РусКрипто 2016

Выбор и комбинирование элементов для построения комплексной системы кибер-физической безопасности

Десницкий В.А., Левшун Д.С., Котенко И.В.

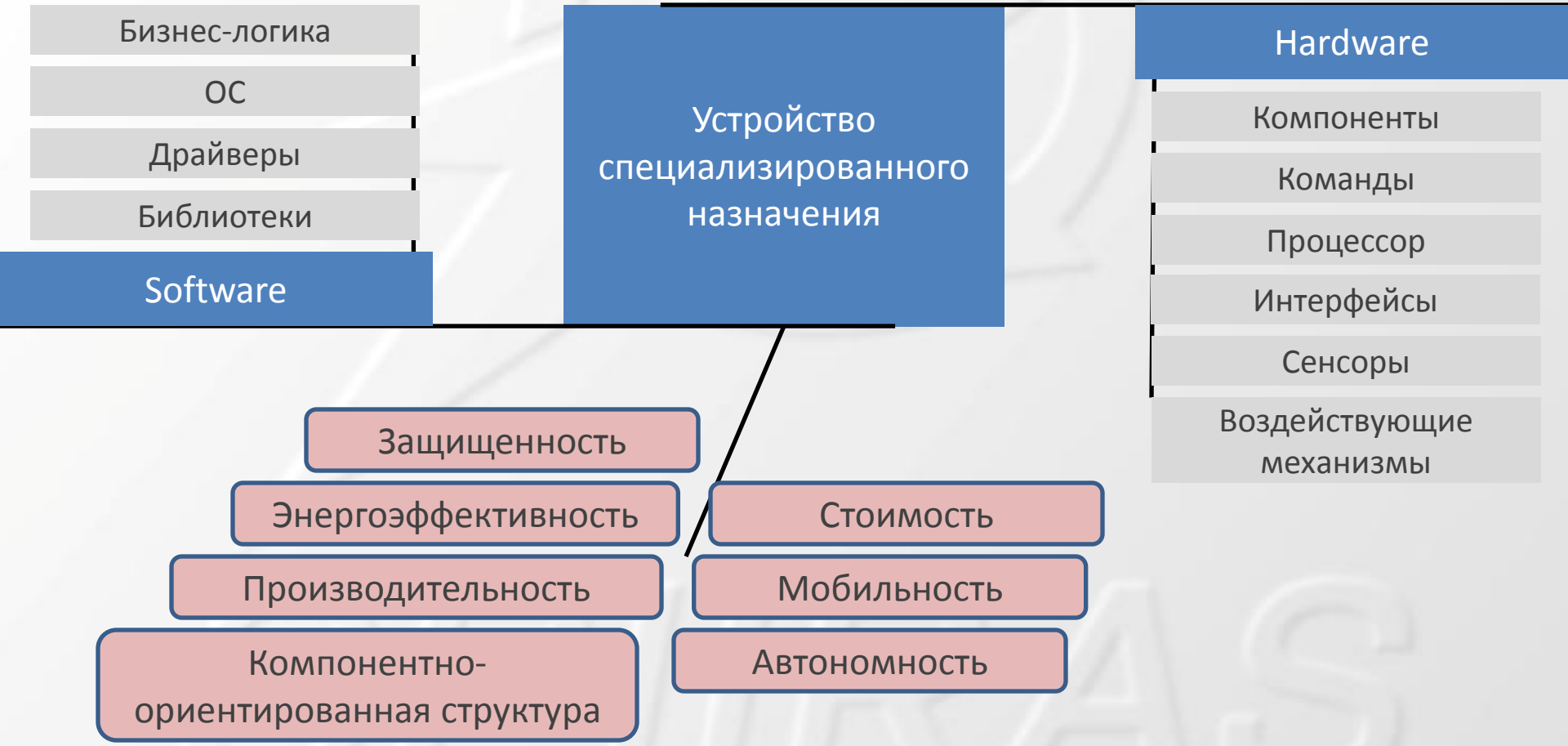
Санкт-Петербургский Институт Информатики и Автоматизации Российской Академии Наук (СПИИРАН)

Области применения

- **Высокая степень взаимодействия** между встроенными устройствами, с одной стороны, и элементами программно-аппаратного окружения и пользователями системы, с другой стороны

- **Критически важный характер** таких систем

Встроенные устройства (ВУ)



Методика проектирования защищенных ВУ

Спецификации

вход

Требования

Доступные компоненты

Бизнес-логика

Окружение

Проблемы защиты

Нарушители

Угрозы

Комбинирование встраиваемых компонентов на основе правил

выход

Конфигурация

comp1 comp2 comp3

SW/HW компоненты защиты

Выполнение функц. требований защиты

Проверка нефункц. ограничений

Дискретная оптимизация на множестве компонентов защиты

Стадии методики

№	стадия
1	Определение функциональных требований защиты
2	Идентификация альтернатив компонентов защиты
3	Определение численных нефункциональных ограничений
4	Получение значений нефункциональных показателей компонентов защиты
5	Получение критериев отбор компонентов защиты
6	Вычисление суммарных нефункциональных значений для конфигураций
7	Получение оптимальной конфигурации

Определение функциональных требований защиты (1/3)

Классификация нарушителя по типу доступа к ВУ (Rae'03)

- **$Type_0$** - no access (social engineering)
- **$Type_1$** - no direct access (TCP/IP)
- **$Type_2$** - remote access (Wi-Fi, IR, Bluetooth)
- **$Type_3$** - outward access (COM, USB)
- **$Type_4$** - full access (microchip)

Классификация нарушителя по уровню возможностей (Abraham'01)

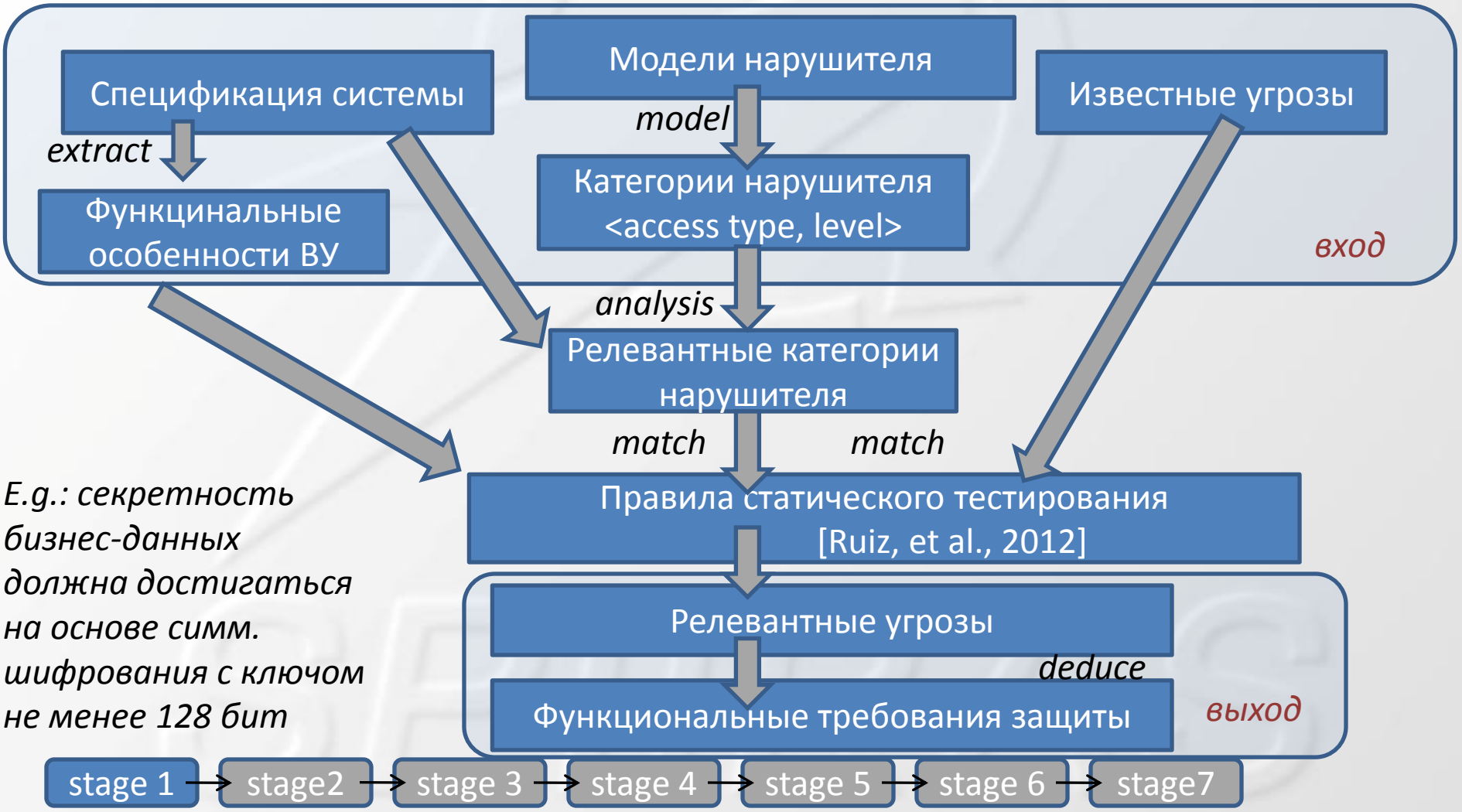
- **$Level_1$** - public accessed tools, well-known vulnerabilities
- **$Level_2$** - specialized tools, previously unknown vulnerabilities
- **$Level_3$** - group of intruders level 2

Категории нарушителя

(T_1, L_1)	(T_2, L_1)	(T_3, L_1)	(T_4, L_1)	(T_5, L_1)
(T_1, L_2)	(T_2, L_2)	(T_3, L_2)	(T_4, L_2)	(T_5, L_2)
(T_1, L_3)	(T_2, L_3)	(T_3, L_3)	(T_4, L_3)	(T_5, L_3)

stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

Определение функциональных требований защиты (2/3)



E.g.: секретность бизнес-данных должна достигаться на основе симм. шифрования с ключом не менее 128 бит

Определение функциональных требований защиты (3/3)

Правила статического тестирования

(funct_feature, intruder_cat) → threats

Примеры правил статического тестирования

If not(has_Internet_connection(device)) → no $Type_1$ Intruder

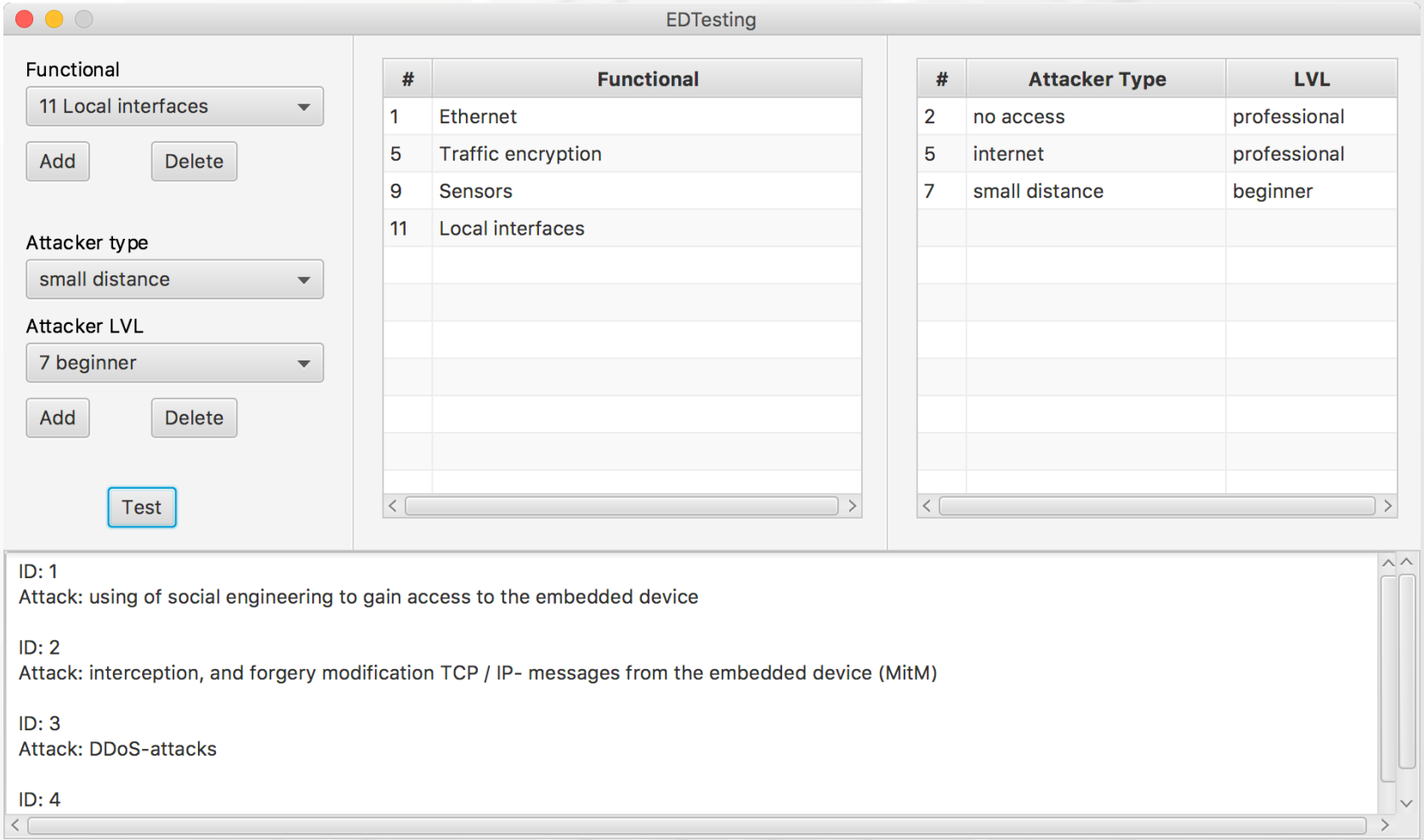
(functional_feature = "Traffic encryption") && ((~~type=1~~ & level=3) v
(type=2 & level=3) v (type=3 & level=3) v (type=4 & level=3)) →
threat = "cryptographic analysis of encrypted messages"

If low financial value of device data→ no $Level_3$ Intruders (no reason to protect against $Level_3$ Intruders)

If (comm_interface, $Level_1$ and $Level_2$ intruder only)→ “crypto analysis attack” is practically impossible

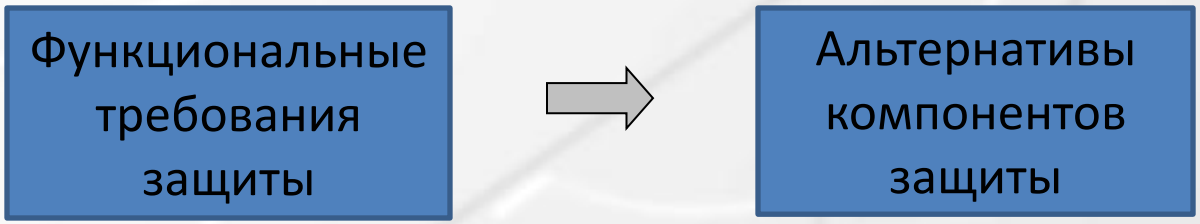
stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

Средство статического тестирования



stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

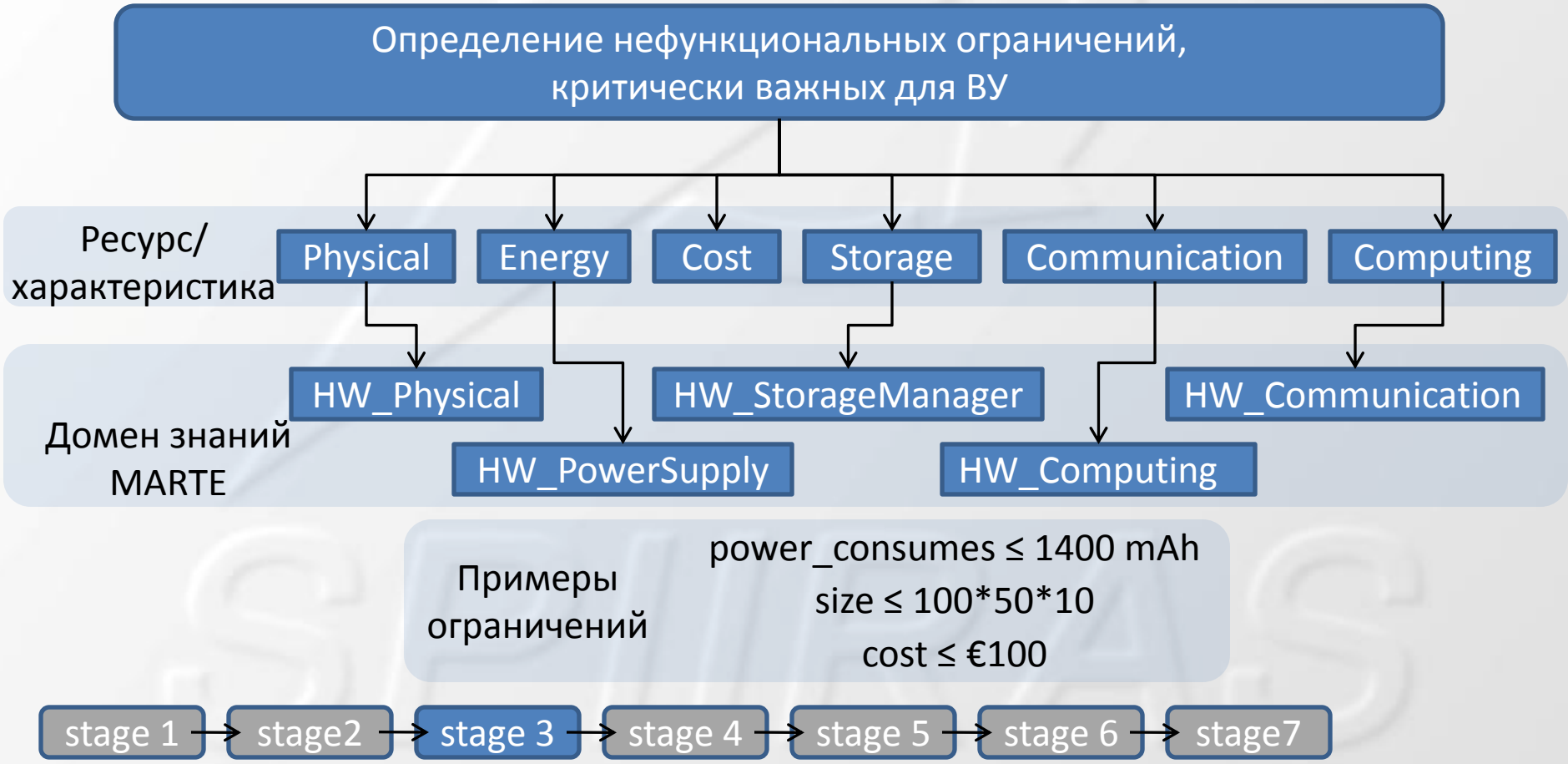
Идентификация альтернатив компонентов защиты



E.g.: “обеспечение секретности бизнес-данных на основе SW-средств защиты” →
“симметричное шифрование” AES/128/192/256, IDEA, … .

Определение численных нефункциональных ограничений

Использование MARTE
“UML profile for Modeling and Analysis of Real-Time and Embedded Systems” (OMG group)

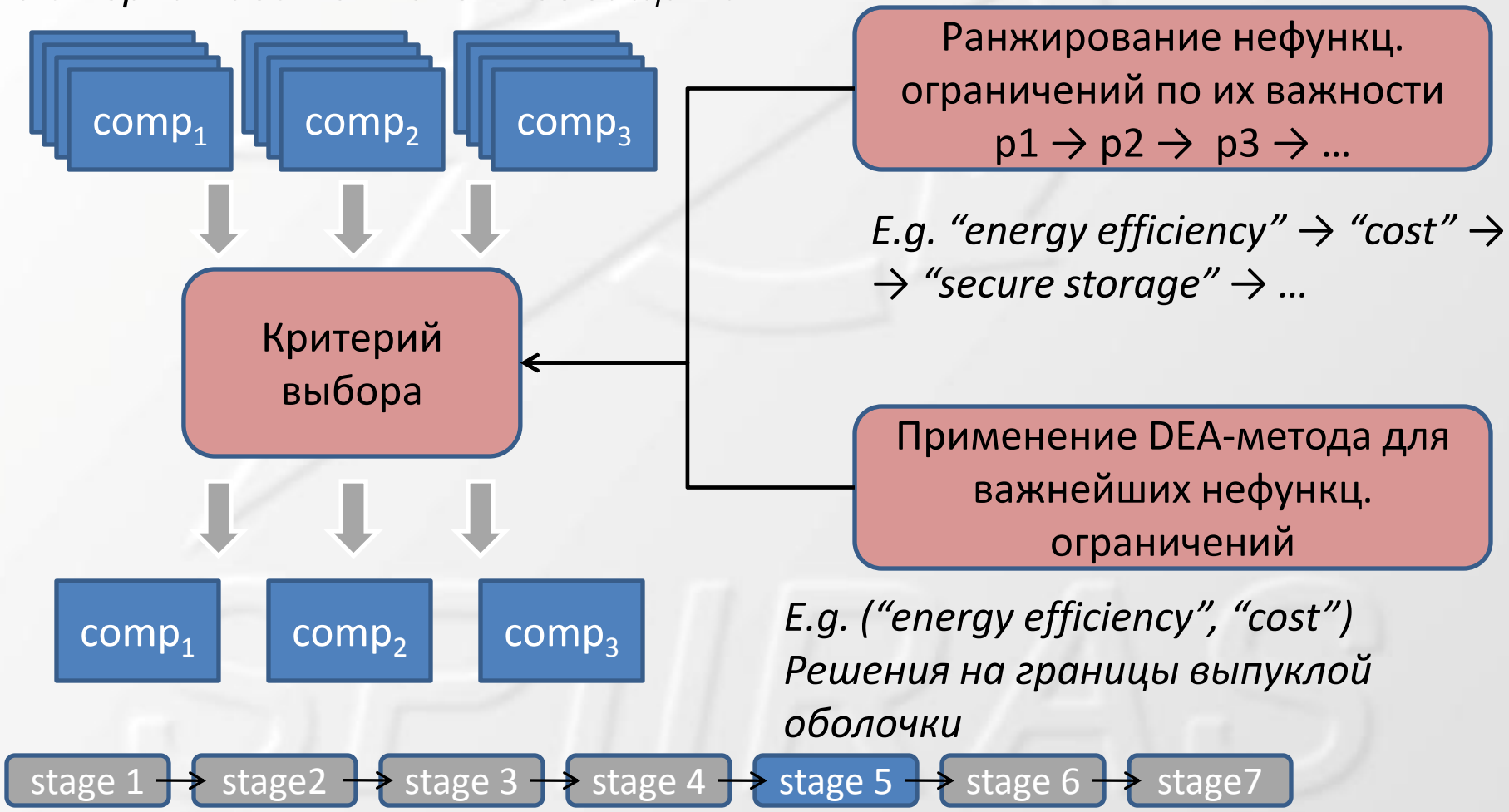


Получение значений нефункциональных показателей компонентов защиты

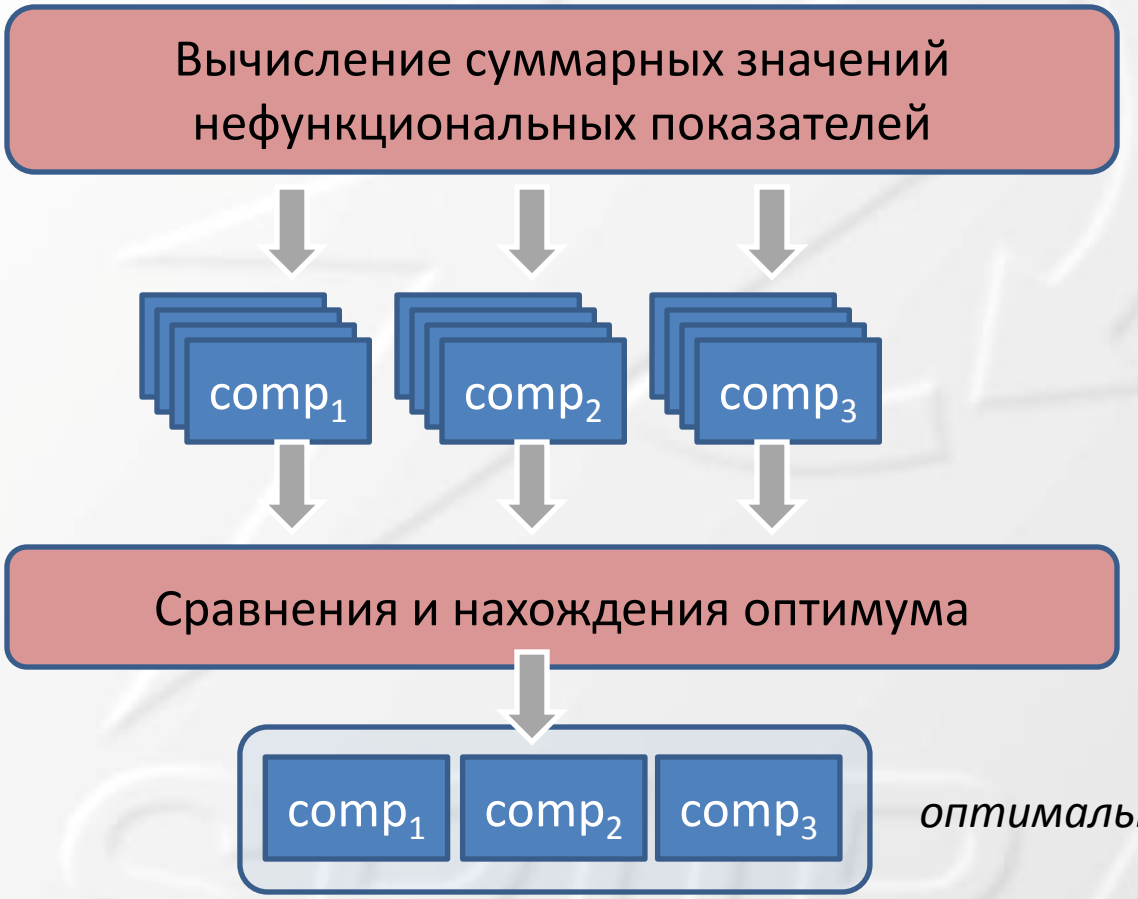
stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

Получение критериев отбор компонентов защиты

Альтернативы компонентов защиты

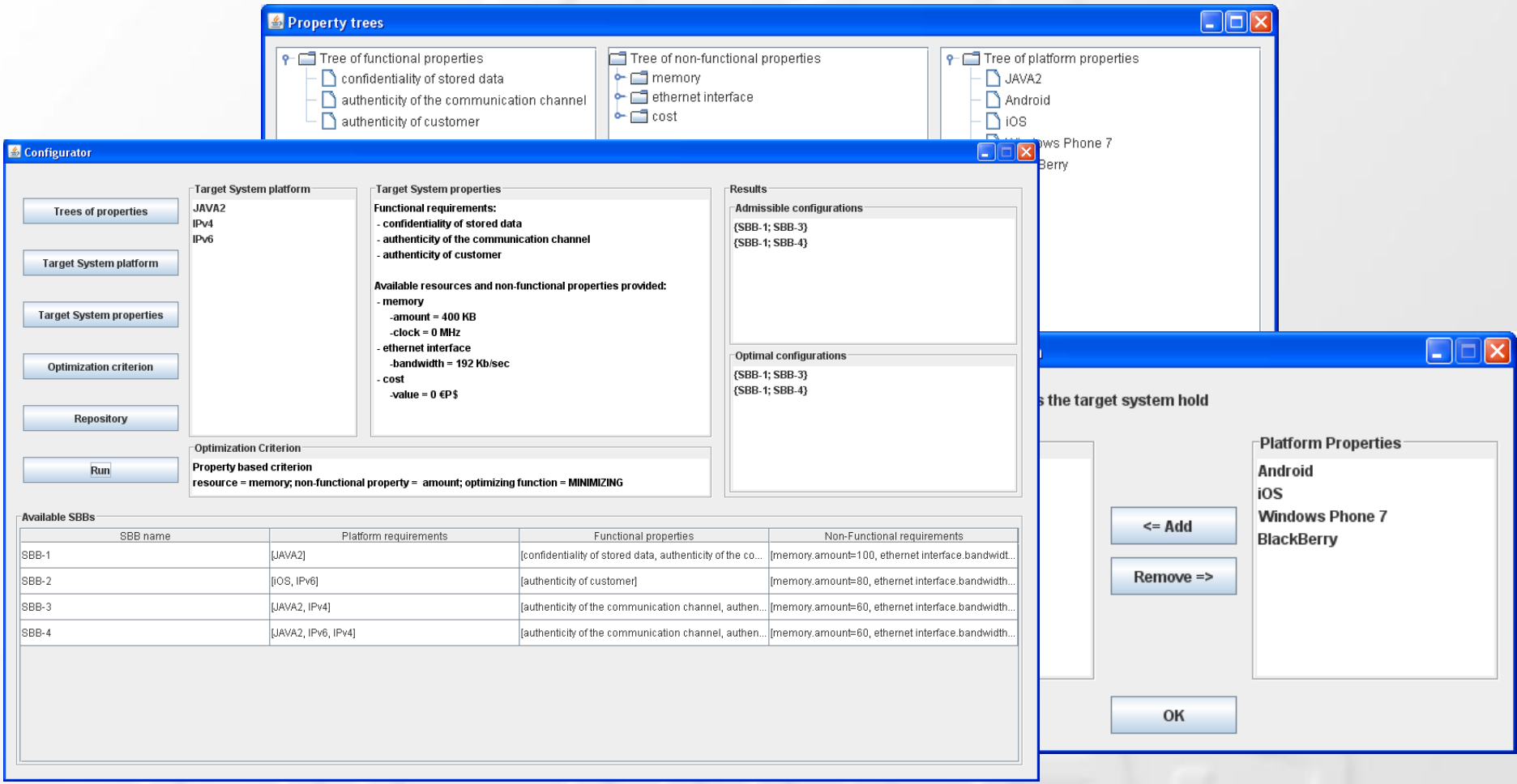


Выбор оптимального набора компонентов защиты (1/2)



stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

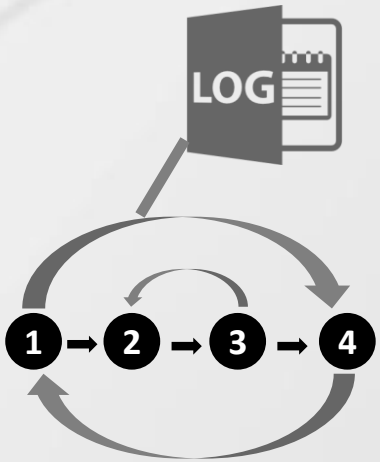
Выбор оптимального набора компонентов защиты (2/2)



stage 1 → stage2 → stage 3 → stage 4 → stage 5 → stage 6 → stage7

Proof-of-the-concept

- Разработка системы комплексной безопасности в части контроля периметра - система контроля периметра (СКП)
- Контроль доступа на основе ролей
  - Физический доступ в помещение
  - Доступ к ученой записи ПК



1. **entrance** to the room
2. **start** OS session
3. **start and** OS session
4. **exit** from the room

Состояния пользователя	
S1	вошел в помещение
S2	Вошел в учетную запись ПК (начало сеанса работы с ОС)
S3	завершил сеанс работы с ОС
S4	покинул помещение

Методика проектирования защищенных ВУ

функциональные требования

hardware

HTTP HTTPS SOAP

software

- Формирование **функциональных требований** и выбор необходимых SW/HW компонентов.

альтернативы

Arduino Yun, micro SD

Beaglebone Black, Wi-Fi adapter

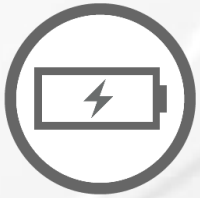
Raspberry Pi B+, Wi-Pi module

Intel Galileo, Wi-Fi Kit

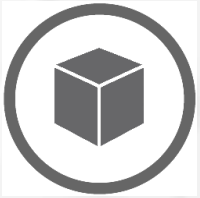
Альтернативы

нефункциональные требования

стоимость



энергоэффективность



занимаемое пространство

- Формирование **нефункциональных требований** и выбор **оптимальных** SW/HW компонентов

Альтернативы

Arduino Yun, micro SD

Beaglebone Black, Wi-Fi adapter

Raspberry Pi B+, Wi-Pi module

Intel Galileo, Wi-Fi Kit

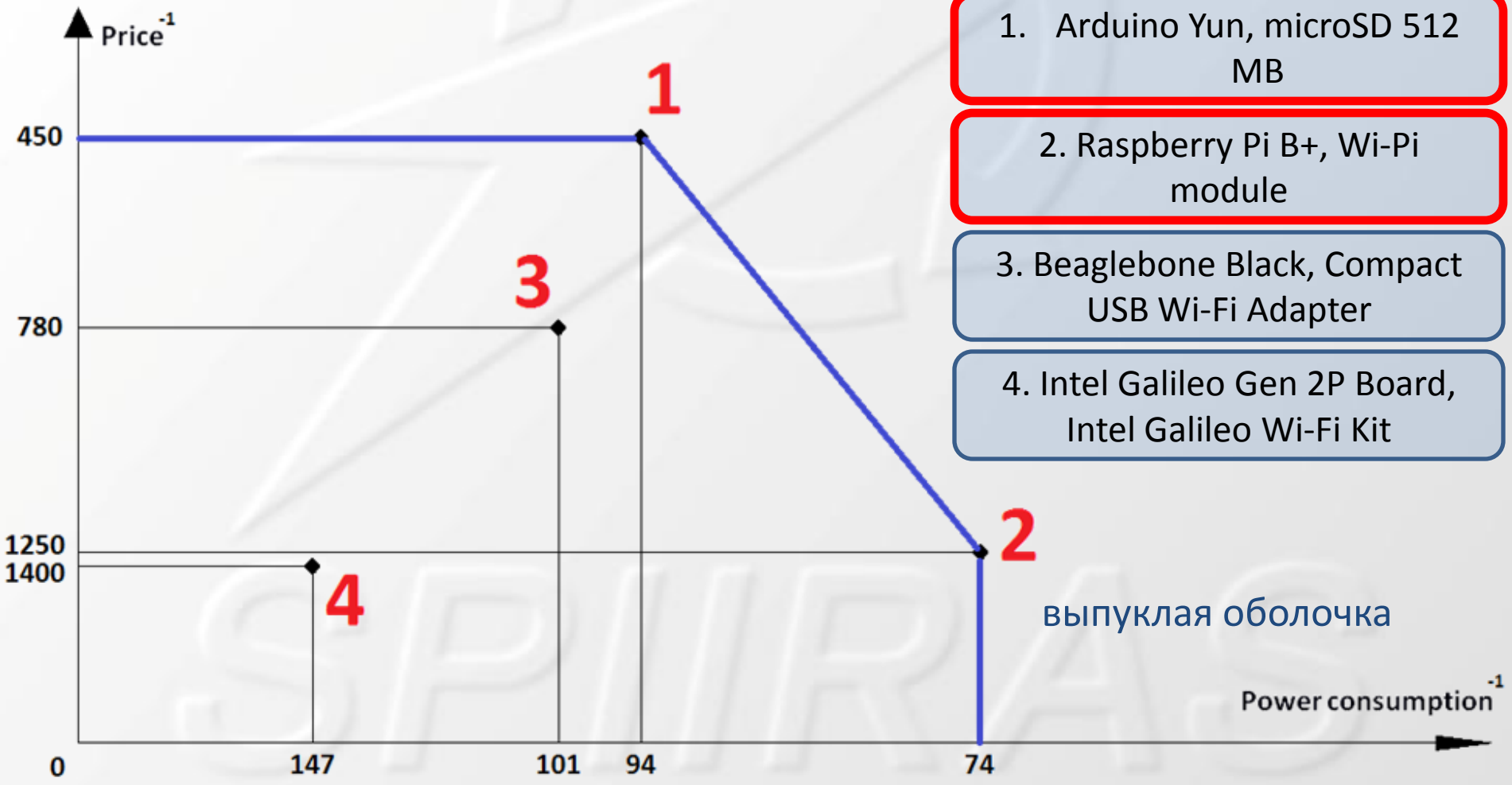
Суммарные значения нефункциональных показателей

Компоненты защиты	Энергопотреболение (mAh)	Цена (€)	Размеры (mm)
Arduino Yun, microSD 512 MB	450	94	73*53*8
Raspberry Pi B+, Wi-Pi module	1250	74	60*36*7
Beaglebone Black, Compact USB Wi-Fi Adapter	780	101	86*53*7
Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit	1400	147	123*72*9

Применения критерия выбора на основе DEA-метода

Альтернативы

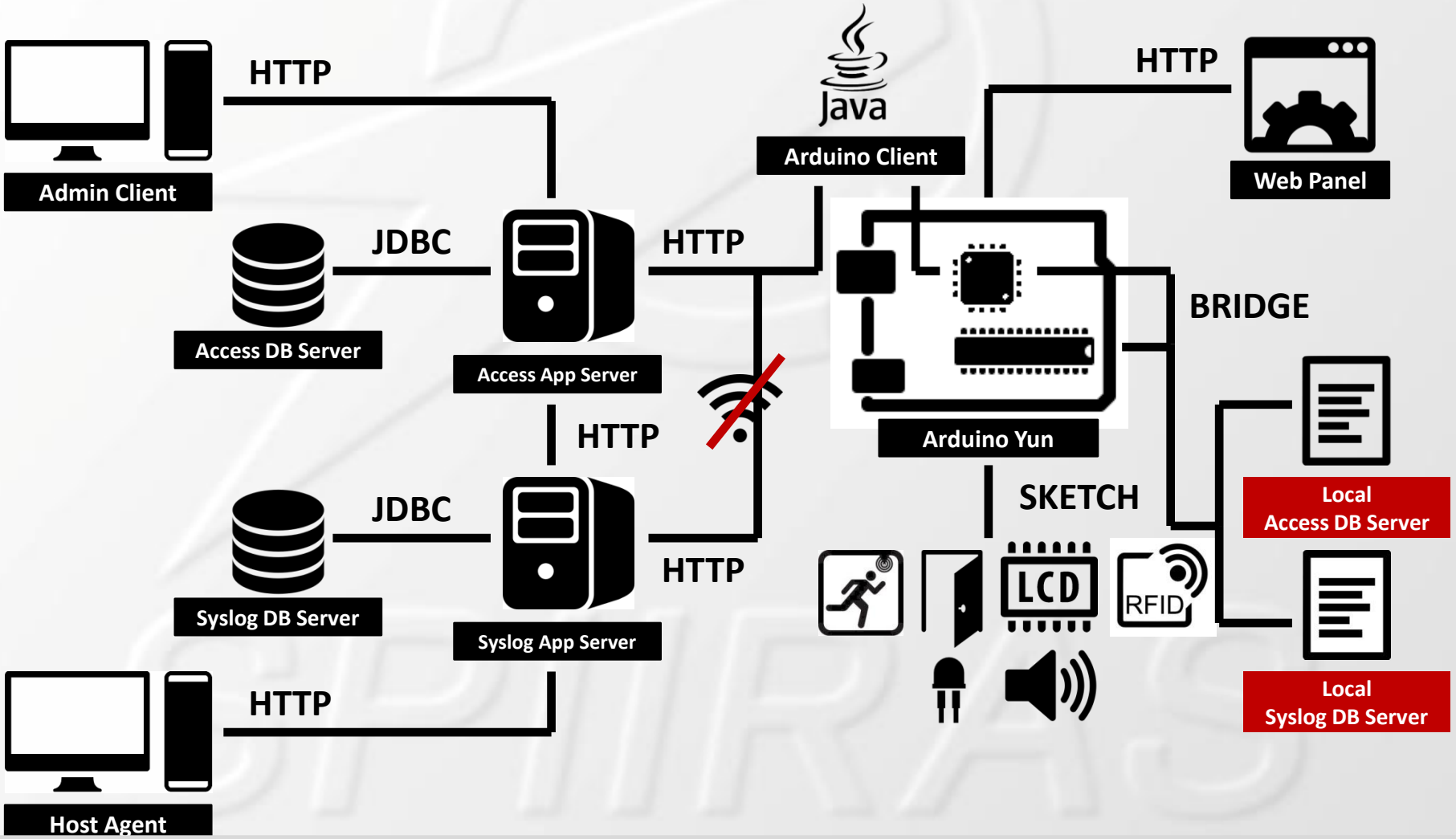
1. Arduino Yun, microSD 512 MB
2. Raspberry Pi B+, Wi-Pi module
3. Beaglebone Black, Compact USB Wi-Fi Adapter
4. Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit



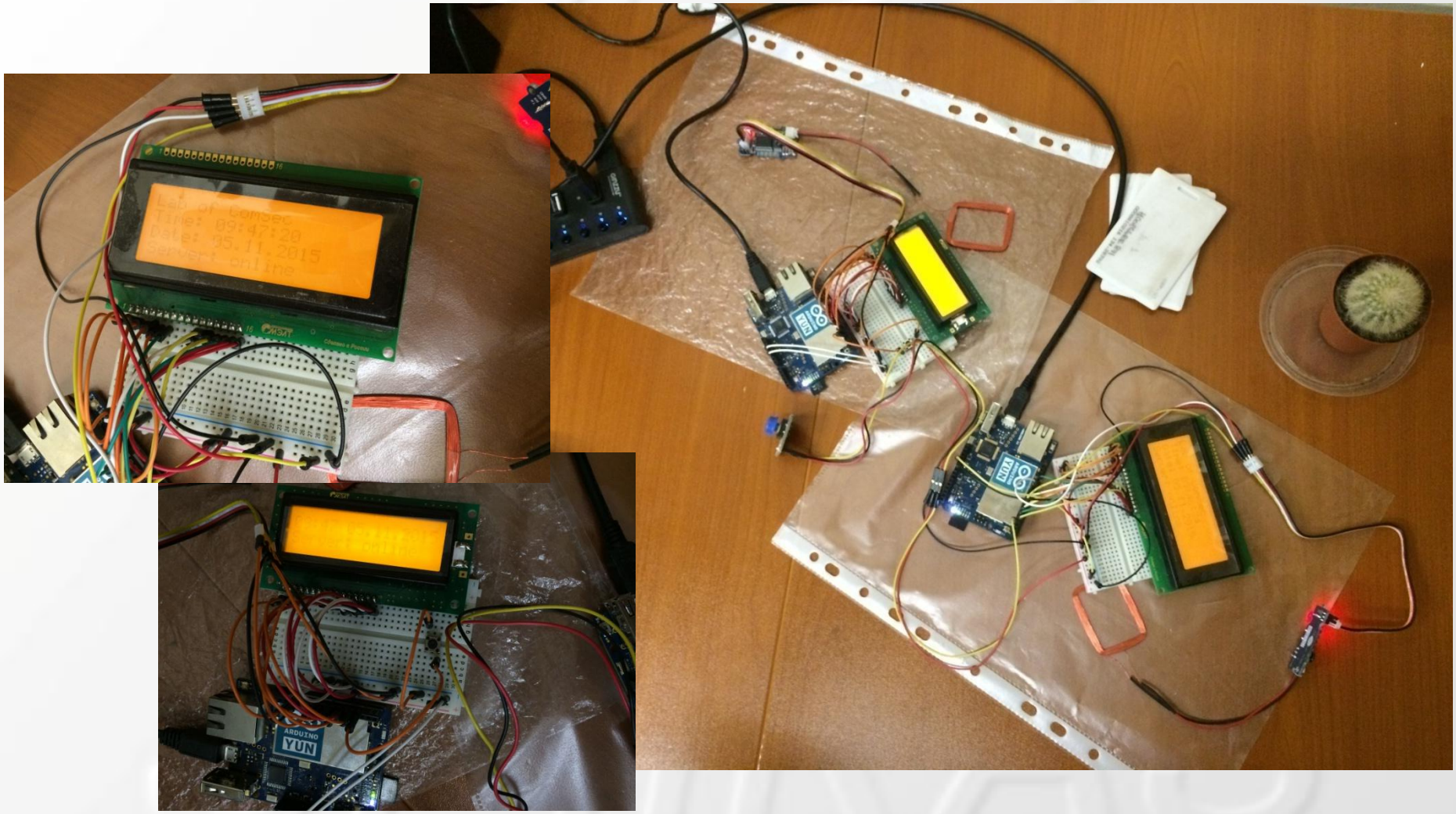
выпуклая оболочка

Архитектура СКП

Аварийный режим



Прототип СКП



Заключение

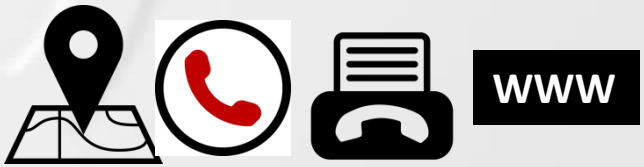
Основной вклад

- Методика проектирования защищенных ВУ
  - регламентирует действия разработчика защищенного ВУ
  - Автоматизирует (1) определение угроз и (2) комбинирование компонентов защиты с использованием двух разработанных программных средств принятия решений
- Прототип системы комплексной безопасности в части подсистемы контроля периметра (proof-of-the-concept)

Контактная информация

Лаборатория проблем компьютерной безопасности
СПИИРАН

- http://comsec.spb.ru
- desnitsky@comsec.spb.ru



Благодарности

- Работа выполнена в СПИИРАН при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029.