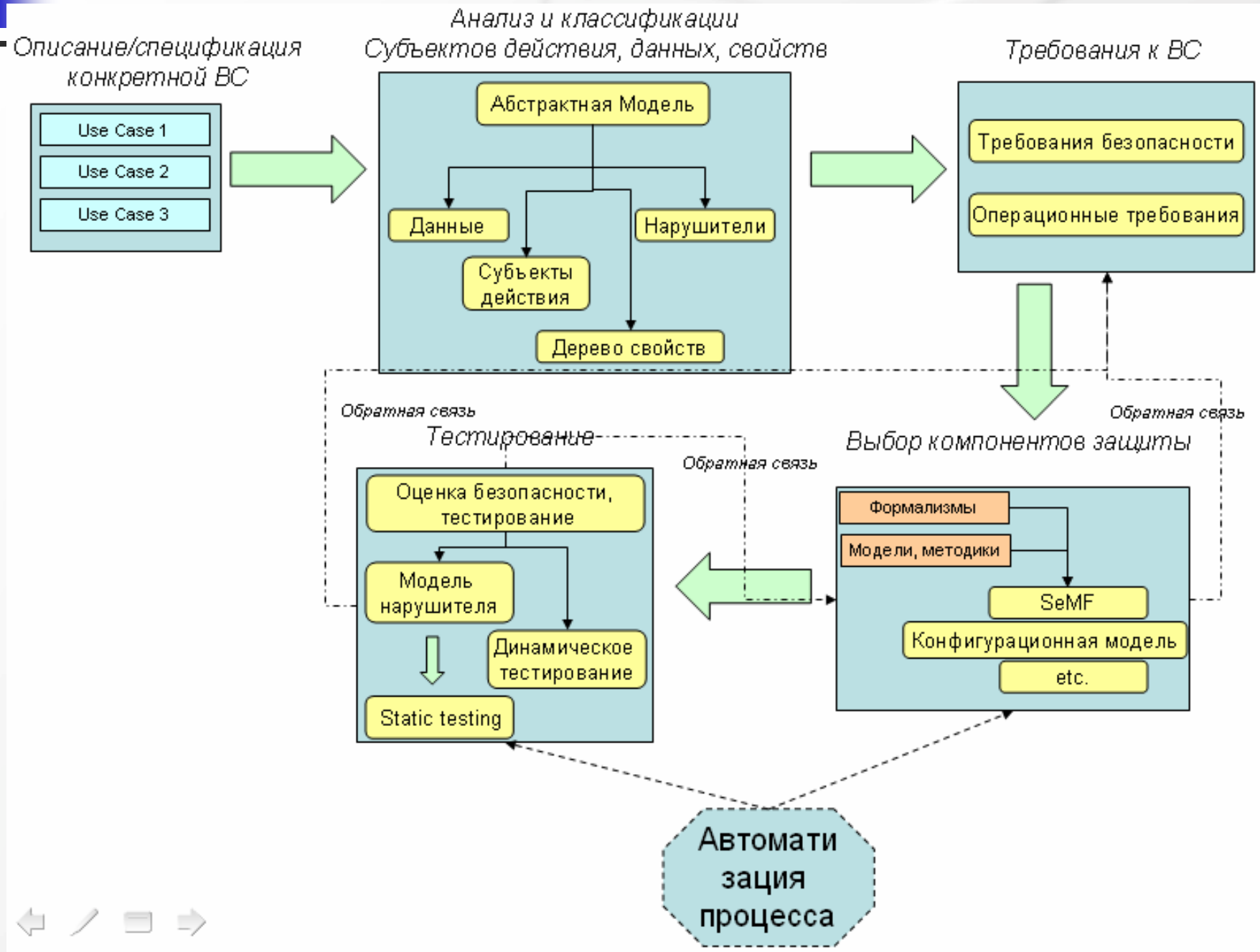
Проект SecFutur

- Работа проводится в рамках Европейского исследовательского проекта FP7 SecFutur
  - Design of Secure and energy-efficient embedded systems for Future Internet applications
- Проект посвящен исследованию вопросов построения безопасных встроенных систем *(ВС)*
- Цели:
  - Формирование унифицированного процесса построения безопасных встроенных систем *(УППБВС)*, в рамках которого вопросы безопасности должны учитываться на каждой стадии процесса
  - Автоматизация процесса
  - Достижение компромисса между
    - Безопасностью ВС
    - Ресурсоэффективностью
    - Функциональностью
    - Стоимостью

Решаемые задачи

- В частности, решаются следующие задачи:
  - Построение абстрактной модели ВС
  - Конфигурирование на основе существующих средств защиты
  - Оценка безопасности и построение автоматизированной среды тестирования
  - Программная реализация и обоснование эффективности предлагаемых решений
  - Применение для нескольких областей приложения (Use Cases)

Процесс построения безопасных ВС



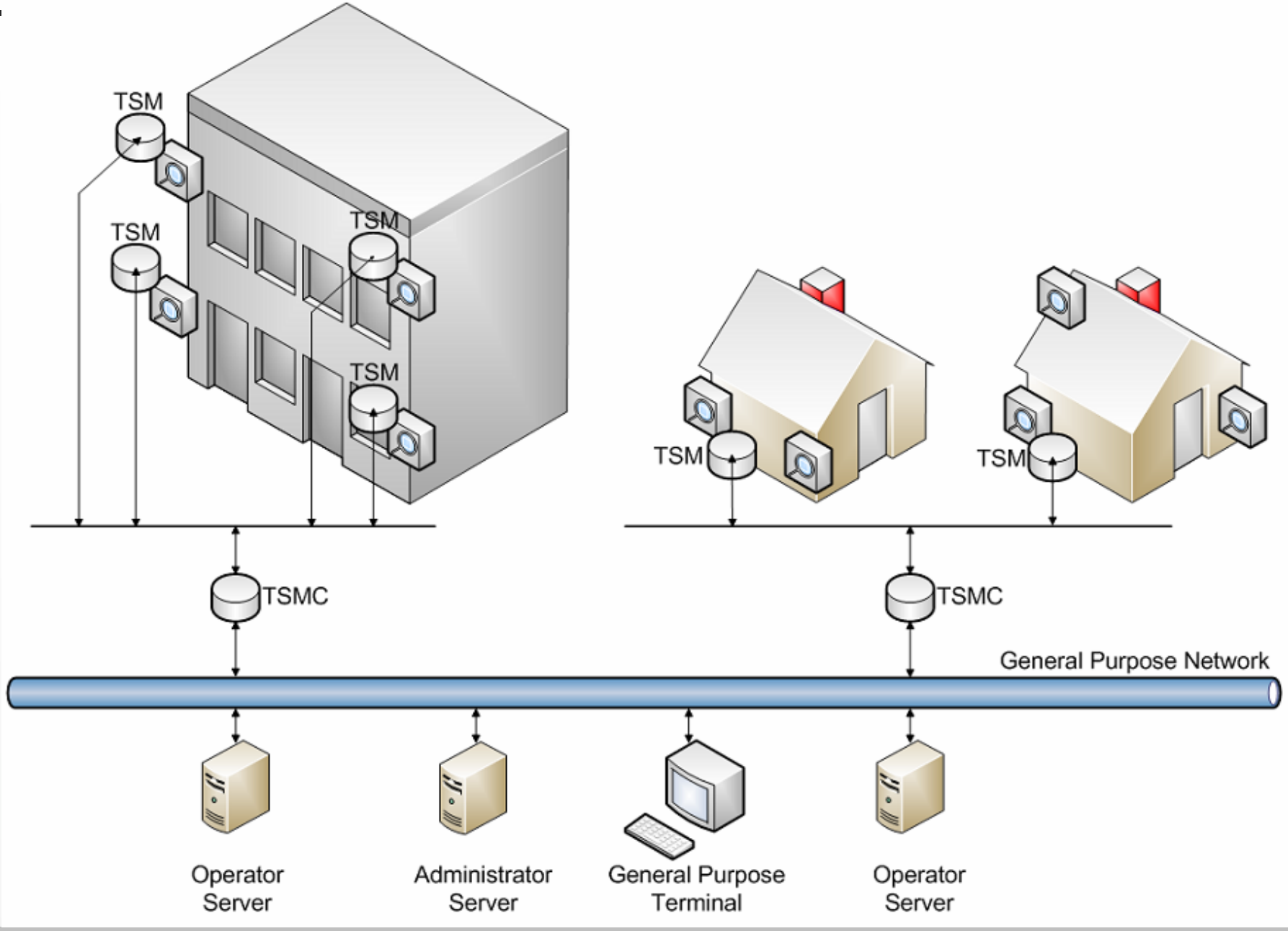
Use Cases

- Use Cases *(примеры использования и применения)*
  - Мульти-функциональный шлюз для телекоммуникационных сервисов *(Multi-functional service gateway)*
  - Сеть мобильного реагирования при чрезвычайных ситуациях *(Secure ad-hoc wireless mesh communication for crisis management)*
  - Система контроля за расходом электроэнергии потребителями *(Metering devices with legal calibration requirements)*

Use Case: Система контроля за расходом электроэнергии (1/3)

- Система контроля за расходом электроэнергии потребителями
  - Сенсоры *(Trusted Sensor Module, TSM)*
  - Данные измерений
  - Коллекторы *(Trusted Sensor Module Colector, TSMC)*
  - Оператор, администратор
- Возможный нарушитель
  - Нарушение корректной работы сервиса
- Цели безопасности: высоко- уровневые требования к безопасности системы
  - аутентичность данных измерений
  - конфиденциальность данных измерений
  - Доступность данных и сети

Use Case: Система контроля за расходом электроэнергии (2/3)



Use Case: Система контроля за расходом электроэнергии (3/3)

- Цели безопасности
  - Целостность передаваемых данных
  - Целостность данных, хранимых на устройстве
  - Конфиденциальность передаваемых данных
  - Конфиденциальность данных, хранимых на устройстве
  - Контроль потоков данных
  - Отслеживание активности (мониторинг)
  - Безопасное обновление
  - Обнаружение чужеродных компонентов
  - Обнаружение анамалий сигнала сенсоров
  - Защита пользовательских функций
  - Непрерывный мониторинг целостности
  - Защита от «вторичных ошибок» (ошибки бизнес-процесса не быть причиной ошибок в системе безопасности)
  - Разделение ПО и данных
  - И др.

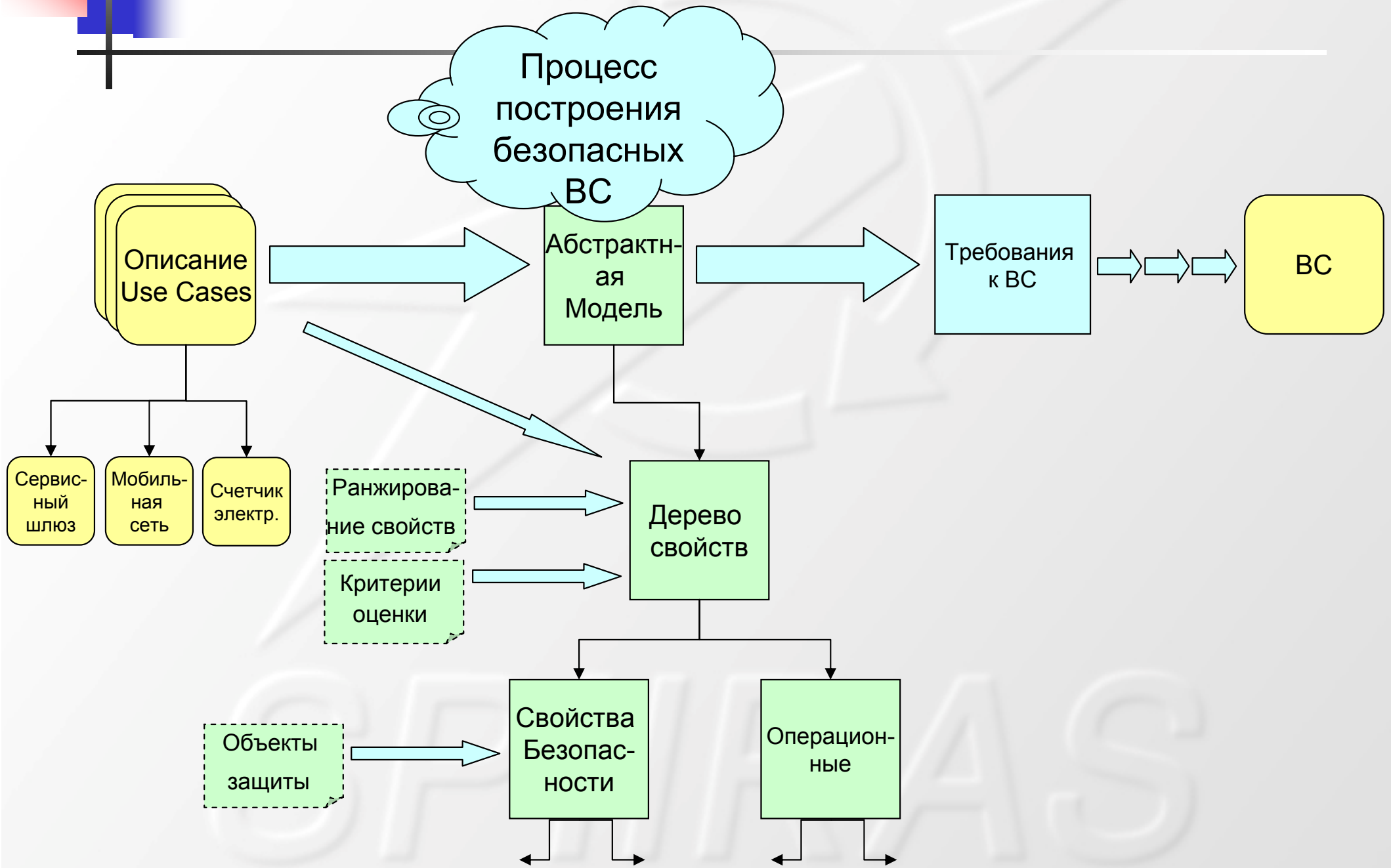
Абстрактная модель (АМ) ВС

- Роль абстрактной модели (АМ):
  - Обобщенное представление ВС в рамках *унифицированного процесса построения безопасных встроенных систем*
    - АМ как интерфейс между ВС и УППБВС
  - Способ формальной спецификации ВС
    - С учетом вопросов безопасности ВС

Абстрактная модель

- АМ включает обобщенное описание
  - Архитектуры ВС
  - Взаимодействия ВС и легитимных пользователей
  - Представления функций ВС
  - **Дерева свойств**
  - **Модели нарушителя**
- Построение способа спецификации на основе UML

Методология применения АМ



Дерево свойств ВС

- Свойства ВС
  - Свойства безопасности
    - Базовые свойства безопасности
    - Специфичные свойства безопасности
  - Другие свойства (не относящиеся к безопасности)

- Свойства ВС
  - Внешние (оцениваются извне ВС)
  - Внутренние (относящиеся к реализации каких-либо функций ВС)

Базовые свойства безопасности

- **Свойства безопасности данных**
  - Конфиденциальность
  - Целостность
  - Доступность
- **Свойства безопасности коммуникаций**
  - Конфиденциальность
  - Целостность
  - Доступность
- **Свойства безопасности платформы**
  - Безопасность ПО
    - Аутентичность ПО *(обнаружение)*
    - Стойкость ПО к модификациям *(препятствование, реагирование)*
  - Аутентичность аппаратного обеспечения
- **Безопасность пользователей**
  - Доступ *(Мандатный/на основе ролей/дискреционный)*
  - Аутентичность пользователей
    - Виды аутентификации (*password based, smart card, biometrics и пр.*)

Специфичные свойства безопасности

- **Внутренние свойства системы** (Свойства, относящиеся к какой-либо функции ВС):
  - **Обновление**
    - Характер обновления
      - Обновление кода/данных
        - Обновление ключей (*небольшие изменения*)
        - Замещение программных компонентов
      - Замещение компонентов аппаратного обеспечения
    - Вид обновления
      - Автоматизированное обновление с удаленного хоста
      - Необходимость участия конечного пользователя
      - Необходимость участия администратора
  - **Наличие коммуникационных интерфейсов**
    - Тип соединения
      - Wire-протоколы (*Ethernet, USB, Firewire и т.п.*)
      - Wireless-протоколы (*Bluetooth, WI-FI, MI-MAX, InfraRed и т.п.*)
    - Объем информации, передаваемой через интерфейс
    - Аутентичность топологии сети
    - Функциональность, получаемая через интерфейс
      - Безопасная маршрутизация, связь с системами навигации и т.п.
    - Тип коммуникации (потоковая/пакетная передача)

Операционные свойства

- Внешние свойства (*оцениваются извне системы*)
  - Свойства ресурсопотребления и производительности
    - Интегральное свойство: производительность с точки зрения конечного пользователя (скорость работы устройства, время реакции)
    - Свойства потребления ресурсов системы
      - CPU
      - Память
      - Пропускная способность соединения
      - ROM
  - Свойства энергопотребления
    - Ресурс аккумуляторы ВС «Battery life»
    - Энергоэффективность
  - Стоимость
    - Аппаратное обеспечение
    - ПО
    - Интеграция, развертывание
    - Поддержка, сопровождение
  - Физические характеристики ВС (размеры, вес, форм-фактор устройства)

Ранжирование и критерии оценки

- **Значения свойства**
  - **Бинарные** *(+)/(-)*
    - Наличие некоторой функции, особенности поведения или SW/HW-компонента
    - Важность свойства
  - **Ранжирование значений**
    - Энергоэффективность
      - Метрики расхода электроэнергии
      - Классы энергопотребления устройств (ср. *Директива ЕС 92/75/ЕС*)
    - Свойства производительности
      - Метрики: время, количество тактов CPU, величина пропускной способности соединения, количество выделяемых сегментов памяти и пр..
    - Доступность
      - Метрики:
        - Отношение между временем работы системы и всем временем
        - Вероятностные оценки
    - Свойства обновления
      - Метрики:
        - Частота обновления
        - Интенсивность (объемы замещаемого кода/данных за промежуток времени)

Декомпозиция абстрактной модели

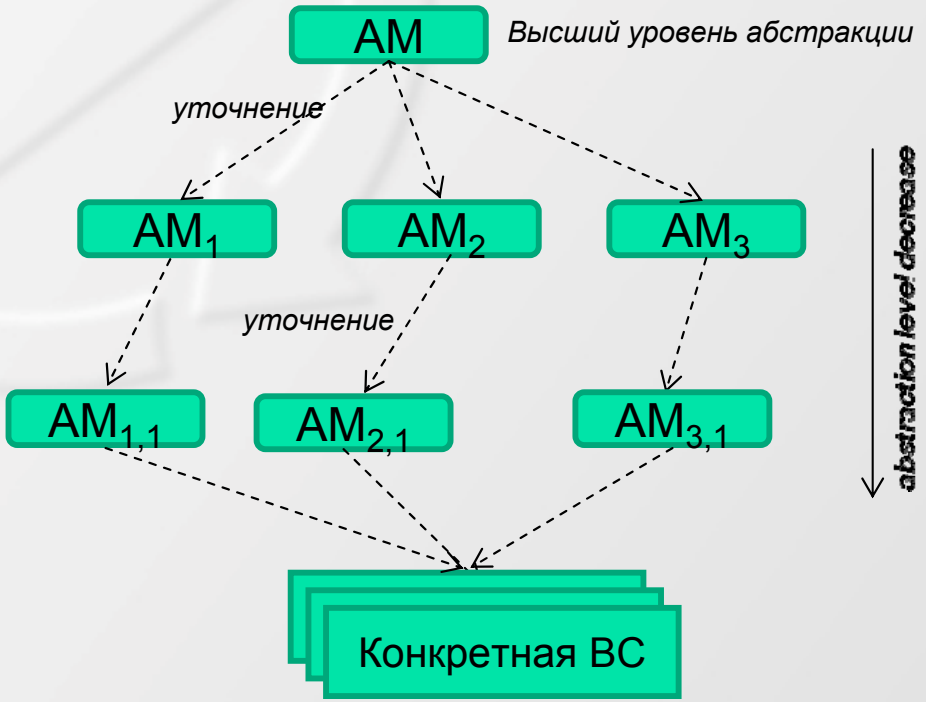
В соответствии с видами коммуникаций ВС

- AM_1: Отдельное встроенное устройство
- AM_2: ВС с локальными коммуникациями
- AM_3: ВС, управляемое и/или аттестуемое удаленными сущностями через Интернет
- Пример:

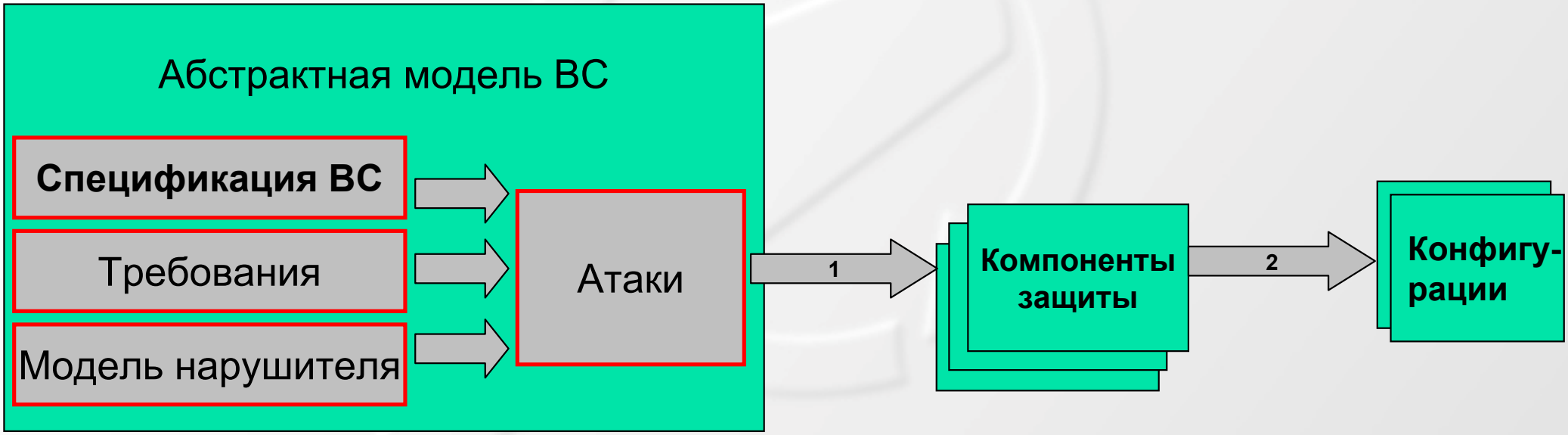
  $AM_{1,1}$:
  - Мобильные устройства контроля кровеносного давления человека

  $AM_{2,1}$:
  - Автоматизированные счетчики топлива на АЗС

  $AM_{3,1}$:
  - Распределенная система измерения и контроля расхода электроэнергии потребителями



Задача конфигурирования



1. Сопоставляет встроенной системе множество возможных компонентов безопасности, нацеленных на противодействие атакам
2. Методика поиска оптимальной комбинации компонентов *(оптимальность по свойству(-ам): свойства производительности, энергоэффективности, безопасности и пр.)*

Представление атак

- Обобщенная модель атак на ВС
  - Цели атакующего
  - Возможные действия
  - Ресурсы, инструменты, методы
- Классификации атак на ВС
  - [Rae, et al 2003] – классификация нарушителя исходя из уровня его взаимодействия с ВС
  - [Abraham, et al 1991] – классы нарушителя в соответствии с его возможностями

Классификация по типу взаимодействия с ВС

Нарушитель

Нарушитель типа 1.

Не имеет прямого доступа к устройству, н-р, сетевой доступ при по протоколам TCP/IP

Нарушитель типа 2.

Имеет прямой удаленный доступ к устройству, н-р, посредством Wi-Fi

Нарушитель типа 3.

Имеет прямой внешний доступ к устройству, н-р, через интерфейсы USB, JTag

Нарушитель типа 4.

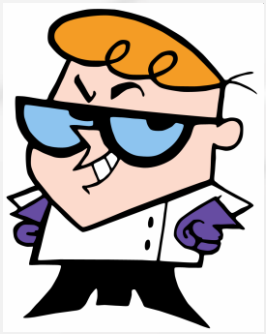
Имеет полный доступ к устройству, включая доступ к его электронным компонентам

Классификация по уровню возможностей нарушителя

Нарушитель

Уровень 1.

У нарушителя нет полного знания о системе и есть доступ только к общедоступному оборудованию



Уровень 2.

У нарушителя есть информация о конкретной системе и есть доступ к средне-сложному оборудованию

Уровень 3.

Нарушитель представляет собой организацию, у которой есть доступ к лабораторному оборудованию любой сложности и которая может создавать группы нарушителей 2-го типа

Описание нарушителей

Нару-ши-тели	Основные угрозы	Уровень 1	Уровень 2	Уровень 3
Тип 1	Перехват, анализ и подделка сообщений, передаваемых по сети, классические сетевые атаки на устройство	Использование общедоступных программных средств, таких как Nessus, Nmap, etc. Использование открытых баз уязвимостей	Поиск новых уязвимостей для конкретных ВС и создание программных средств для реализации атак на найденные уязвимости	Реализация распределенных атак и криптоанализ используемых протоколов
Тип 2	Перехват, анализ и подделка сообщений, передаваемых через беспроводные интерфейсы, удаленный съем информации (side-channels атаки) и атаки на сенсоры устройства	Атаки практически невозможны, т.к. нарушитель не имеет достаточных знаний и технических средств	Использование ИК и Bluetooth-модулей со своим ПО	Реализация любых доступных атак, включая прямое воздействие на электронные компоненты ВС
Тип 3	Атаки на интерфейсы ВС, к которым имеется прямой доступ. Атаки через данные, поступающие от сенсоров ВС (помещение устройства в полностью контролируемую среду)	Атаки практически невозможны, т.к. нарушитель не имеет достаточных знаний и технических средств	Реализация атак через прямое подключение к интерфейсам ВС	Реализация любых доступных атак, включая прямое воздействие на электронные компоненты ВС
Тип 4	Считывание данных напрямую с микросхем, Подмена электронных компонентов ВС	Атаки практически невозможны, т.к. нарушитель не имеет достаточных знаний и технических средств	Атаки практически невозможны из-за высокой сложности требуемого оборудования	Реализация любых доступных атак, включая анализ электронных компонентов при помощи электронных микроскопов

Применение модели нарушителя

- Модель нарушителя применяется для:
  - автоматизации проверки абстрактной модели ВС на наличие потенциальных уязвимостей
  - автоматизации построения списка тестов для физической проверки ВС
  - построения списка возможных компонентов защиты и конфигурационной модели
  - определения необходимого уровня защищенности от нарушителей различных типов и уровней

Дальнейшие исследования

- Расширение абстрактной модели, с учетом рассматриваемых примеров применения (Use Cases)
- Разработка UML-представления АМ и спецификация Use Cases
- Реализация конфигурационной модели
- Проведение тестирования ВС на основе модели нарушителя

Контактная информация

Десницкий Василий Алексеевич (СПИИРАН)
desnitsky@comsec.spb.ru
http://comsec.spb.ru/Desnitsky
Чечулин Андрей Алексеевич (СПИИРАН)
chechulin@comsec.spb.ru
http://comsec.spb.ru/Chechulin

Благодарности

Работа выполняется при финансовой поддержке РФФИ (проект 10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2) и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.