ПРОЕКТИРОВАНИЕ И ВЕРИФИКАЦИЯ МЕХАНИЗМОВ ЗАЩИТЫ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ НА ОСНОВЕ ЭКСПЕРТНЫХ ЗНАНИЙ

Десницкий В.А.

Лаборатория проблем компьютерной безопасности,
СПИИРАН,
Санкт-Петербург, Россия

РусКрипто'2014, 27 марта 2014 г.

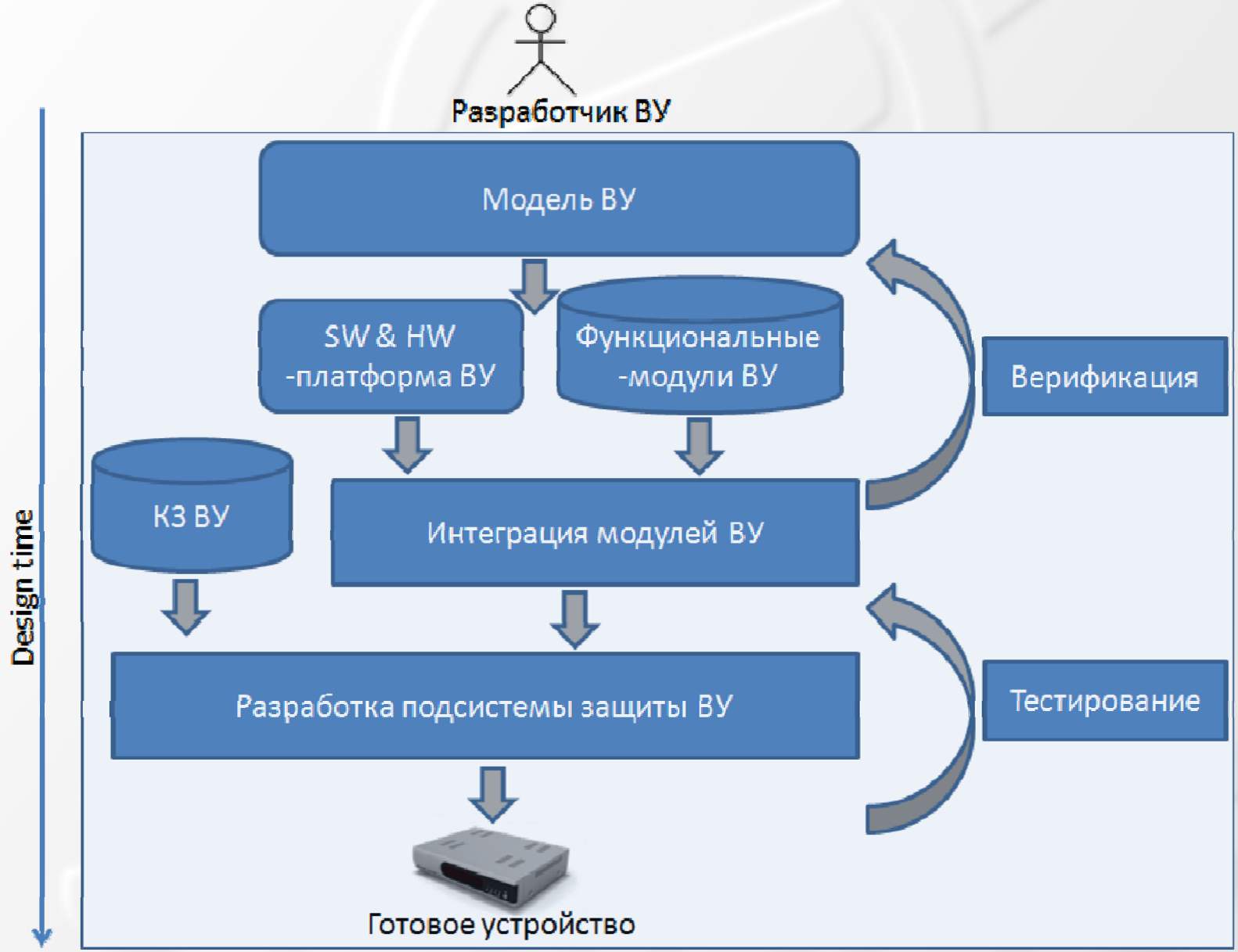
Встроенные устройства (ВУ)

- Автомобили
  - Контроль двигателя, АКП, АБС и др.
- Авиация
  - Управление полетом, системы диспетчерского контроля и др.
- Связь
  - Коммутация, цифровые ресиверы, мобильные телефоны, маршрутизаторы, IP телефония, КПК и др.
- Бытовая техника
  - Телевизоры, холодильники, СВЧ печи и др.
- Коммерческая техника
  - Автоматизированный контроль, кассовые аппараты, системы управления запасами и др.

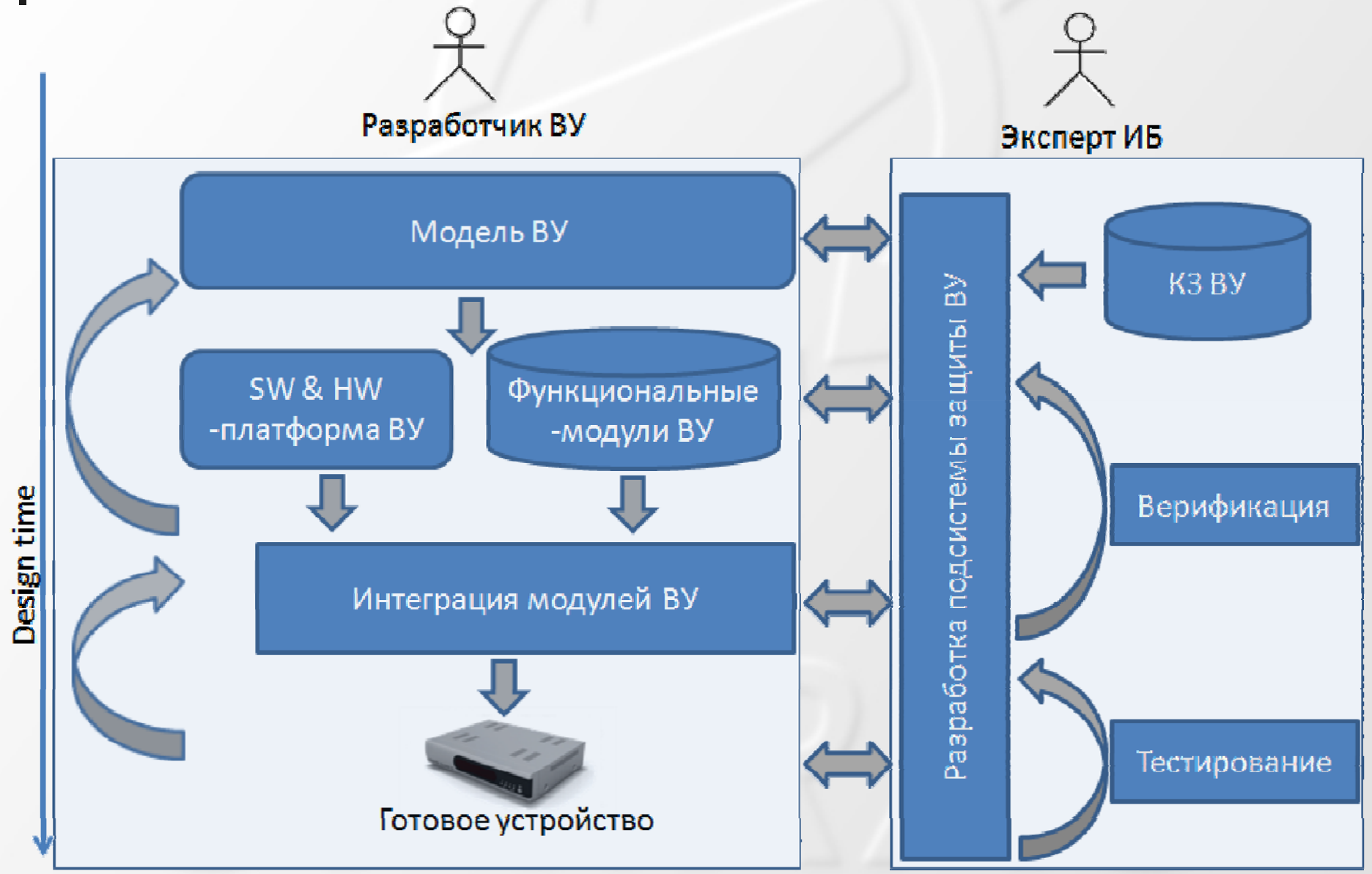
Проектирования систем с ВУ

- Специализированное назначение ВУ
- Особенности ВУ
  - Специфичные угрозы ИБ
  - Ресурсопотребление → производительность → функциональность
  - Автономность → энергопотребление & степень встраиваемости в систему верхнего уровня
  - Мобильность
  - Физические характеристики
  - Компонентно-ориентированная структура ВУ → внутр. связи
  - Стоимостные ограничения
- Сложность проектирования:
  - Анализ и учет ограничений ВУ
  - Слабая формализация и структуризация области знаний ИБ ВУ

Процесс проектирования ВУ (1/4)



Процесс проектирования ВУ (2/4)



Процесс проектирования ВУ (3/4)

- *Роль эксперта в обл. ИБ:*

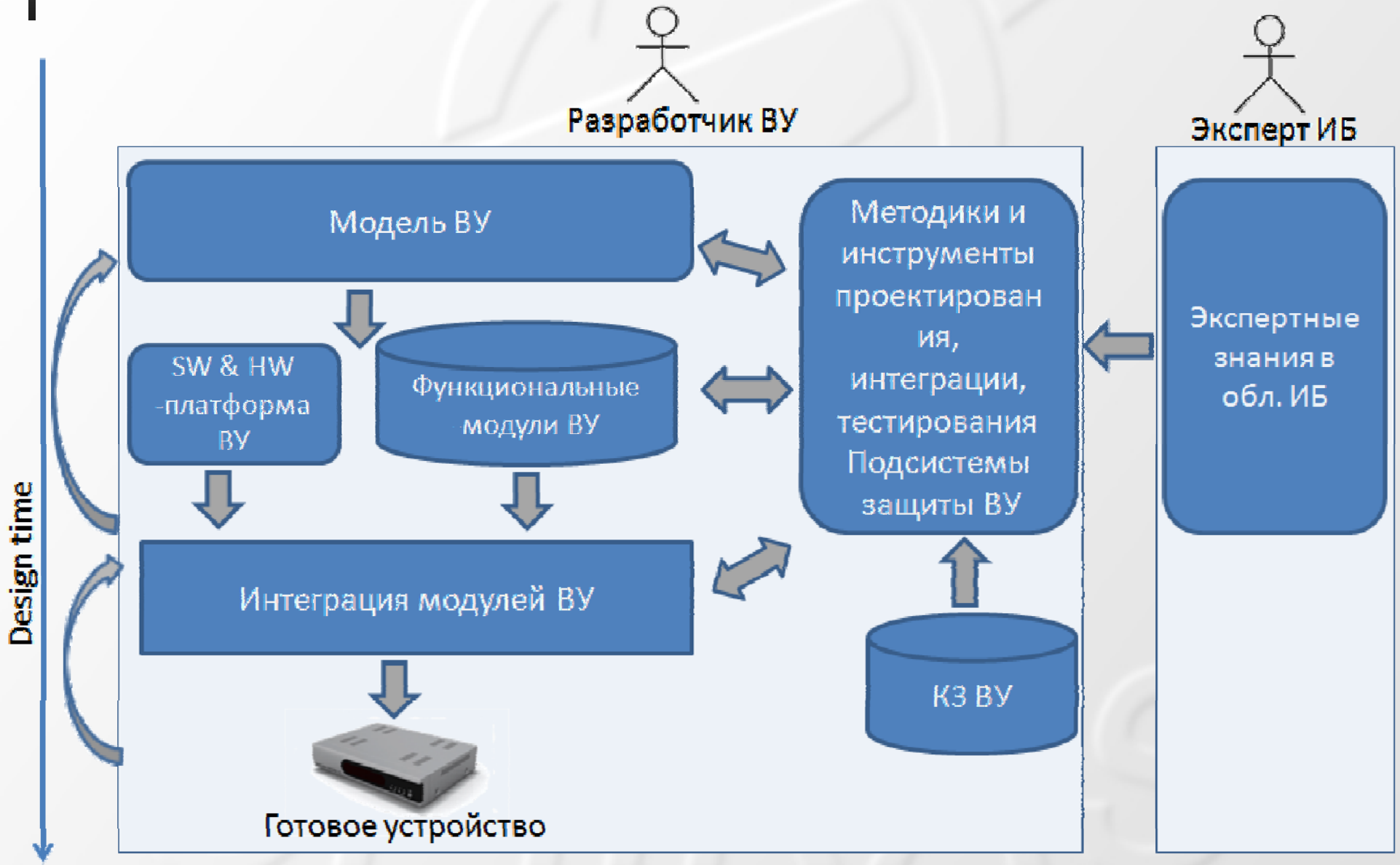
I. модель угроз, ранжирование угроз → требования защиты → шаблоны защиты → базовые КЗ, их реализация/интеграция

II. анализ возможных связей и конфликтов между КЗ

III. анализ связей и несоответствий между функциональной частью ВУ и подсистемой защиты ВУ

{security} ↔ {*utility*, *safety*, resource consumption и др.}

Процесс проектирования ВУ (4/4)



Задачи исследования

Задачи:

1. Выявление экспертных знаний (ЭЗ) в области ИБ ВУ
   - В т.ч.: знания о нарушителях ВУ, КЗ их функц. и нефункц. Требованиях и ограничениях, информационных потоках (ИП) и др.
2. На основе ЭЗ разработка частных методик и программных инструментов проектирования и анализа

Источники ЭЗ:

- Существующие информационно телекоммуникационные системы: STB (Technicolor), MD (Mixed-mode), TMN (Ruag)
- Научно-исследовательские работы в области

Онтологическое представление ЭЗ (классы и отношения):

- Формализация ЭЗ, уточнение семантики
- Входные данные для автоматизации проектирования, верификации и принятия решений защиты ВУ

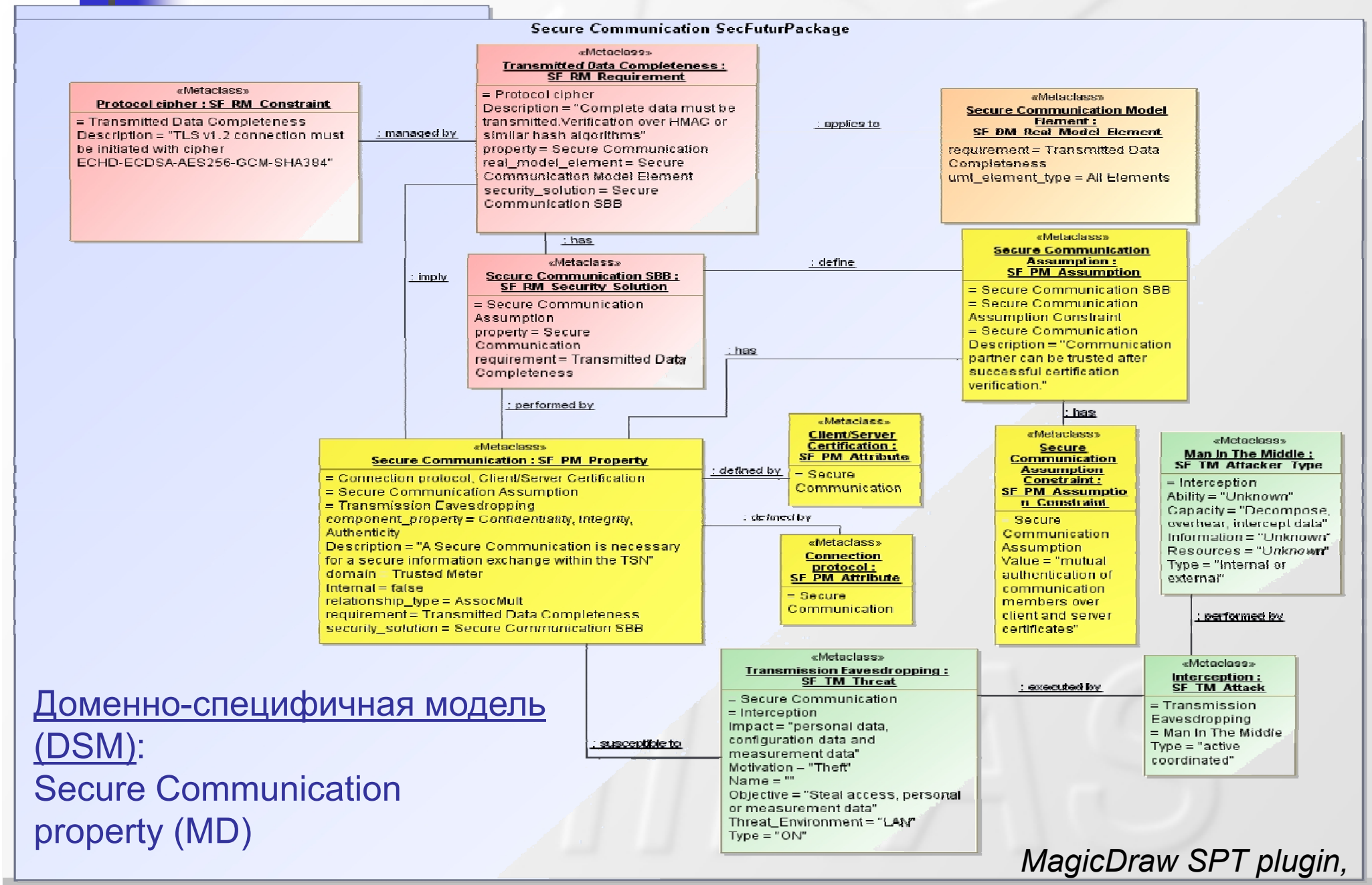
Релевантные работы

- Ключевые проблемы проектирования встроенных устройств:
  - *Myagmar S., Lee A.J., Yurcik W. Threat Modeling as a Basis for Security Requirements // Symposium on Requirements Engineering for Information Security, 2005*
  - *Rae A.J., Wildman L.P. A Taxonomy of Attacks on Secure Devices // Australian Information Warfare and IT Security, 20–21 November 2003, Australia, pp. 251–264, 2003.*
  - *Kommerling O., Kuhn M.G. Design principles for tamper-resistant smartcard processors // Proceedings of the USENIX Workshop on Smartcard Technology, pp. 9–20, Chicago, May 10–11, 1999.*
- Модели проектирования систем со встроенными устройствами:
  - *Rein A., Rudolph C., Ruiz J.F. Building Secure Systems Using a Security Engineering Process and Security Building Blocks // Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS-Workshop), 2013, http://subs.emis.de/LNI/Proceedings/Proceedings198.html*
  - *Eby M., Werner J., Karsai G., Ledeczi A. Integrating Security Modeling into Embedded System Design // Engineering of Computer-Based Systems, pp. 221-228, 2007*
  - *Nadjm-Tehrani S., Vasilevskaya M. Towards a Security Domain Model for Embedded Systems // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011.*
  - *Mana A., Ruiz J.F. A Security Modelling Framework for Systems of Embedded Components // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011*
  - *Rudolph C. Security Engineering and Modelling of Set-top Boxes // RISE'12, Workshop on Redefining and Integrating Security Engineering at ASE/IEEE International Conference on Cyber Security 12, IEEE, 2012*

Примеры экспертных знаний

Предмет ЭЗ	Примеры ЭЗ	Применение ЭЗ	Публикации
Проблемы защиты ВУ (Embedded security design challenges). Известные модели нарушителей ВУ	Работы в обл.: [Ravi'04], [Kocher'04], [Henzinger'06], [Werner'07], [Eby'07], [Raghunathan'07] , [Khelladi'08], [Rippel'09], [Ukil'11], [Burleson'12], и др. Модели нарушителя [Rae'03], [Grand'04], [Abraham'91]	Методика верификации спецификаций ВУ на предмет выявление потенциальных атак на ВУ	– Jose Fran. Ruiz, Vasily Desnitsky, Rajesh Harjani, Antonio Manna, Igor Kotenko and Andrey Chechulin. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February, 2012. P.261-268. – Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3, С.68-75.
Информация о КЗ ВУ, требованиях и ограничениях и Эвристика порядка учета нефункц. Требований	Спецификация нефункц. и функц. требований	Инструмент принятия решений комбинирования КЗ Конфигуратор КЗ ВУ	– Vasily Desnitsky, Igor Kotenko, Andrey Chechulin. Configuration-based approach to embedded device security. Lecture Notes in Computer Science, Springer-Verlag. The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October 17-19, 2012, St. Petersburg, Russia. P.270-285. – Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013. С.44-54.
Типовые конфликты между КЗ ВУ	Три типа конфликтов КЗ	Методика выявления конфликтов КЗ ВУ	– Десницкий В.А., Чечулин А.А. Анализ несовместимостей компонентов защиты в процессе проектирования безопасных встроенных устройств // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.17-19.
Информация о системе и информационных потоках (ИП) Знания о типовых конфликтов и аномалиях ИП	Правила запрета и разрешения ИП вида rule:=(aFlow, true/false) aFlow := (Us, Ns, Is, Ut, Nt, It, T)	Методика и программный инструмент верификации ИП на основе SPIN	– Десницкий В.А., Котенко И.В., Чечулин А.А. Верификация информационных потоков для проектирования защищенных информационных систем со встроенными устройствами // Системы высокой доступности, № 3 (9), 2013. С.112-118.

Представление ЭЗ с использованием UML



Доменно-специфичная модель (DSM):
Secure Communication property (MD)

MagicDraw SPT plugin, [Mixed-mode use case]

(I) Статическое тестирование (1/3)

Классы нарушителей по типу взаимодействия с ВУ [Rae'03]

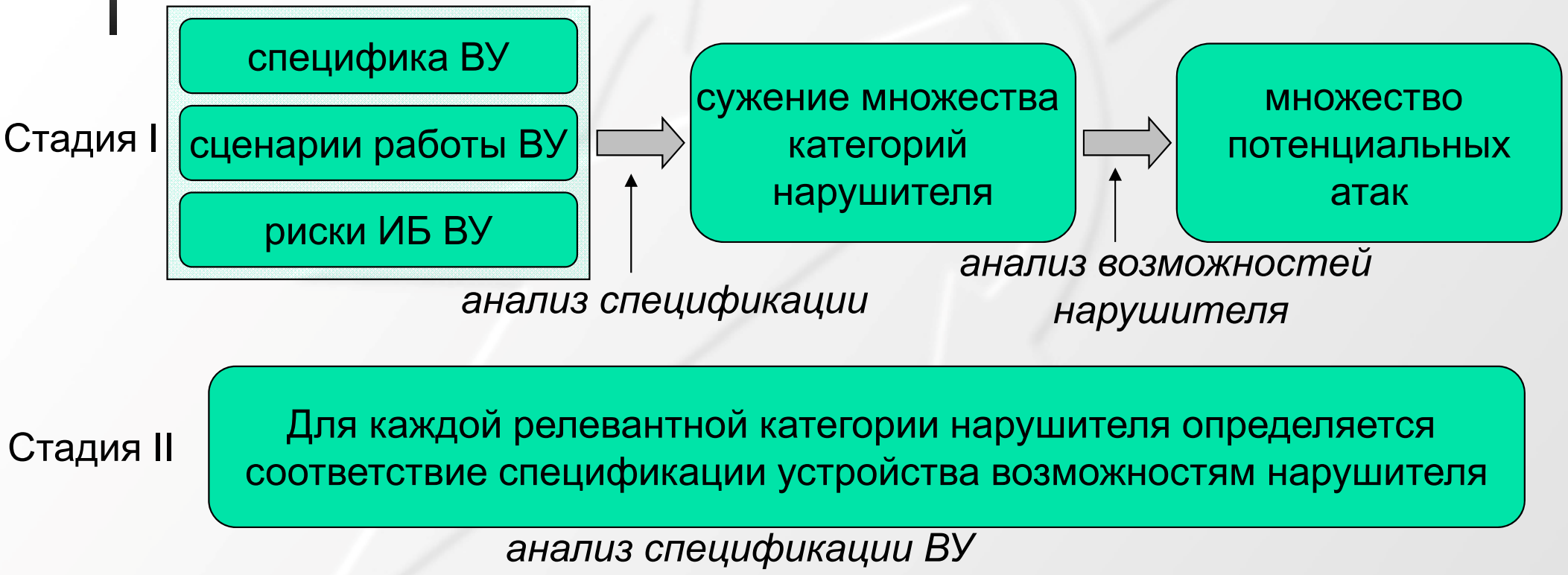
- Тип 1 (T_1). Взаимодействует с ВУ через сеть Интернет
- Тип 2 (T_2). Находится в непосредственной близости от ВУ, но не имеет физического доступа к нему
- Тип 3 (T_3). Есть физический доступ к ВУ, но нет возможности доступа к встроенным в него электронным компонентам
- Тип 4 (T_4). Есть полный доступ к ВУ и к его электронным компонентам

(I) Статическое тестирование (2/3)

Классы нарушителей уровню возможностей [Abraham'91]

- Уровень 1 (I_1). Минимальный или средний уровень навыков и общедоступные средства
- Уровень 2 (I_2). Инженерные навыки и специальные, но общедоступные средства
- Уровень 3 (I_3). Инженерные навыки и высоко специализированное лабораторное оборудование

(I) Статическое тестирование (3/3)



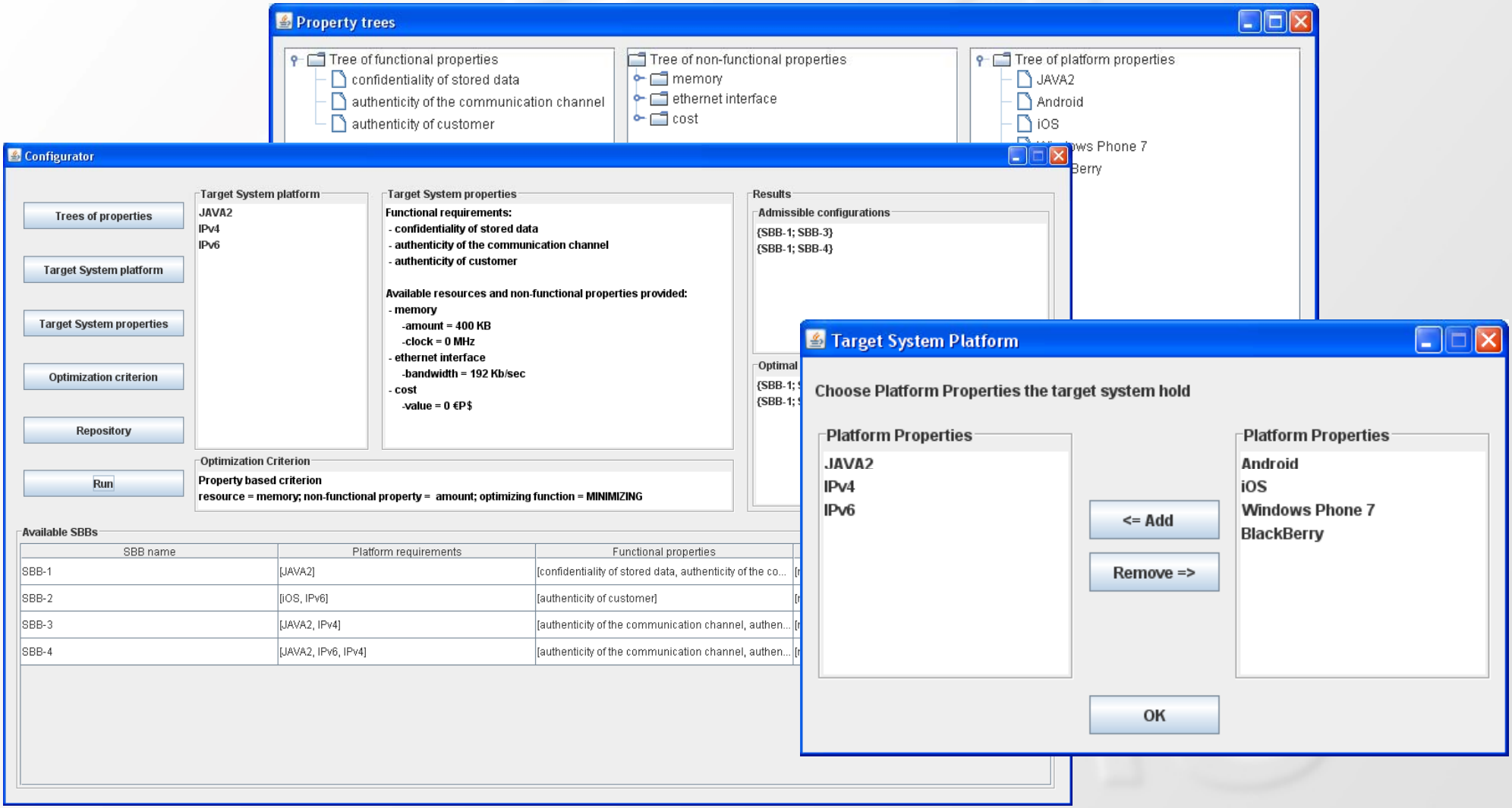
- Пример правил тестирования (ЭЗ):

  If ! has_Internet_connection(device) → no T_1 intruder

  If I_1 intruder → криптоанализ практически невозможен

(II) Конфигурирование КЗ (1/2)

Инструмент принятия решений комбинирования КЗ на основе функциональных и нефункциональных требований и ограничений КЗ и ВУ



(II) Средство конфигурирования КЗ (2/2)

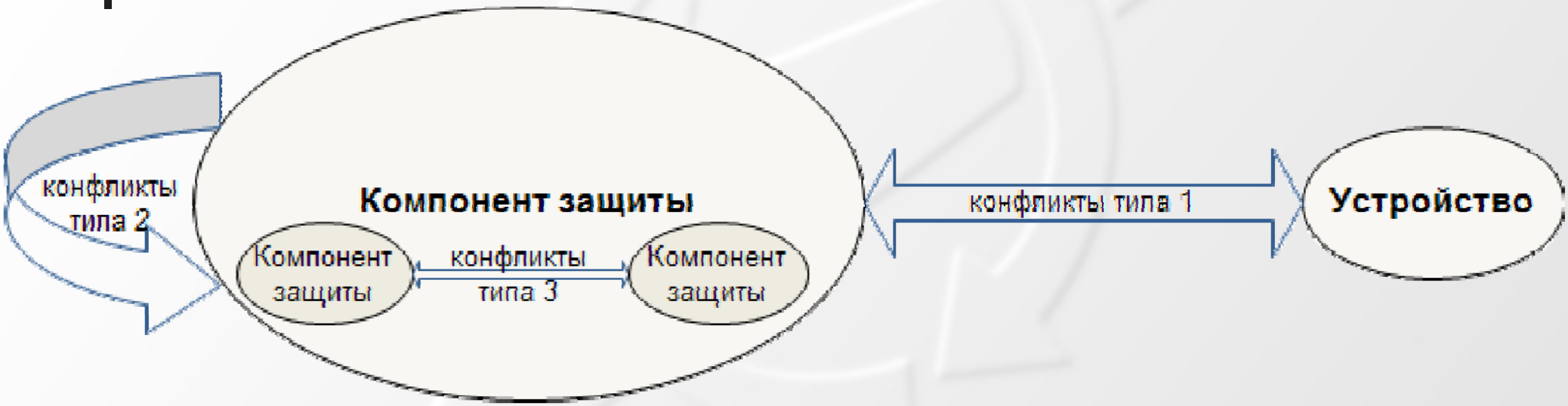
Таблица признаков эвристики

Вид ресурса с соотв. с MARTE	Признаки ВУ и сервисов	Пример системы	Ранг
HW_PowerSupply (ресурс энергопотребления)	Наличие постоянного источника питания	MD, STB	0
	Заменяемость ВУ или аккумулятора	TMN	1
	Эпизодический доступ к централизованному источнику питания	TMN	1
	Высокая зависимость целей ВУ от HW_PowerSupply	TMN	2
HW_StorageManager (ресурс хранения)	ВУ не хранит больших массивов данных, потеря данных некритична	MD *(данные измерений)*	0
	Хранение больших массивов данных, потеря данных некритична	STB *(видео-данные)*	1
	Хранение больших или заранее неограниченных массивов данных, критичность потери	TMN *(данные с сенсоров ВУ, история их значений)*	2
HW_Computing (вычислительный ресурс)	Нет сложных вычислений, нет срочности	–	0
	Нет сложных вычислений, своевременность	MD *(снятые данных с сенсора)*	1
	Сложные вычисления, срочность малая	STB *(кодир./ декодир. видео данных)*	2
	Сложные вычисления, возможна срочность	TMN *(обработка в реальном времени)*	2
HW_Communication (коммуникационный ресурс)	Нет коммуникаций (или они не требуются для выполнения сервисов ВУ)	–	0
	Важность коммуникаций для сервисов ВУ, небольшие объемы данных	MD	1
	Важность коммуникаций, большие массивы данных	STB, TMN	2

(III) Анализ конфликтов КЗ (1/2)

- **Эвристический анализ – выявление известных типов конфликтов:**
- Тип 1 – противоречия вследствие недостаточной согласованности компонента защиты и спецификации устройства
- Тип 2 – противоречия между функциями защиты нескольких компонентов защиты
- Тип 3 – противоречия между базовыми компонентами защиты, входящими в один комплексный компонент

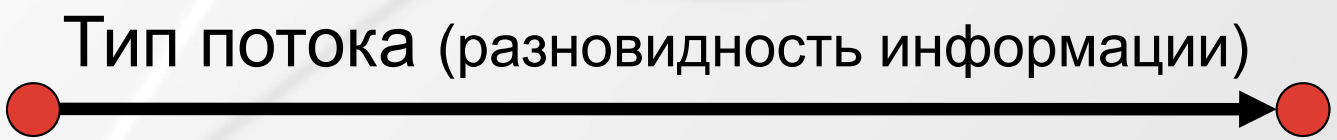
(III) Анализ конфликтов КЗ (2/2)



- Примеры
- Тип 1: TPM & дублирование с исп. доп. модуля хранения
- Тип 2: Компонент резервного копирования данных и компонент гарантированного уничтожения данных ВУ при наступлении определенного события
- Тип 3: избыточное хранение RAID с исп. нескольких защищенных модулей & несоответствующие хар-ки модулей (объем, скорость диска)

(IV) Верификация информационных потоков (1/4)

- Использование SPIN (http://spinroot.com) – «проверка на модели» (Model Checking) для выявления конфликтов и несоответствий в политике безопасности
- Определение потоков и модели системы на языке PROMELA (PROcess MEta Language)



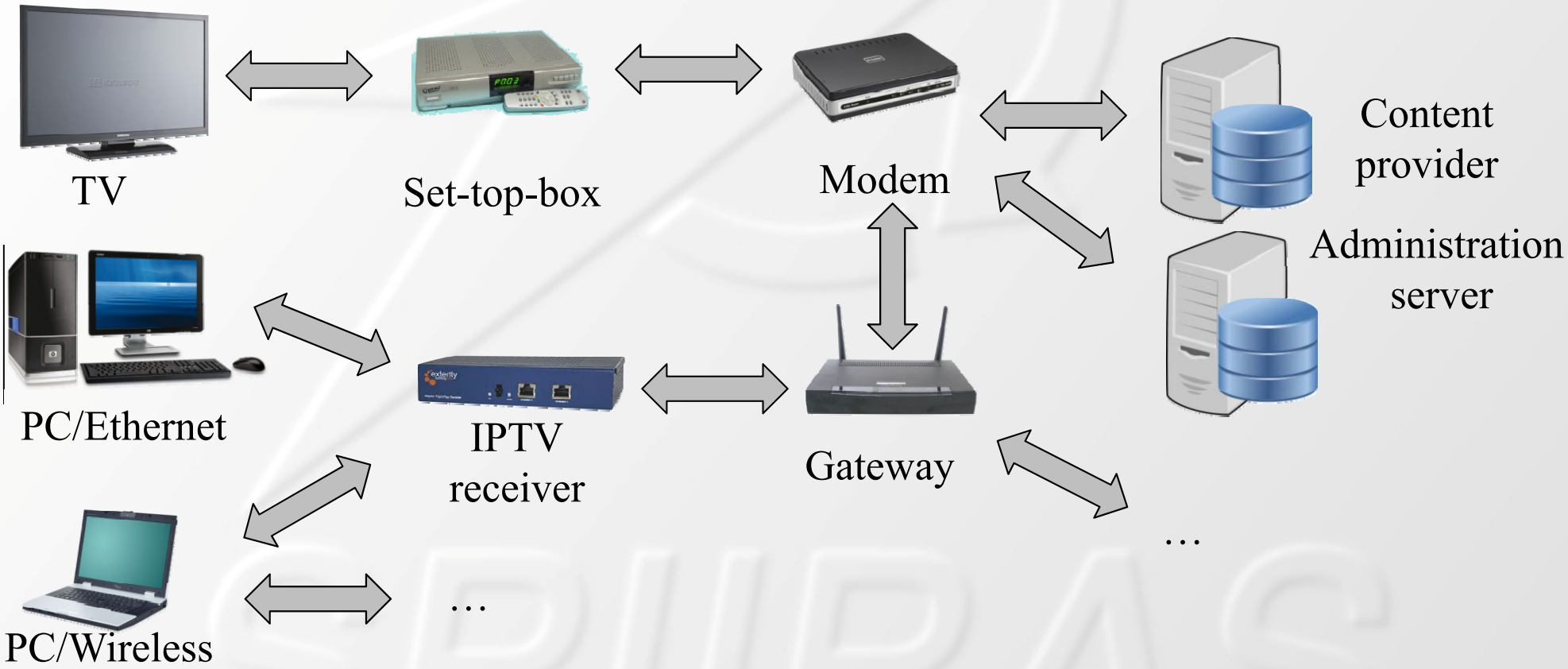
- User-source
- Node-source
- Interface-source

- User-target
- Node-target
- Interface-target

aFlow := (Us, Ns, Is, Ut, Nt, It, T)

(IV) Верификация информационных потоков (2/4)

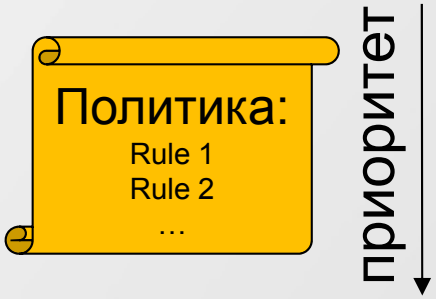
Применение в телекоммуникационных системах



(IV) Верификация информационных потоков (3/4)

Модель системы:

- Users:
  - customer, operator, technician, etc.
- Nodes:
  - TV device, customer PC, set-top-box, gateway, content provider, etc.
- Interfaces:
  - wire, wireless, Ethernet, Wi-Fi, etc.
- Types of flows:
  - paid content, free content, control and authentication data, encrypted data, DRM protected data, etc. *(the ones may intersect)*



Rule1 := (flow1, allow/deny)
Rule2 := (flow2, deny/allow)

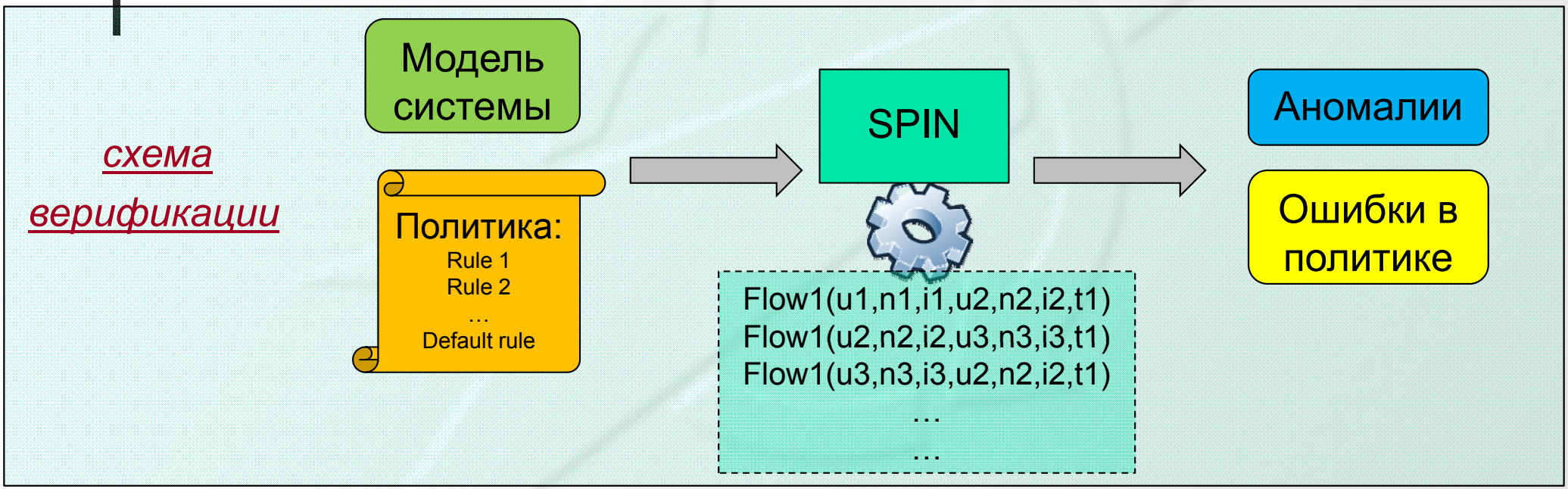
Пример потока:

flow1 := (customer, customer PC, Wi-Fi, any, Administration server, any, authentication data)

Пример правила политики:

(flow1, deny)

(IV) Верификация информационных потоков (4/4)



Аномалия: обнаружено правило, которое ни разу не было выполнено

Вероятно, правило избыточно

Ошибка в политике

Необходимо пересмотреть политику

пример аномалии (ЭЗ)

(IV) Средство верификации (1/3)

Пример описания моделируемой системы:

Open... | ReOpen | Save | Save As... | Syntax Check | Redundancy Check | Symbol Table | Find:

```
6           /* ACTION */
7           mtype = {allow, deny};
8           mtype action;
9
10          /* HOSTS */
11          mtype = {any_host, operatorPC, TSNPC, RemotePC, OCSS, TSNS, Gateway, GPT,
TSMC, TSM, TS, TM, TSN_server, AdministratorServer, AdministratorPC, OperatorPC};
12          mtype host1;
13          mtype host2;
14
15          /* USERS */
16          mtype = {any_user, manufacturer, calibrator, technician, TSN_administrator, operator_
TRM, Operator_OAB, operator_administrator, customer, Operator};
17          mtype user1;
18          mtype user2;
19
20          /* INTERFACES */
21          mtype interface1;
22          mtype interface2;
23          mtype = {any_interface, local_interface, remote_interface}
24
25          /* TYPE */
26          mtype type;
27          mtype = {any_type, Customer_account_data, Privacy_non_relevant_data,Privacy_rele
vant_consumption_data, Manufacturer_certificate, Calibration_certificate, Administrator_user_ac
count_data, Operator_user_account_data, Installation_certificate, Deinstallation_certificate, Com
```

(IV) Средство верификации (2/3)

Пример правил:

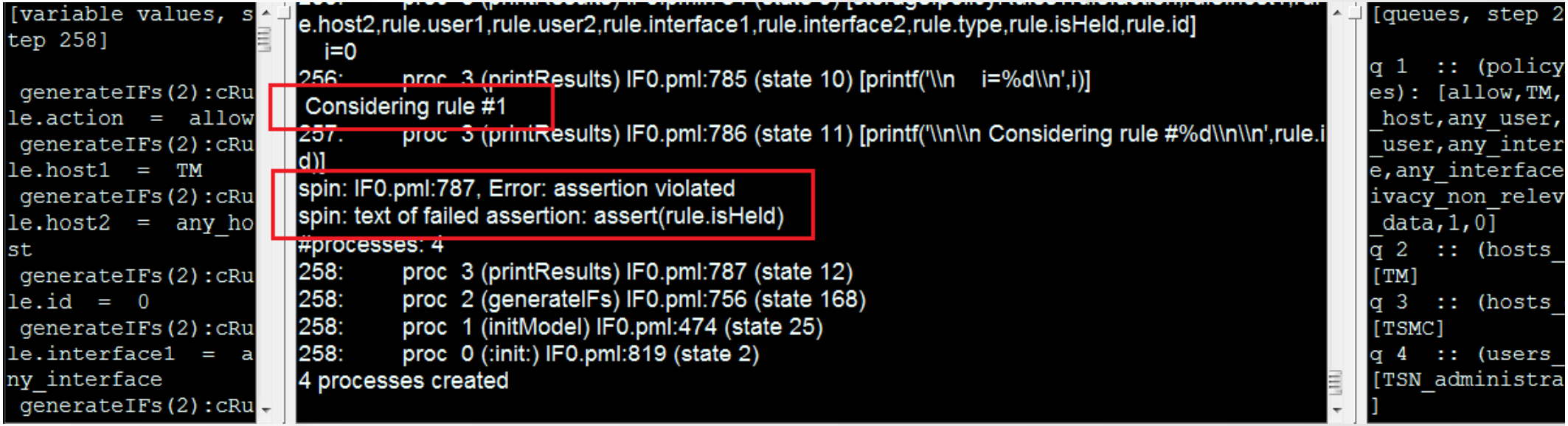
Open… | ReOpen | Save | Save As… | Syntax Check | Redundancy Check | Symbol Table | Find:

```
nformation which can be read from existing electromechanical meters and it is not considered to
be privacy relevant. */
81
82          rule0.user1 = any_user;
83          rule0.user2 = any_user;
84          rule0.interface1 = local_interface;
85          rule0.interface2 = any_interface;
86          rule0.host1 = TM;
87          rule0.host2 = any_host;
88          rule0.type = Privacy_non_relevant_data;
89          rule0.action = allow;
90          rule0.isHeld = false;
91          rule0.id = 0;
92          storage.policyRules!rule0;
93
94          rule1.user1 = any_user;
95          rule1.user2 = any_user;
96          rule1.interface1 = any_interface;
97          rule1.interface2 = any_interface;
98          rule1.host1 = TM;
99          rule1.host2 = any_host;
100         rule1.type = Privacy_non_relevant_data;//Privacy_relevant_consumption_data;
101         rule1.action = deny;
102         rule1.isHeld = false;
103         rule1.id = 1;
104         storage.policyRules!rule1;
```

```
Spin Version 6.2.2 -- 6 June 2012
iSpin Version 1.1.0 -- 7 June 2012
TclTk Version 8.5/8.5
1 E:/Work/SecFutur/doc/Information flows/IF0.pml:1
```

(IV) Средство верификации (3/3)

Результаты верификации:



Заключение

- Дальнейшая работа:
  - Уточнение ЭЗ для конкретных компонентов проектирования и верификации
  - Формирование онтологического представления с использованием Protégé
  - Разработка инструментов проектирования и верификации на основе ЭЗ

Контактная информация

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

Благодарности

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2) и проекта ENGENSEC программы Европейского Сообщества TEMPUS.

ВОПРОСЫ?