

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)

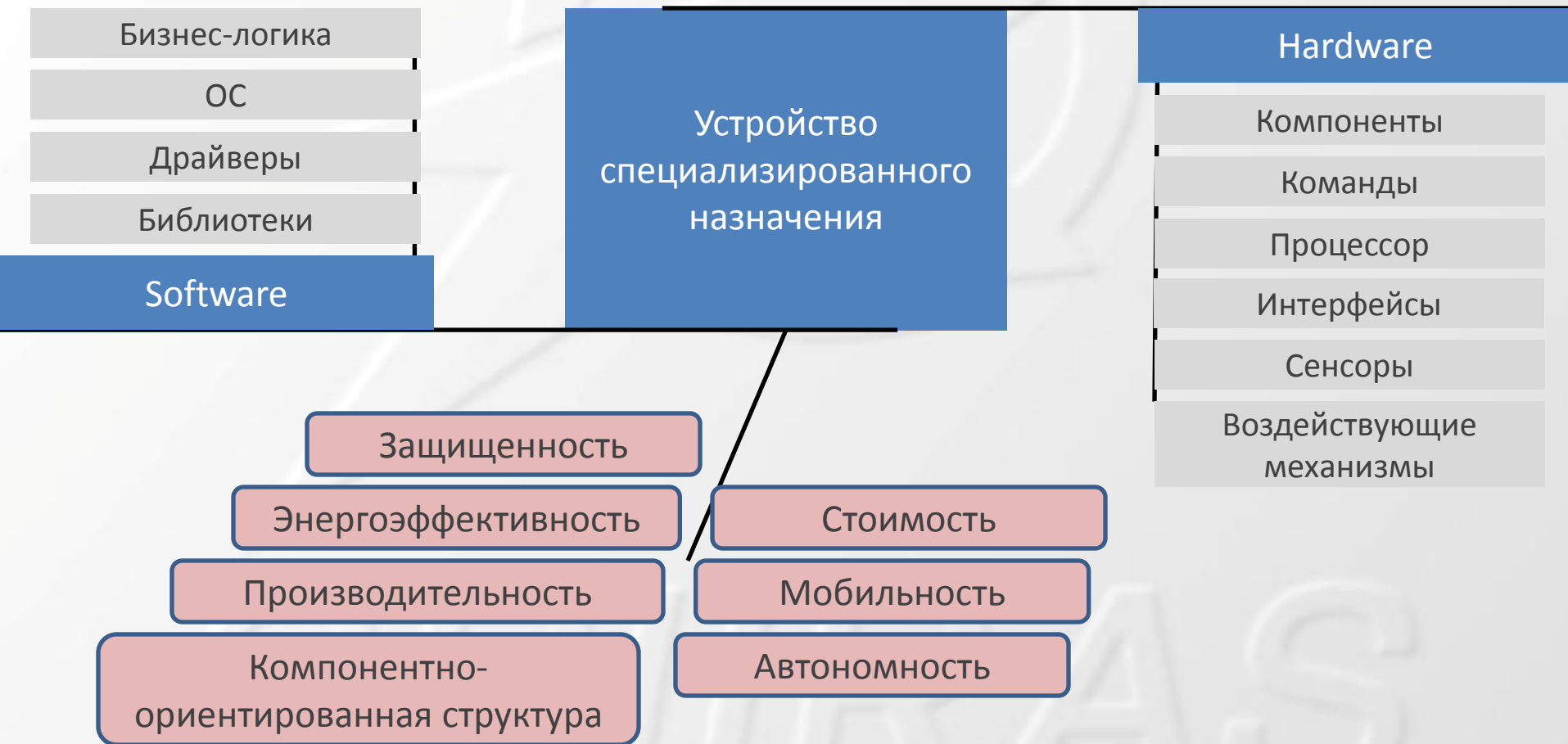
Области применения

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

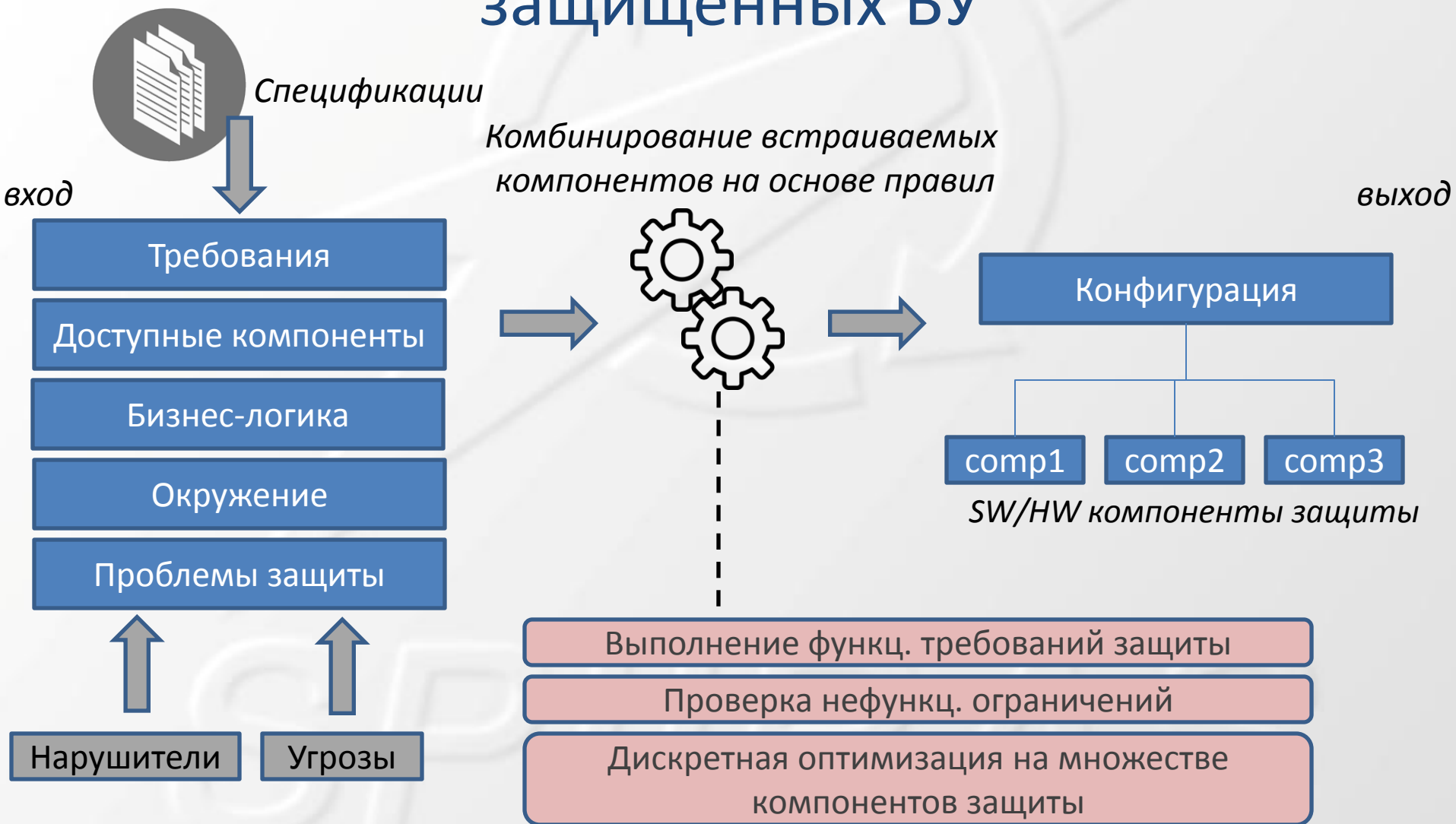


- **Критически важный характер** таких систем

Встроенные устройства (ВУ)



Методика проектирования защищенных ВУ



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)

Type₀ - no access (social engineering)

Type₁ - no direct access (TCP/IP)

Type₂ - remote access (Wi-Fi, IR, Bluetooth)

Type₃ - outward access (COM, USB)

Type₄ - full access (microchip)

Классификация нарушителя по уровню возможностей (Abraham'01)

Level₁ - public accessed tools, well-known vulnerabilities

Level₂ - specialized tools, previously unknown vulnerabilities

Level₃ - 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

stage 2

stage 3

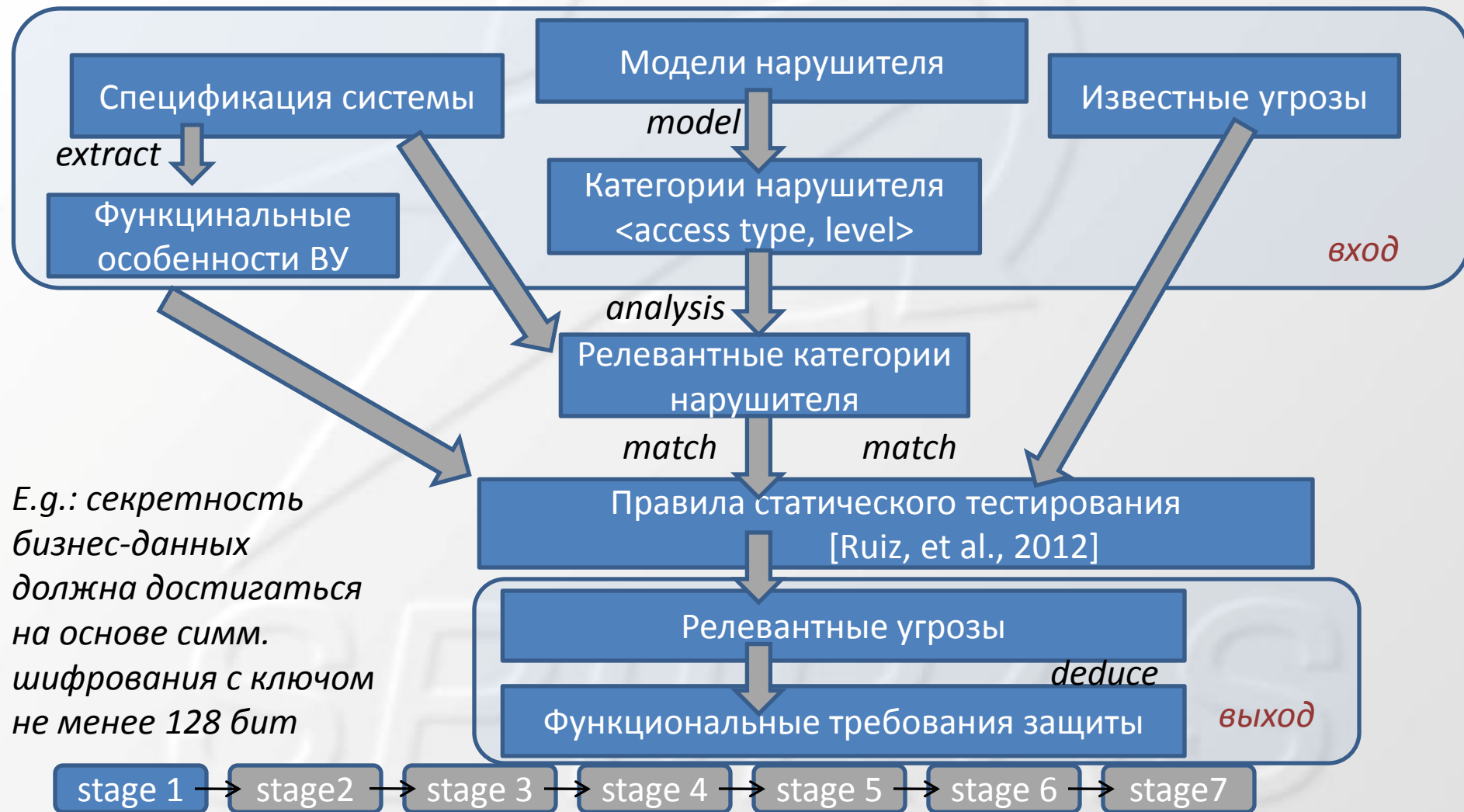
stage 4

stage 5

stage 6

stage 7

Определение функциональных требований защиты (2/3)



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 Type₁ 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 Level₃ Intruders (no reason to protect against Level₃ Intruders)

If (comm_interface, Level₁ and Level₂ intruder only) → "crypto analysis attack" is practically impossible

stage 1 → stage 2 → stage 3 → stage 4 → stage 5 → stage 6 → stage 7

Средство статического тестирования

EDTesting

Functional

11 Local interfaces

Add Delete

Attacker type

small distance

Attacker LVL

7 beginner

Add Delete

Test

#	Functional
1	Ethernet
5	Traffic encryption
9	Sensors
11	Local interfaces

#	Attacker Type	LVL
2	no access	professional
5	internet	professional
7	small distance	beginner

ID: 1
Attack: using of social engineering to gain access to the embedded device

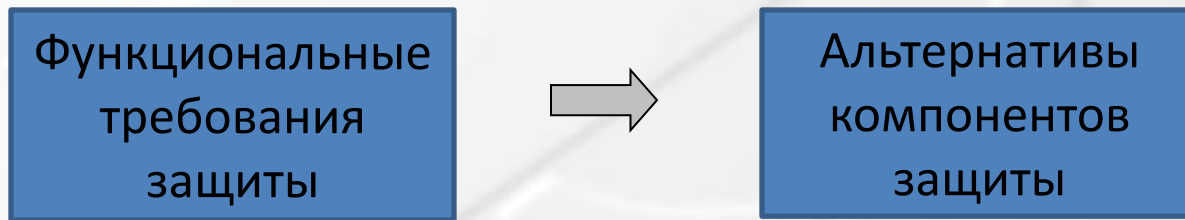
ID: 2
Attack: interception, and forgery modification TCP / IP- messages from the embedded device (MitM)

ID: 3
Attack: DDoS-attacks

ID: 4



Идентификация альтернатив компонентов защиты



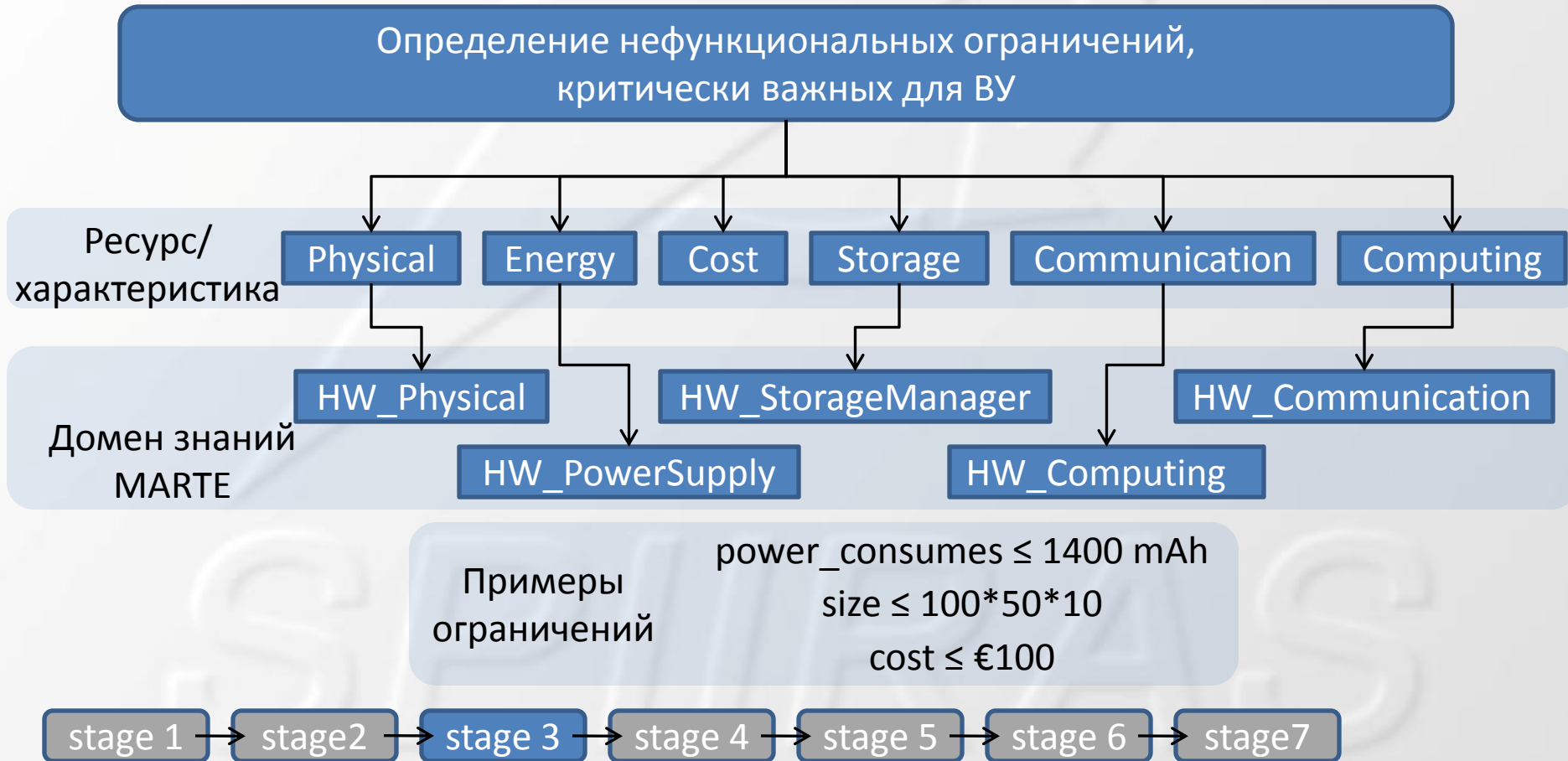
E.g.: “обеспечение секретности бизнес-данных на основе SW-средств защиты” → “симметричное шифрование” AES/128/192/256, IDEA, ...



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

Оценка нефункциональных показателей для
компонентов защиты

Сбор данных от
разработчиков
SW/HW модулей

Эмпирически –
путем
моделирования
компонентов
защиты (когда это
возможно)

Аналитически, на
основе опыта
работы со
сходными
компонентами

stage 1

stage 2

stage 3

stage 4

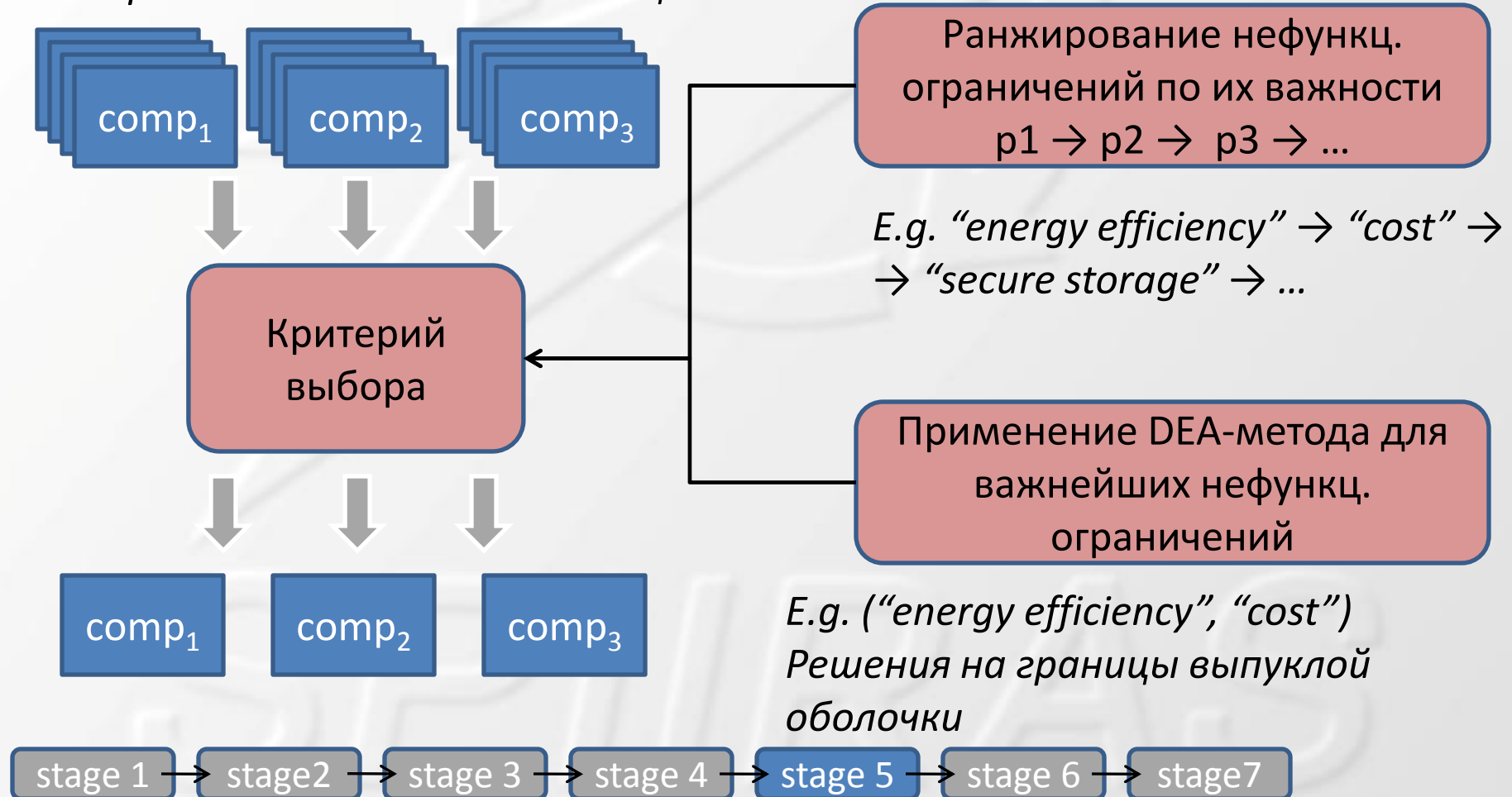
stage 5

stage 6

stage 7

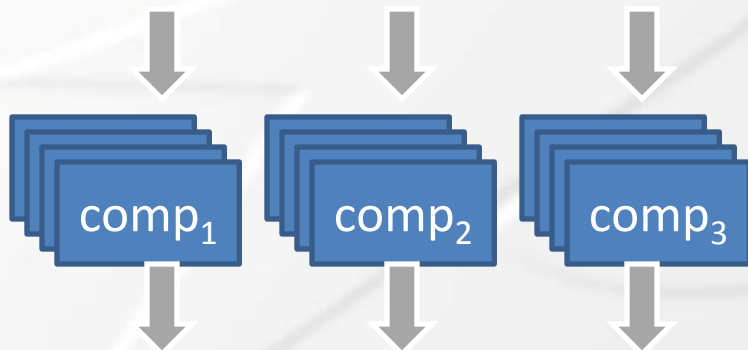
Получение критериев отбор КОМПОНЕНТОВ ЗАЩИТЫ

Альтернативы компонентов защиты



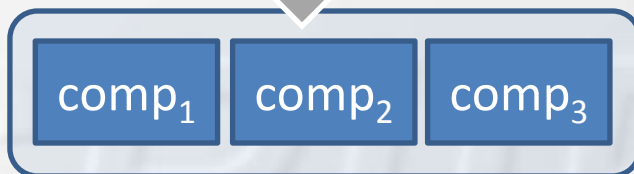
Выбор оптимального набора компонентов защиты (1/2)

Вычисление суммарных значений
нефункциональных показателей



Сравнения и нахождения оптимума

дискретная оптимизация



оптимальное решение



Выбор оптимального набора компонентов защиты (2/2)

The image shows a software configurator interface with several windows. The main window, titled 'Configurator', displays the following information:

- Trees of properties:** Three trees are visible: 'Tree of functional properties' (containing confidentiality of stored data, authenticity of the communication channel, authenticity of customer), 'Tree of non-functional properties' (containing memory, ethernet interface, cost), and 'Tree of platform properties' (containing JAVA2, Android, iOS).
- Target System platform:** JAVA2, IPV4, IPV6.
- Target System properties:**
 - Functional requirements:** confidentiality of stored data, authenticity of the communication channel, authenticity of customer.
 - Available resources and non-functional properties provided:** memory (amount = 400 KB, clock = 0 MHz), ethernet interface (bandwidth = 192 Kb/sec), cost (value = 0 €\$).
- Results:**
 - Admissible configurations:** {SBB-1; SBB-3}, {SBB-1; SBB-4}.
 - Optimal configurations:** {SBB-1; SBB-3}, {SBB-1; SBB-4}.
- Optimization Criterion:** Property based criterion, resource = memory; non-functional property = amount; optimizing function = MINIMIZING.
- Available SBBs:** A table with 4 rows and 4 columns.

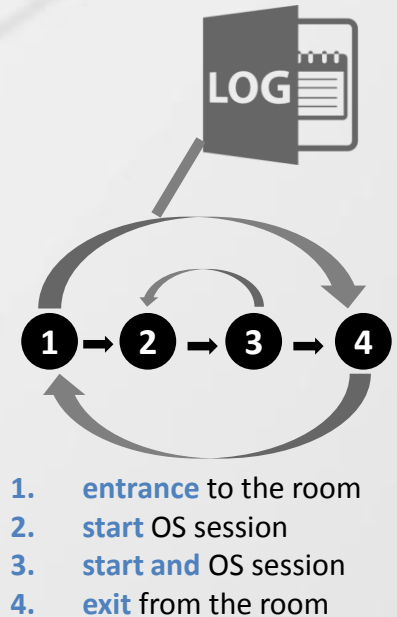
SBB name	Platform requirements	Functional properties	Non-Functional requirements
SBB-1	{JAVA2}	{confidentiality of stored data, authenticity of the co...	{memory.amount=100, ethernet interface.bandwidth...
SBB-2	{iOS, IPV6}	{authenticity of customer}	{memory.amount=80, ethernet interface.bandwidth...
SBB-3	{JAVA2, IPV4}	{authenticity of the communication channel, authen...	{memory.amount=60, ethernet interface.bandwidth...
SBB-4	{JAVA2, IPV6, IPV4}	{authenticity of the communication channel, authen...	{memory.amount=60, ethernet interface.bandwidth...

A secondary window titled 'Platform Properties' shows a list of selected properties: Android, iOS, Windows Phone 7, BlackBerry. It includes buttons for '<= Add', 'Remove =>', and 'OK'.



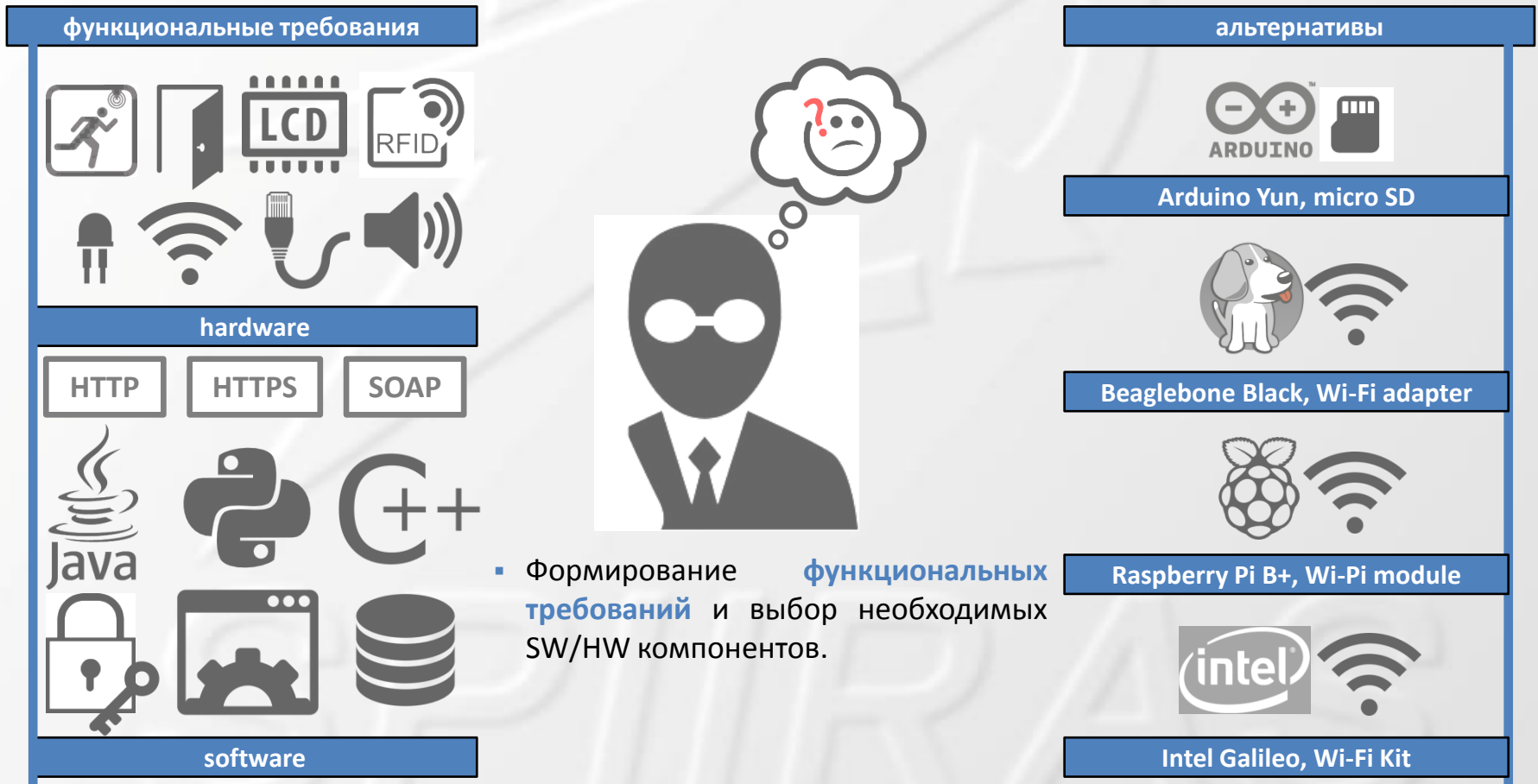
Proof-of-the-concept

- 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



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

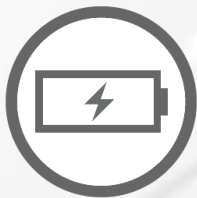


Альтернативы

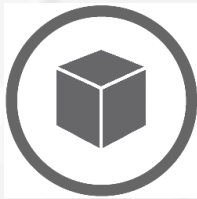
нефункциональные требования



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



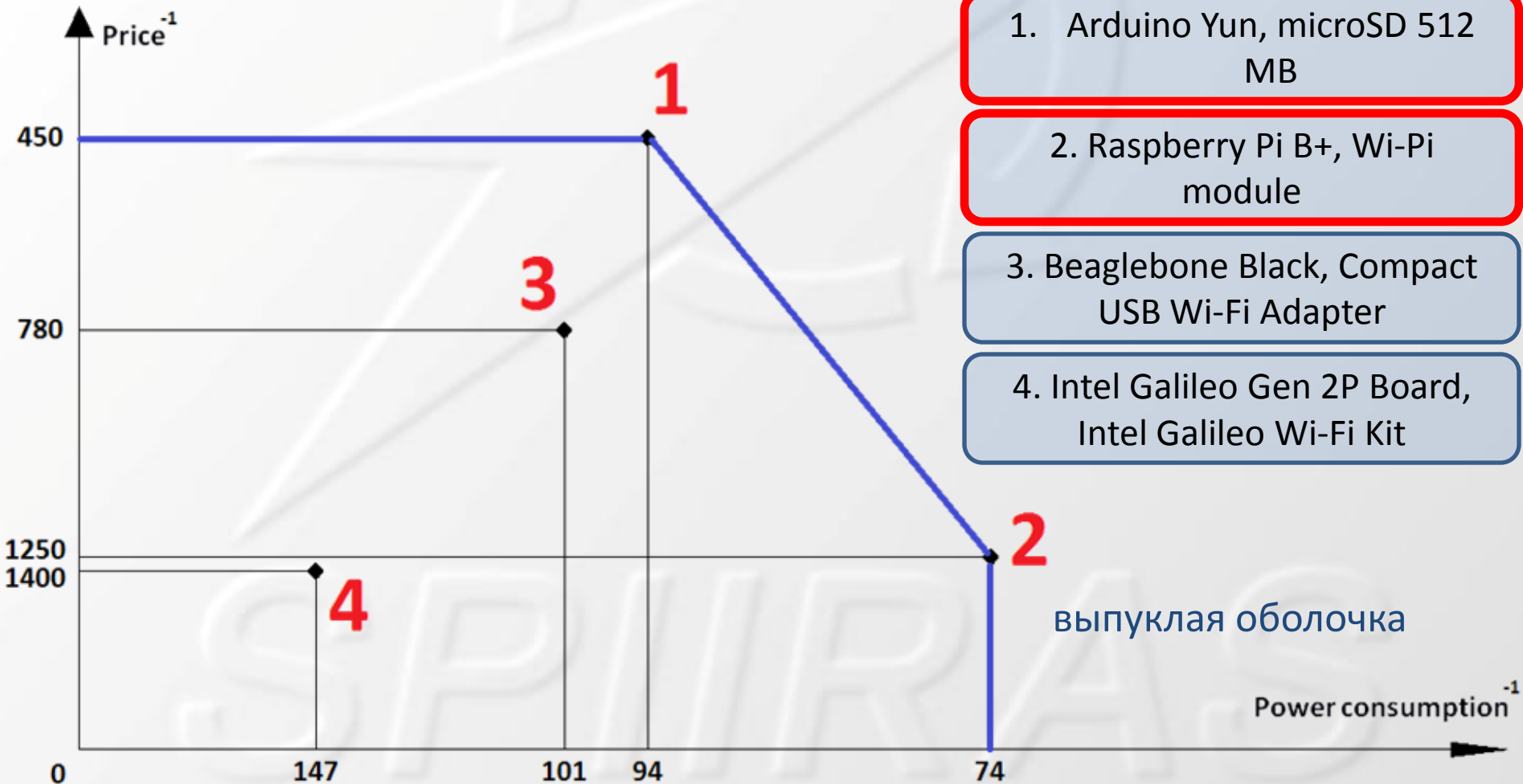
Intel Galileo, Wi-Fi Kit

Суммарные значения нефункциональных показателей

Компоненты защиты	Энергопотребление (mAh)	Цена (€)	Размеры (mm)
Arduino Yun, microSD 512 MB	450	94	73*53*8
Raspberry Pi B+, Wi-Fi 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

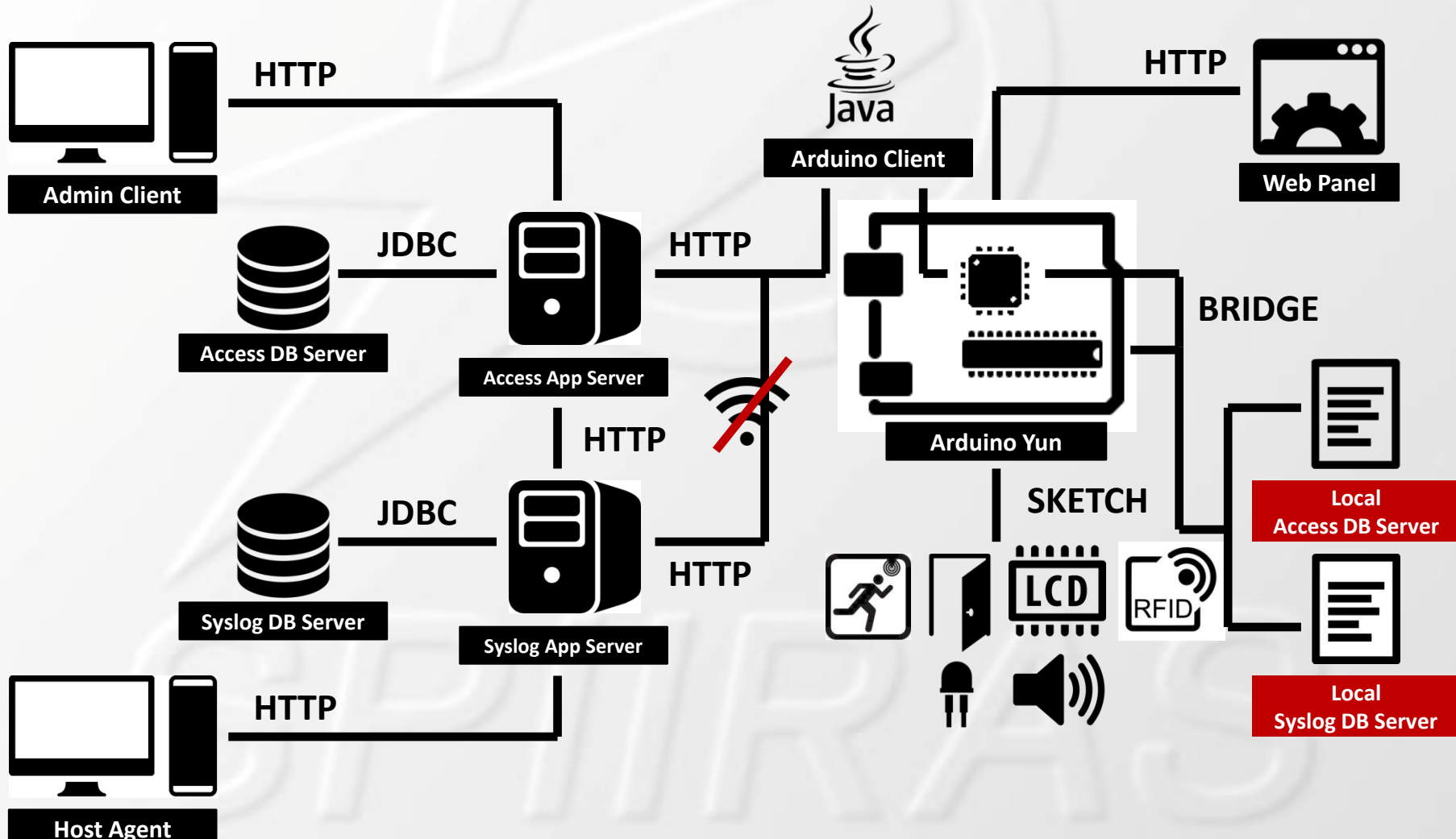
Применения критерия выбора на основе DEA-метода

Альтернативы

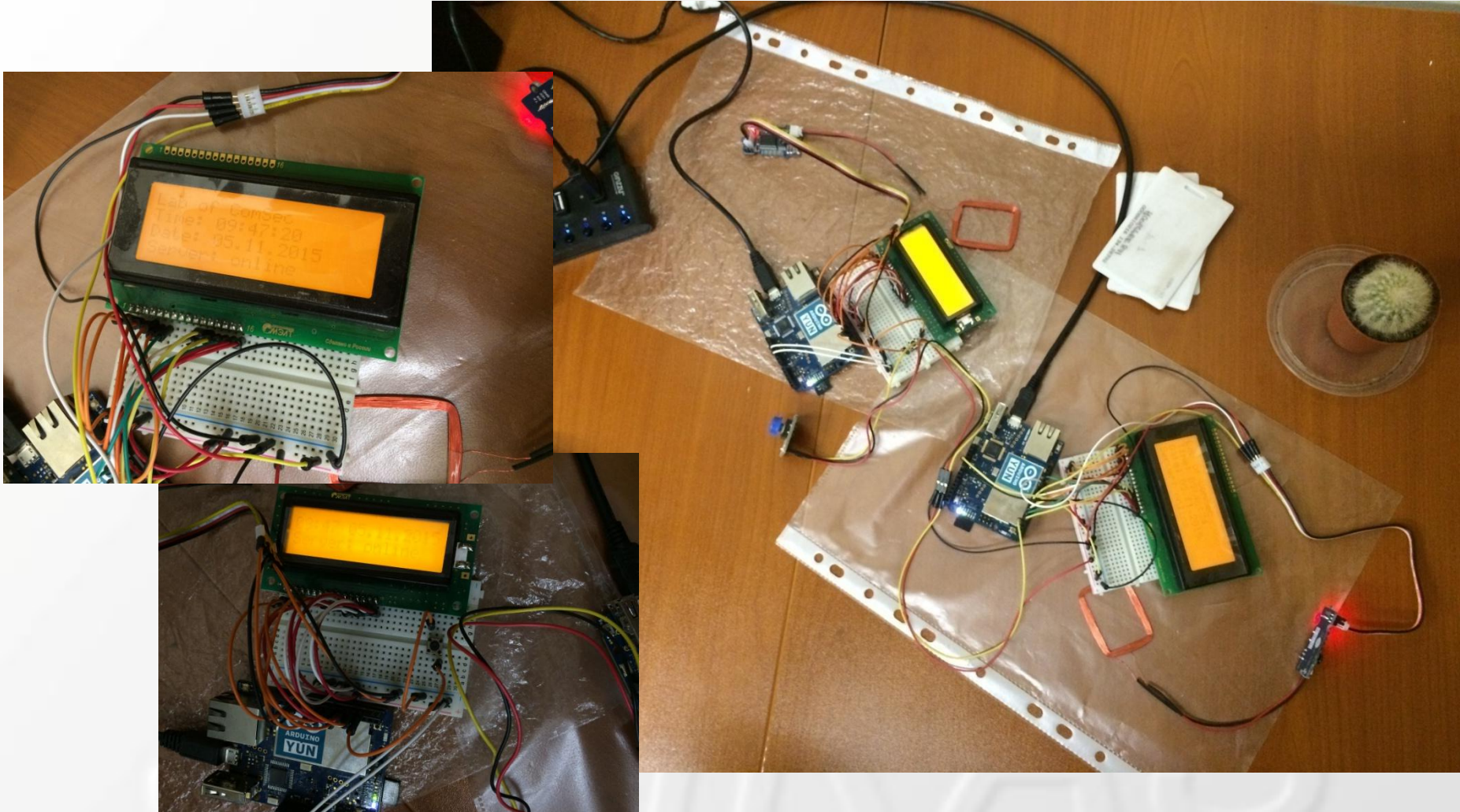


Архитектура СКП

Аварийный режим



Прототип СКП



РусКрипто 2016, 24 марта 2016 г.

Заключение

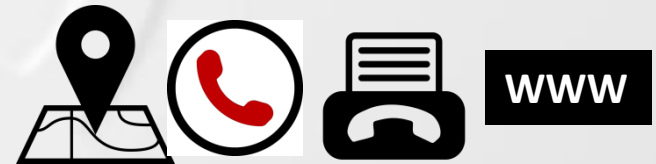
Основной вклад

- 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.

