Учёный совет ИПУ РАН
5 октября 2017 года

Новые аспекты кибербезопасности

Д.т.н., профессор Назаров А.Н., заведующий лабораторией 79 «Управление безопасностью киберфизических систем»

Москва
2017

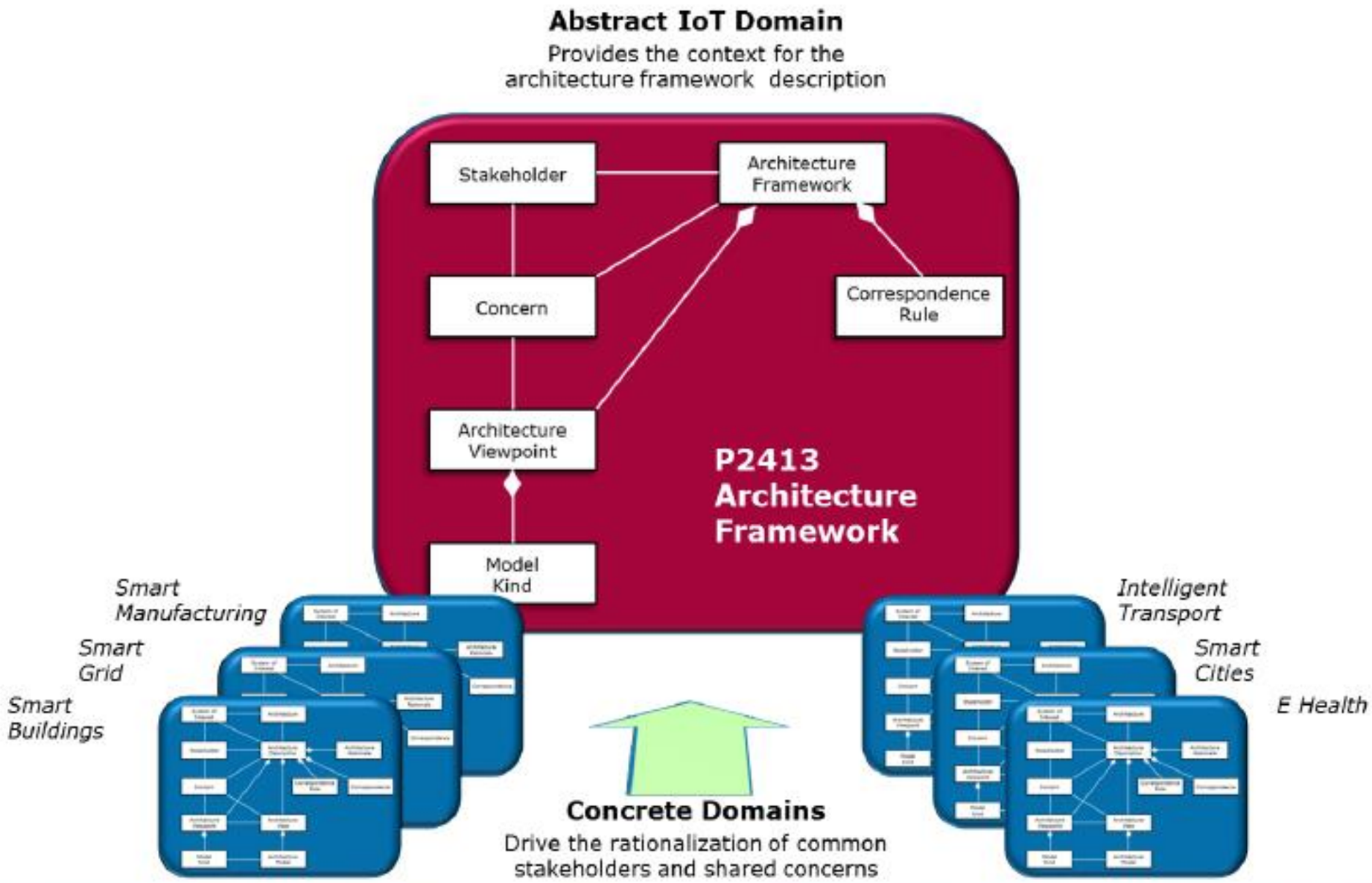
Новые аспекты кибербезопасности

Система оценки, мониторинга и управления (СОМУ) рисками ИБ для IoT

Авторский коллектив от ИПУ РАН: проф. Рыжов А.П., проф.Назаров А.Н.,…

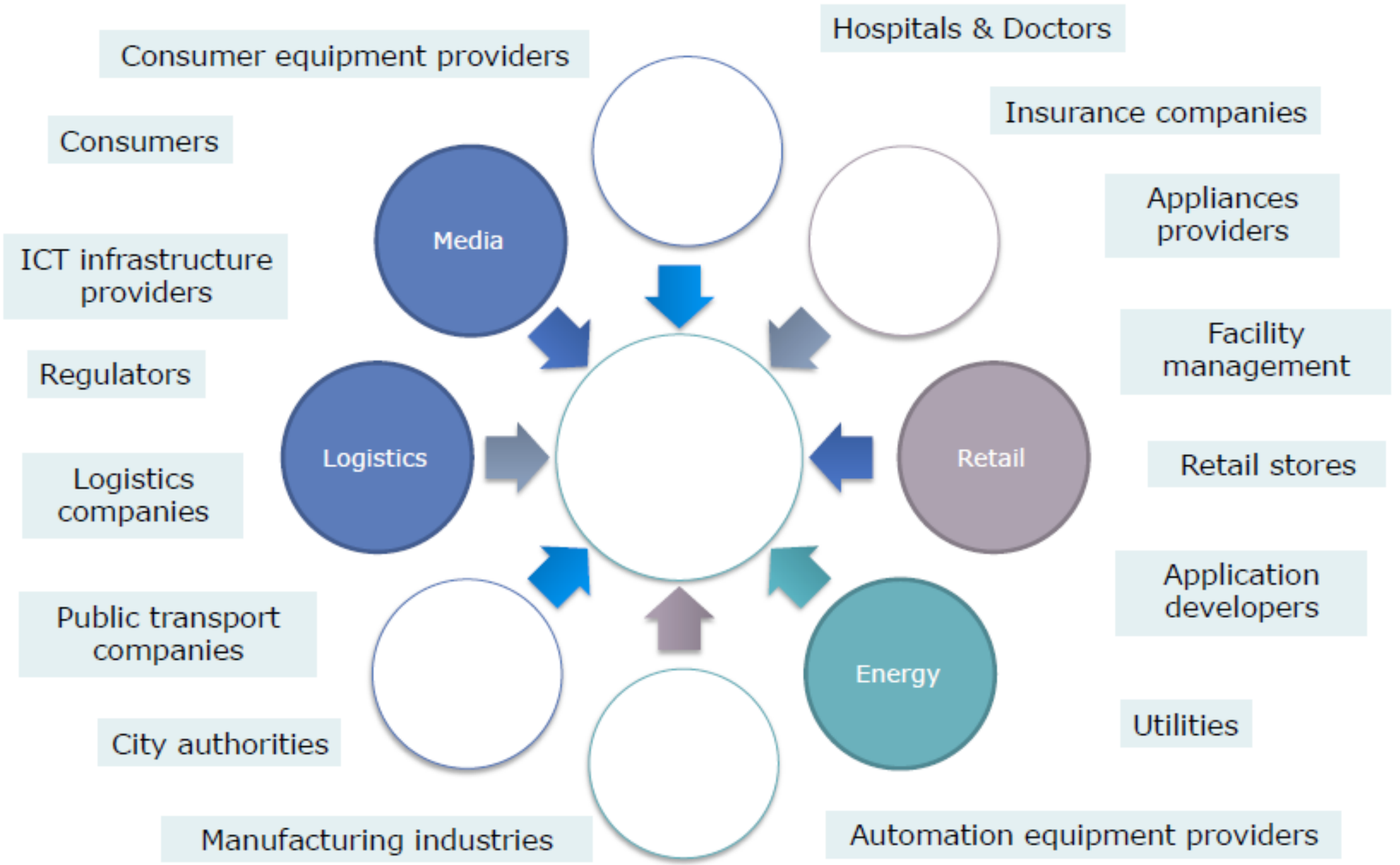
Новые аспекты кибербезопасности

P2413 Architecture Framework



Новые аспекты кибербезопасности

Where does the input come from?*



IEEE STANDARDS ASSOCIATION

*due to the diversity of IoT application areas only selected domains and stakeholders are shown

IEEE

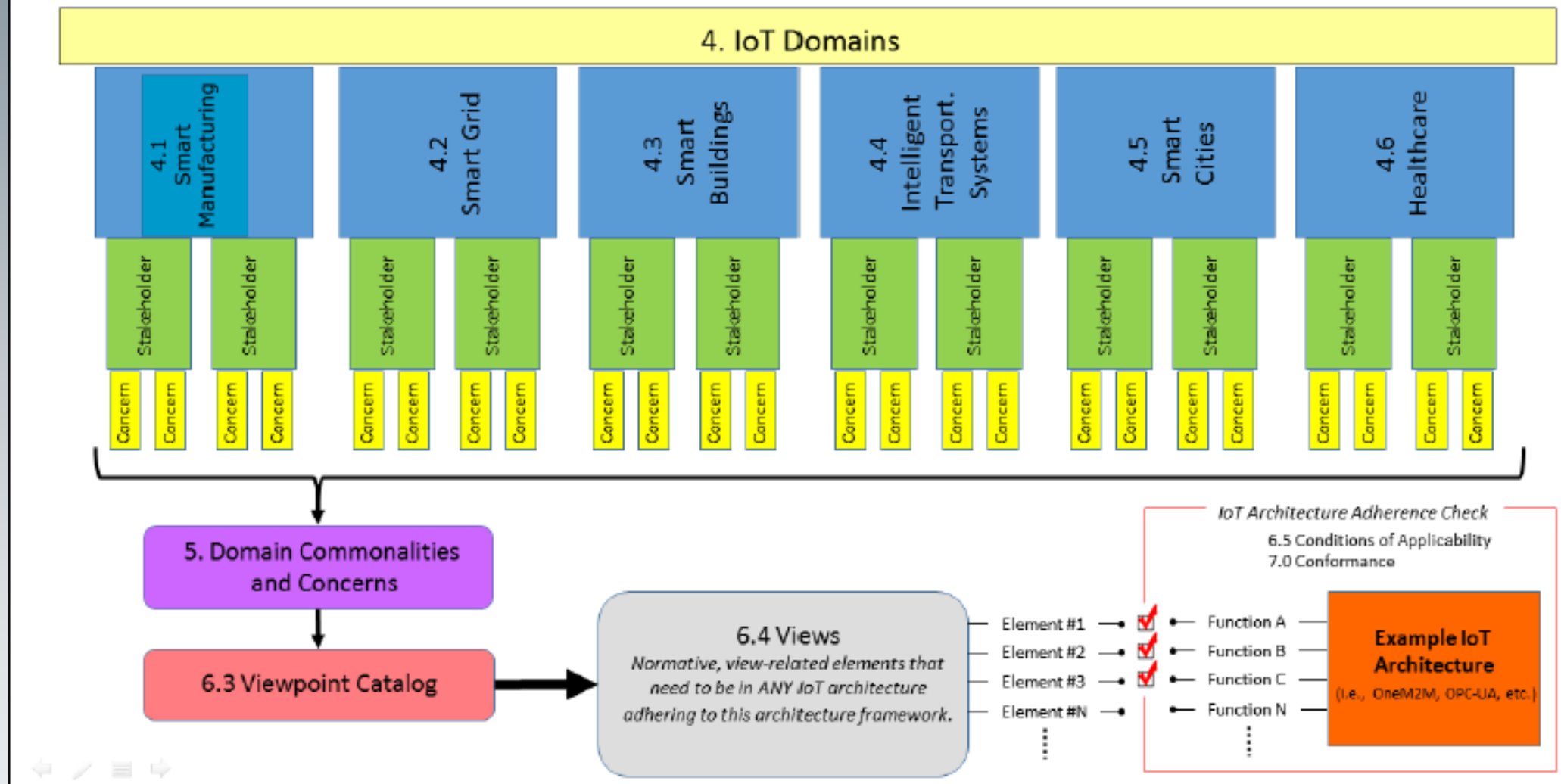
Новые аспекты кибербезопасности

Basic Document Structure

Part 1	**IoT: Vertical Application Domains** Provides descriptions of IoT behaviors in the context of vertical application domains	*Informative*
Part 2	**IoT: Modeling the Horizontal** Discussion of the core characteristics across IoT domains	
Part 3	**Architecture Framework** IEEE/IEC/ISO 42010:2011 conformant description of the P2413 IoT Architecture Framework	*Normative*
Part n **Annex**	**Using the IoT Architecture Framework** Further elaborates the P2413 IoT Architecture Framework to develop a domain specific IEEE/IEC/ISO 42010:2011 conformant architectural description	*Informative*

Новые аспекты кибербезопасности

Architecture Framework Dev Process



Новые аспекты кибербезопасности

Предпосылки (top 3)

- Развитие IoT, рост числа подключаемых устройств
- Слабое внимание производителей к вопросам информационной безопасности устройств
- Потенциал незаконного использования возможностей устройств в сети

Новые аспекты кибербезопасности

Несколько фактов (из ссылок что более «в тему»)

Умные и опасные? (Вопросы безопасности IoT) http://d-russia.ru/umnye-i-opasnye-voprosy-bezopasnosti-iot.html

Евросоюз хочет заняться регулированием Интернета вещей http://d-russia.ru/evrosoyuz-xochet-zanyatsya-regulirovaniem-interneta-veshhej.html

Конгресс США призывают к разработке стандартов безопасности для Интернета вещей http://d-russia.ru/kongress-ssha-prizyvayut-k-razrabotke-standartov-bezopasnosti-dlya-interneta-veshhej.html

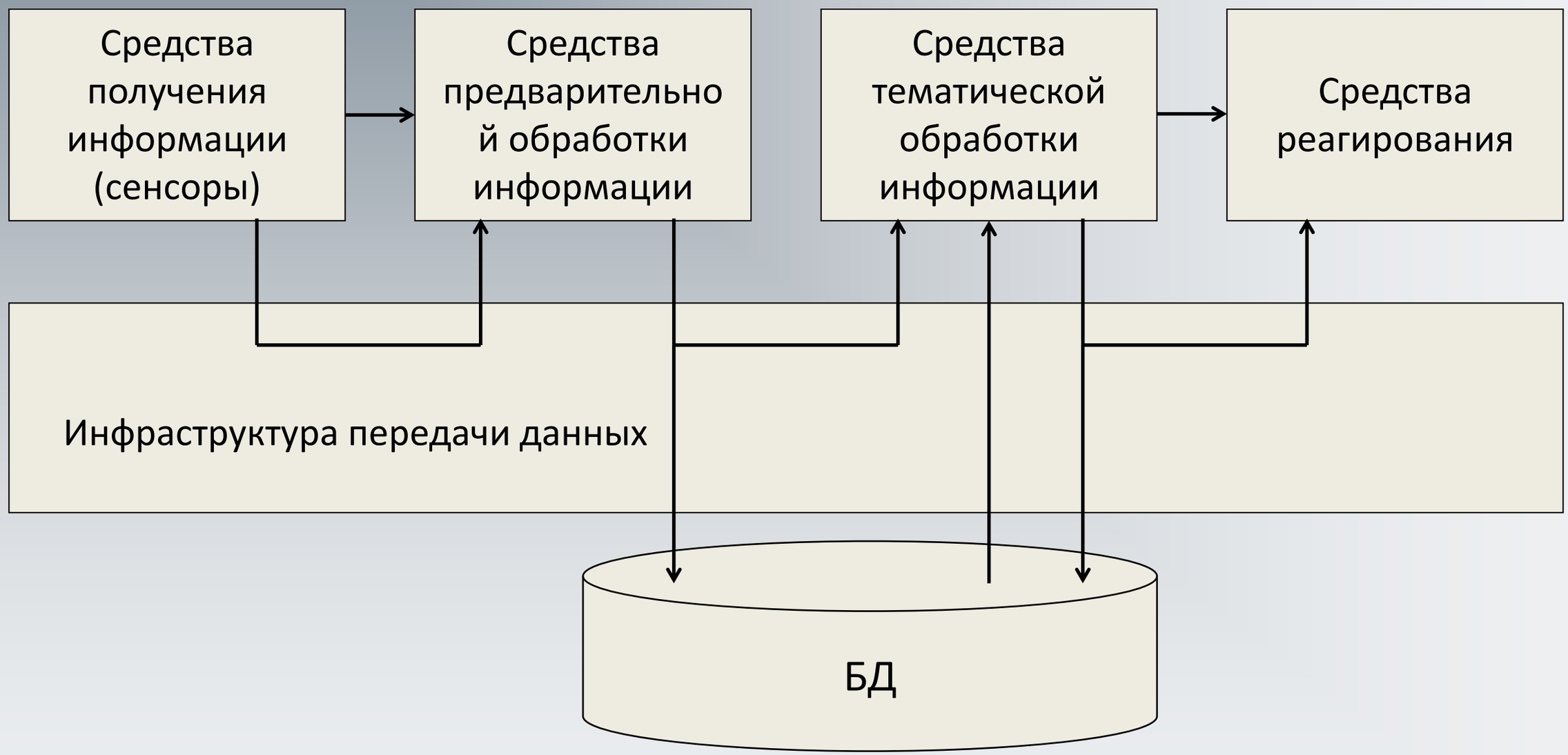
Директор национальной разведки США признал, что Интернет вещей может быть использован для слежки http://d-russia.ru/direktor-nacionalnoj-razvedki-ssha-priznal-chto-internet-veshhej-mozhet-byt-ispolzovan-dlya-slezhki.html

Информационная безопасность в IoT-среде: главные вызовыhttps://iot.ru/bezopasnost/informatsionnaya-bezopasnost-v-iot-srede-glavnye-vyzovy

Новые аспекты кибербезопасности

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Типовая система обеспечения безопасности



Новые аспекты кибербезопасности

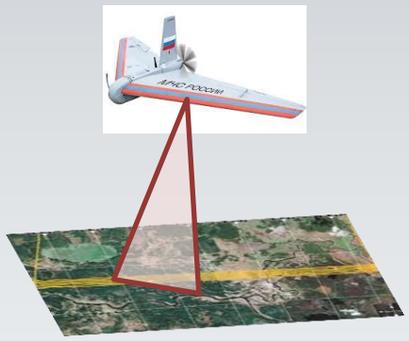
ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Возрастание объёма информации от антропоморфных сенсоров

Миллионы Тб
цифровых космических
снимков

До 64 Гб с одного
устройства

5,5 Гб в час
с одного устройства



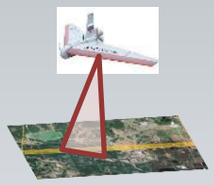
Несколько Тб
за час полета

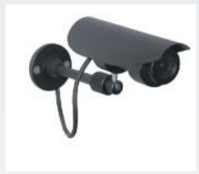
Информация
телефонной связи

Трафик Рунета
> 900 петабайт в месяц

Новые аспекты кибербезопасности

Проблемы обработки возрастающего объёма информации





- Возрастание требований к инфраструктуре передачи данных от средств мониторинга безопасности
- Возрастание требований к инфраструктуре хранения данных
- Сложности с оперативной обработкой данных возрастающего объёма
- Увеличение необходимого числа операторов, осуществляющих обработку данных мониторинга
- Повышение требований к конфиденциальности хранения и обработки данных мониторинга

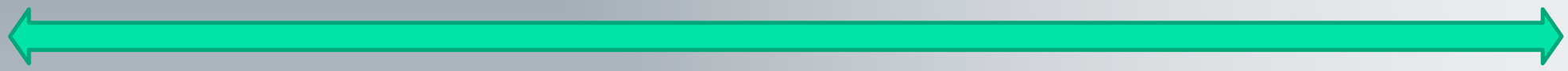
Новые аспекты кибербезопасности

Возможные подходы к созданию системы

«Традиционный»
- все делают люди

Человеко-компьютерная технология оценки и мониторинга сложных процессов

«Искусственный интеллект»
- все делает компьютер



Не удовлетворяет современным требованиям: неэффективно, дорого, не масштабируется…

Быстрая разработка прототипа системы, способного решать поставленную задачу:

Не является реалистичным на сегодня

- **Оценка уровня рисков на основе всей доступной информации**
- **Выявление и оценка факторов, виляющих на текущий уровень рисков**
- **Оценка сильных и слабых сторон возможных действий по улучшению ситуации**
- **Разработка мероприятий по блокированию нежелательных и провоцированию желательных изменений в работе с IoT**
- **Оптимизация бюджетов на развёртывание и эксплуатацию облака IoT с заданным уровнем ИБ**

Новые аспекты кибербезопасности

Проблема формализации оценки риска ИБ

- Показано [Назаров, 2007], что вероятность успеха любой атаки есть сумма неуспеха вероятностей конечного множества функций защиты объекта риска. Множество функций защиты полно.

- Разработаны методические рекомендации [Назаров, 2008], оценки парциального влияния функций защиты на величину риска. Исследованы условия экстремальных значений риска любой атаки.

- Сформулированы [Назаров, 2016] теоретические основы оценки интегральной защищённости объекта риска и риск-критерии защищённости.

Новые аспекты кибербезопасности

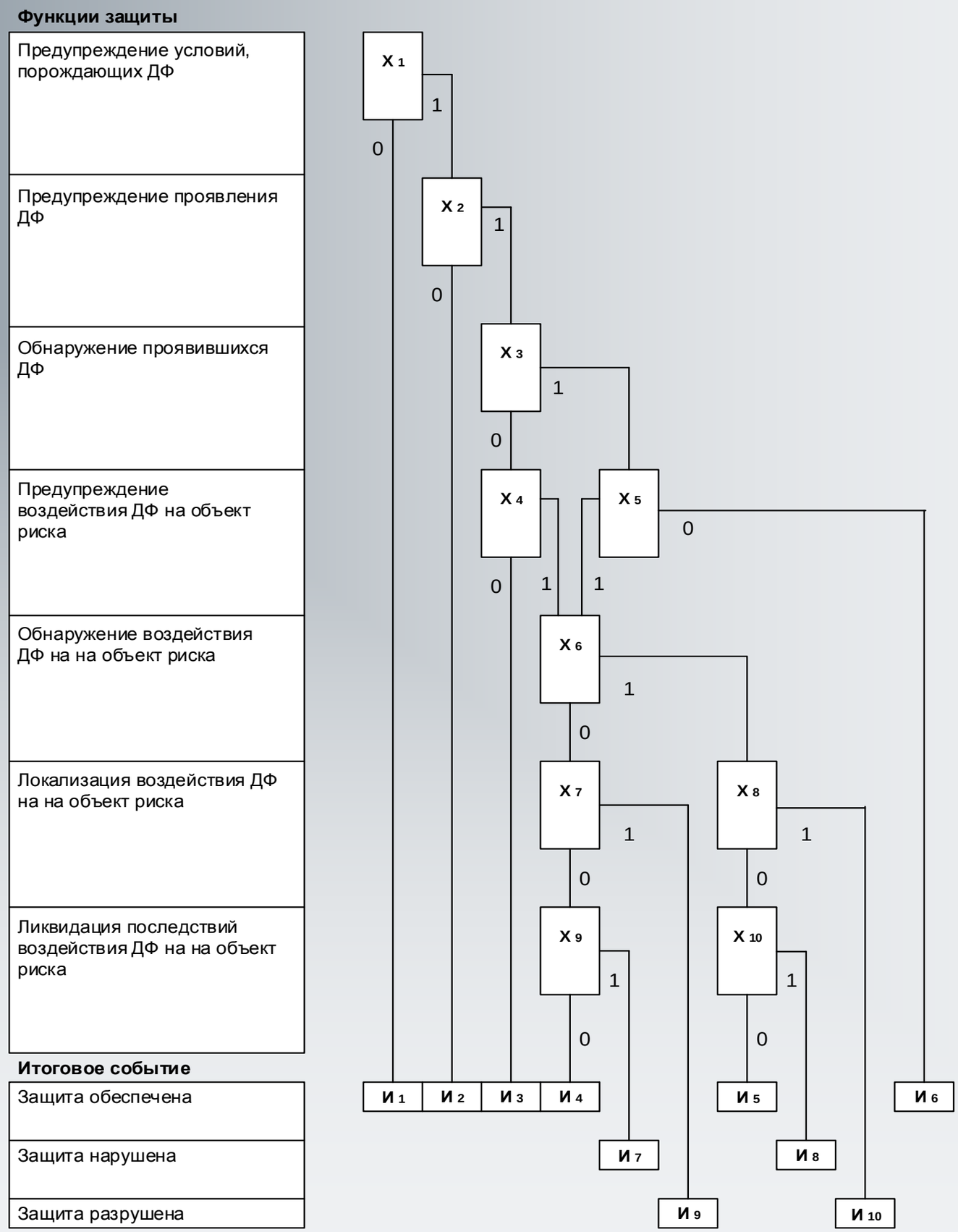
Полная система функций защиты

Таблица 1. Функции защиты

Функция защиты	Назначение функции защиты
X_1	Предупреждение возникновения условий, благоприятствующих порождению (возникновению) дестабилизирующих факторов (ДФ)
X_2	Предупреждение непосредственного проявления ДФ
X_3	Обнаружение проявившихся ДФ
X_4	Предупреждение воздействия на объект риска проявившихся и обнаруженных ДФ
X_5	Предупреждение воздействия на объект риска проявившихся, но необнаруженных ДФ
X_6	Обнаружение воздействия ДФ на объект риска
X_7	Локализация (ограничение) обнаруженного воздействия ДФ на объект риска
X_8	Локализация необнаруженного воздействия ДФ на объект риска
X_9	Ликвидация последствий локализованного обнаруженного воздействия ДФ на объект риска
X_{10}	Ликвидация последствий локализованного необнаруженного воздействия ДФ на объект риска

Новые аспекты кибербезопасности

Причинно-следственные связи функций защиты



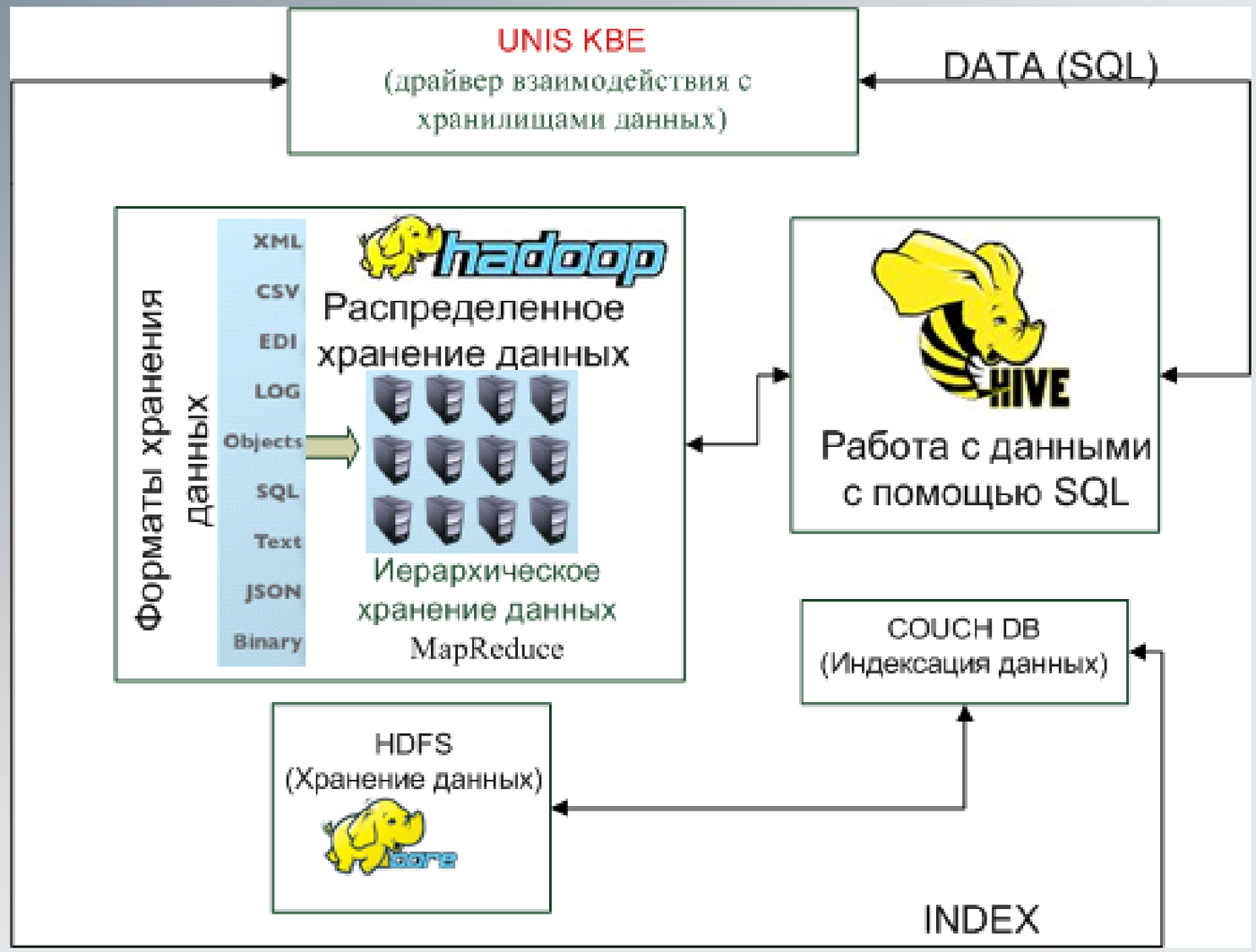
Новые аспекты кибербезопасности

Системы оценки и мониторинга: текущее состояние

- **Решены принципиальные научные вопросы разработки таких систем:**
  - **Модель описания человеком объектов реального мира**
  - **Модель поиска информации в гетерогенных базах данных**
  - **Модель агрегирования информации в нечетких и дискретных иерархических системах**
- **Доказана возможность практического использования теоретических результатов (устойчивость моделей)**
- **Разработан ряд систем на базе полученных результатов**
- **Системы оценки и мониторинга эффективны, когда:**
  - **нет (нельзя построить) математическую модель проблемы/процесса в виде уравнений, автоматов, и т.п.;**
  - **есть аналитики, решающие задачу мониторинга на систематической основе**
- **Мы можем разрабатывать *оптимальные* системы с точки зрения:**
  - **удобства ввода информации аналитиком (пользователем);**
  - **согласованности мнений аналитиков (пользователей);**
  - **информационного обеспечения ввода информации и моделирования**

Новые аспекты кибербезопасности

Иллюстрация использования технологии Hadoop (по материалам ITU)



Новые аспекты кибербезопасности

In the chart below, we display real-world use cases for the various solutions/frameworks.

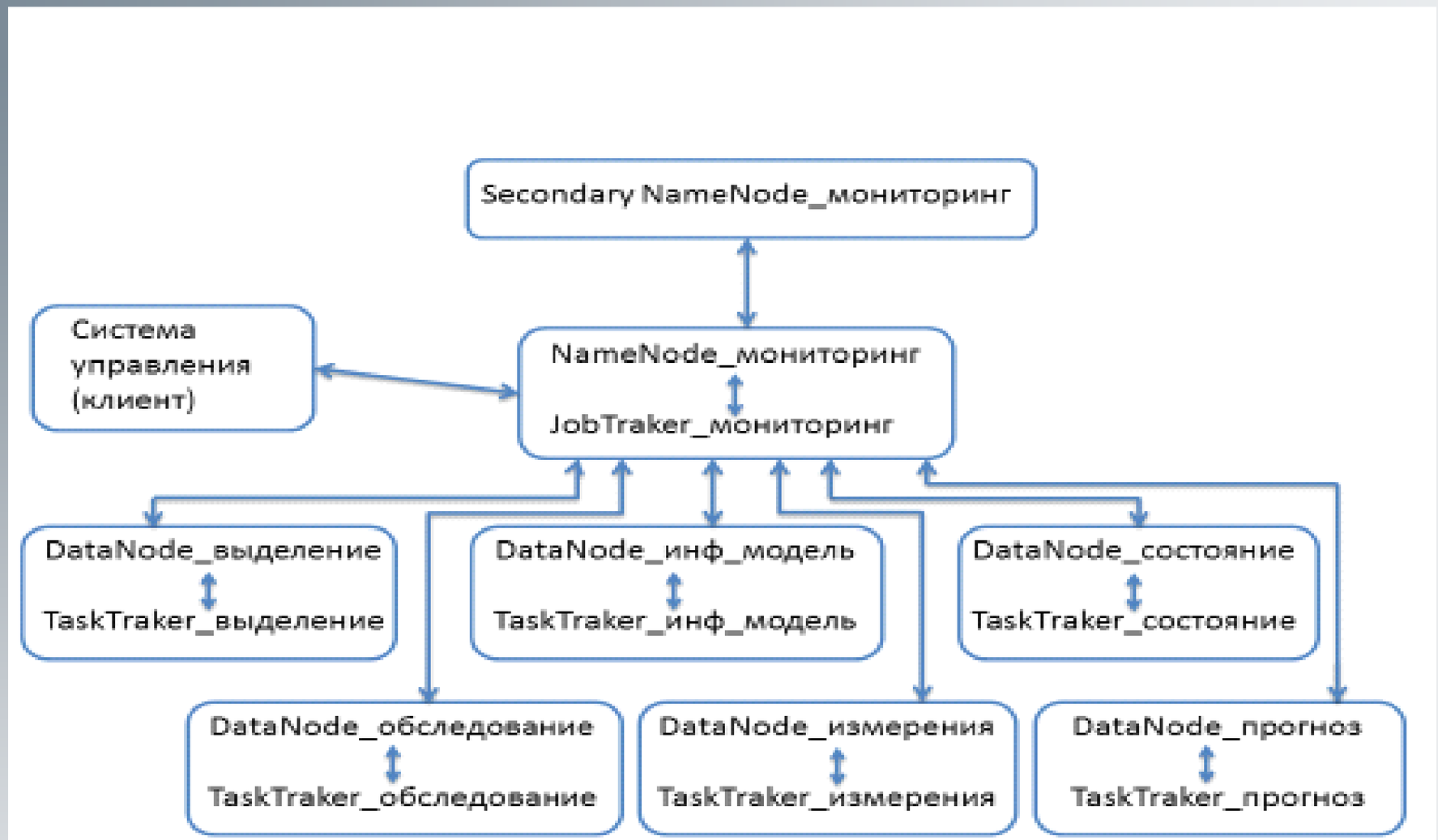
Confirmed in use ✓ | Could support use case ○

USE CASE	Hadoop	MapReduce	Spark	Flink	Storm	SOURCE
JPMorgan Chase is a financial giant which provides services in more than 100 countries. JPMorgan Chase uses HDFS to support the exponentially growing size of data as well as for low latency processing of complex unstructured data.	✓	○	○	○	○	https://www.dezyre.com/article/hadoop-use-cases/232
Cigna leverages Hadoop (including MapReduce) as part of it's architecture to support Descriptive, Predictive and Prescriptive Analytics	✓	✓	○	○	○	http://www.bigdataeverywhere.com/files/chicago/BDE-LeadingaHealthcareCaseStudy-QURAISHI.pdf
ING uses Spark in its data analytics pipeline for anomaly detection. The company's machine learning pipeline uses Spark decision tree ensembles and k-means clustering.			✓	○		http://www.infoworld.com/article/3031690/analytics/why-you-should-use-spark-for-machine-learning.html
Ericsson is leveraging Flink to do real-time analysis on metrics and logs of their cloud infrastructure to include analysis of system behavior and anomaly detection			○	✓	○	http://www.slideshare.net/sbaltagi/apache-flink-realworld-use-cases-for-streaming-analytics
Groupon uses Storm to build real-time data integration systems. Storm helps analyze, clean, normalize, and resolve large amounts of non-unique data points with low latency and high throughput.			○	○	✓	https://www.quora.com/What-are-some-of-the-use-cases-of-Apache-Storm

Методология

Методологически исследования по принятию решения по идентификации наблюдаемого события ИБ для IoT по изменению атрибутов объекта мониторинга проводятся в направлении исследования особенностей применимости нейро-нечеткого формализма для разработки модулей и алгоритмической основы решения научной задачи по идентификации и пресечению кибер-атаки средствами и способами облачной системы web-программирования Hadoop.

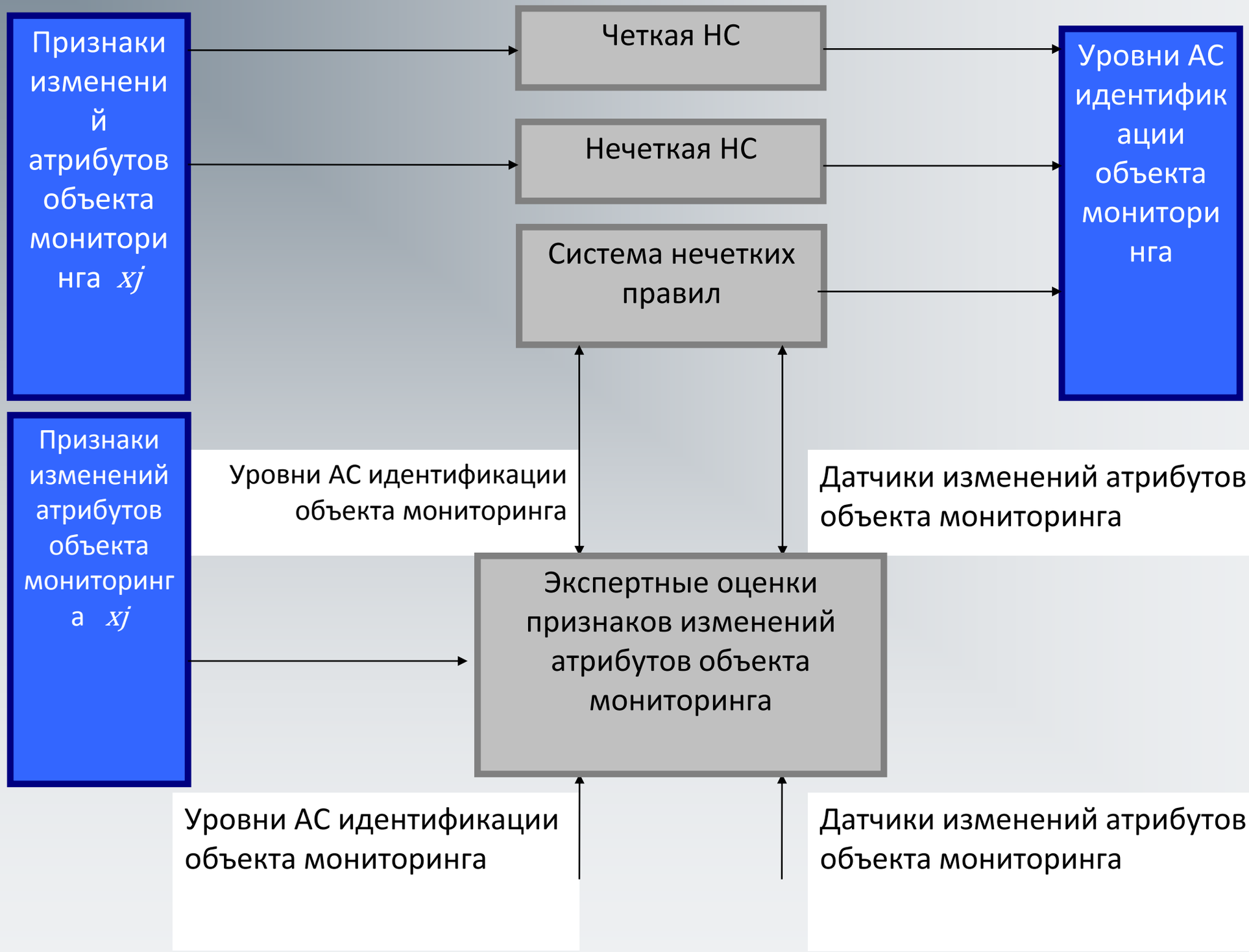
Новые аспекты кибербезопасности



Топология мониторингового кластера Hadoop для СОиБ рисков ИБ для IoT

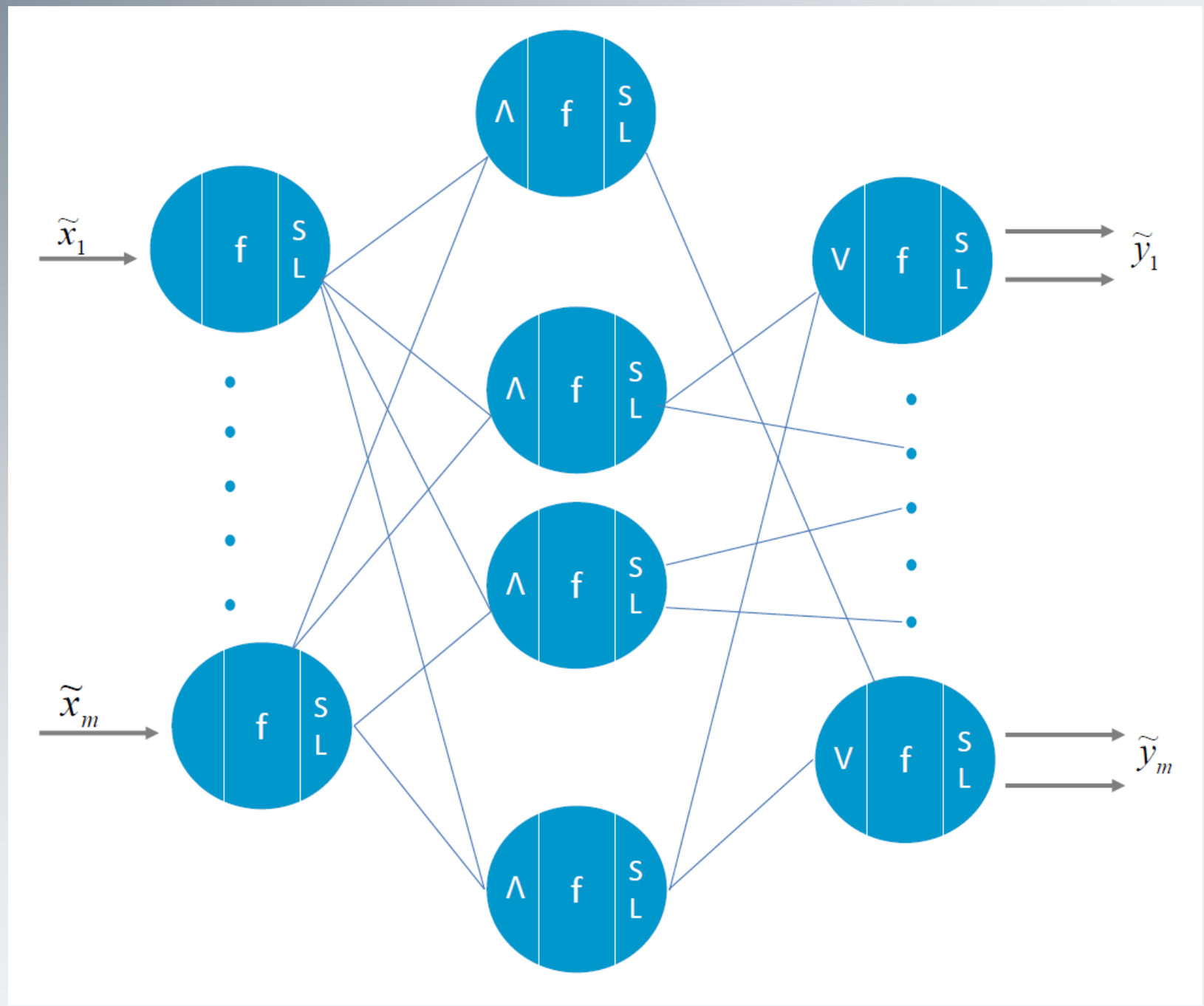
Новые аспекты кибербезопасности

Схема адаптивного классификатора уровня идентификации атаки



Новые аспекты кибербезопасности

Схема нейро-нечёткого классификатора СОиМ



Новые аспекты кибербезопасности

Качество сервисов IoT

Пусть экземпляр продукции **(сервис IoT)** характеризуется совокупностью разнородных величин $x_k, k=\overline{1,m}$. Требования, предъявляемые к качеству продукции заданы в виде двухсторонних полей допусков

$$|\Delta x_k| \le \frac{1}{2} Tx_k, k=\overline{1,m},$$

где $\Delta x_k = x_k - x_{0k}$,

x_{0k} - координата середины поля допуска для величины x_k (значения x_{0k}, $k=\overline{1,m}$ известны), Tx_k - допуск поля допуска.

Альтернативные гипотезы по каждой величине запишутся в следующем виде

$$\left.\begin{array}{l} H_{0k}: |\Delta x_k| \le \frac{1}{2} Tx_k, \\ H_{1k}: |\Delta x_k| > \frac{1}{2} Tx_k, k=\overline{1,m}. \end{array}\right\}$$

Тогда альтернативные гипотезы, представляющие две градации качества продукции **(сервис IoT)**, будут иметь вид

$$\left.\begin{array}{l} H_0: \bigcap\limits_{k=1}^{m} H_{0k} - \text{годная продукция}, \\ H_1: \bigcup\limits_{k=1}^{m} H_{1k} - \text{дефектная продукция}, \end{array}\right\}$$

где «$\bigcap$» и «$\bigcup$» - знаки соответственно произведения и объединения гипотез.

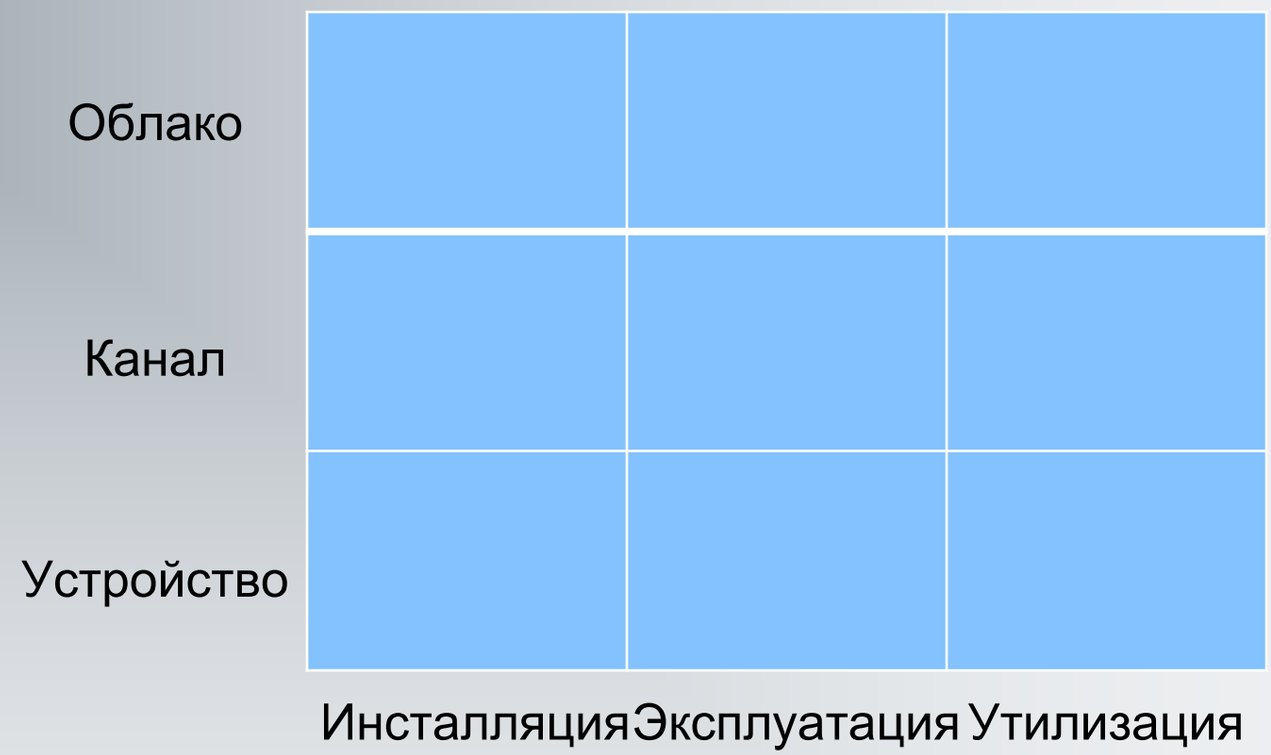
Новые аспекты кибербезопасности

Качество сервисов IoT

- Разработаны алгоритмы определения оптимальных планов измерения для измерительных задач первого и второго типов применительно к различным объектам измерения.
- Получены выражения для оптимальных параметров планов измерения при условии единства измерений для систематической погрешности и дисперсии случайной погрешности.
- Получены алгоритмы формирования оптимальных планов для такой важной в прикладном отношении измерительной задачи как оценка соответствия по качеству экземпляра продукции **(сервиса IoT)** образцовому экземпляру.

Уровни и этапы жизненного цикла

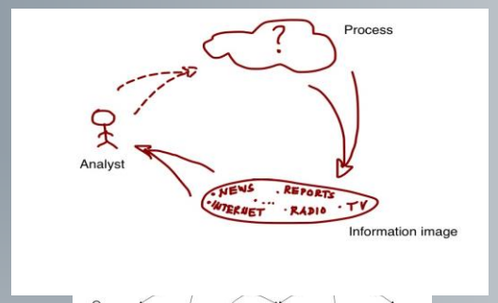
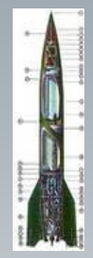
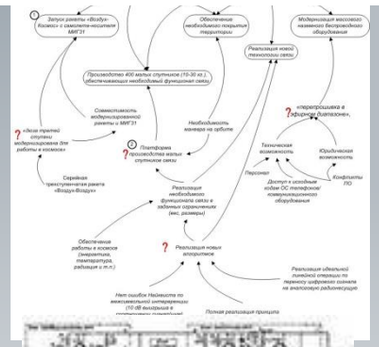
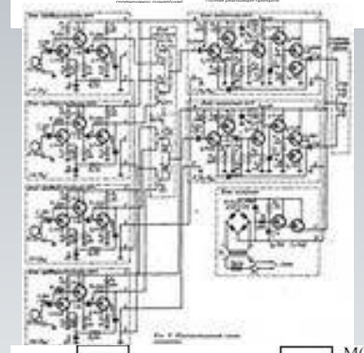
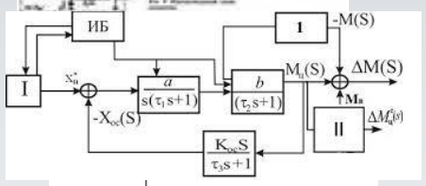
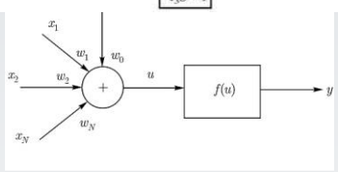
- Уровни
  - Устройство (может иметь структуру)
  - Канал
  - Сеть/облако
- Этапы
  - Инсталляция
  - Эксплуатация
  - Удаление/ утилизация



Каждый квадратик требует своего решения + решение для всей системы

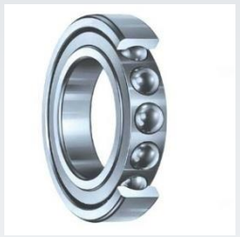
Новые аспекты кибербезопасности

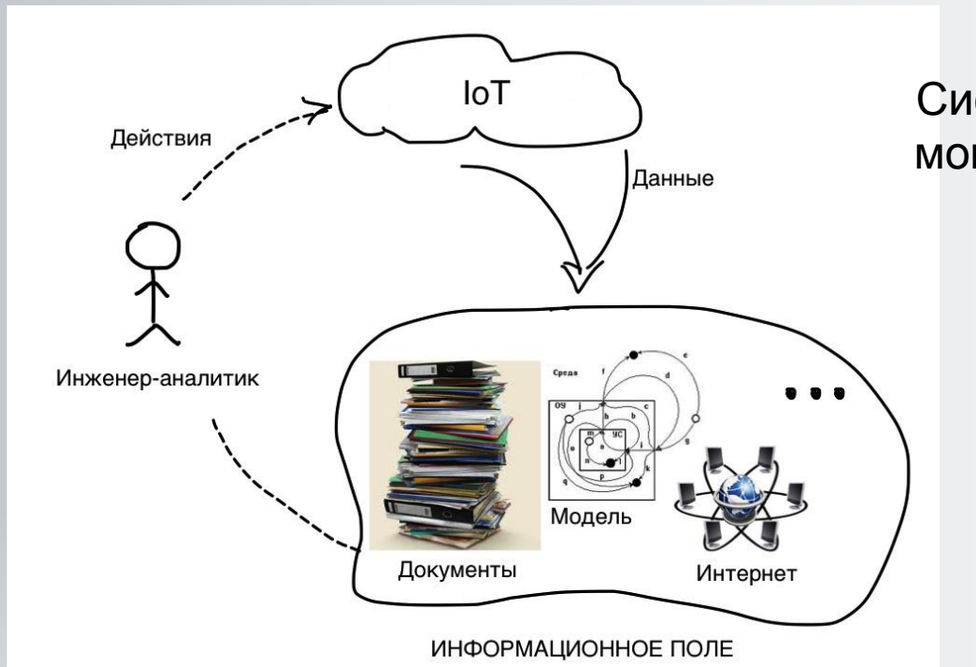
Как может работать/методы

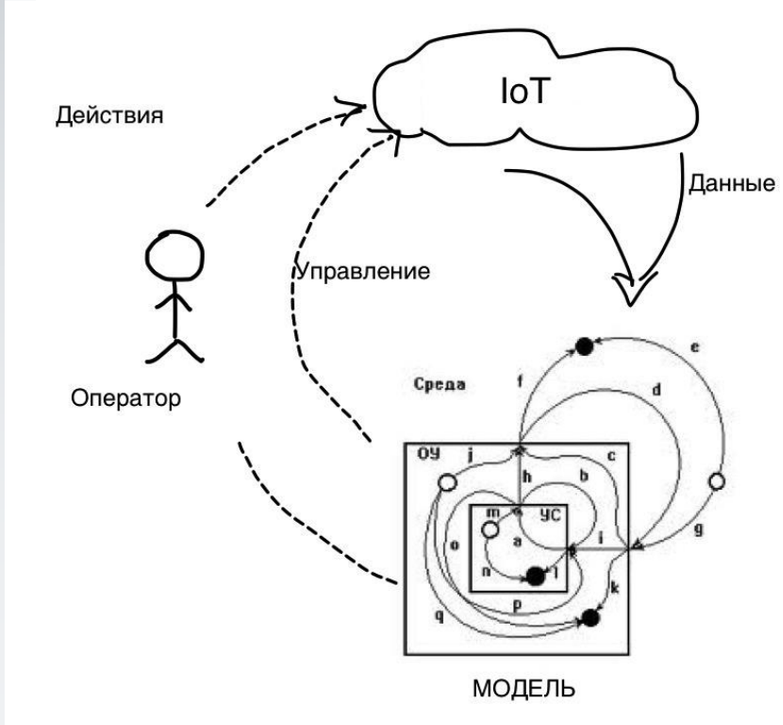
Уровни	Модели	Методы
«Кластер» 		"Система” +: • Нечеткие и дискретные динамические системы • Системы оценки и мониторинга
"Система" 		«Механизм» +: • Многоагентные системы • Системная динамика • Нечеткие когнитивные карты • Сетецентрические модели • Прогнозирование 4
"Механизм" 		«Узел» +: • Модель механизма (если есть) • Классификация • Иерархические системы • Адаптивное управление • Теория автоматического управления • Прогнозирование 3
"Узел" 		«Блок» +: • Модель прибора (если есть) • Кластерный анализ • Мат. статистика • Прогнозирование 2
«Блок» 		• Анализ отклонений • Прогнозирование 1

Новые аспекты кибербезопасности

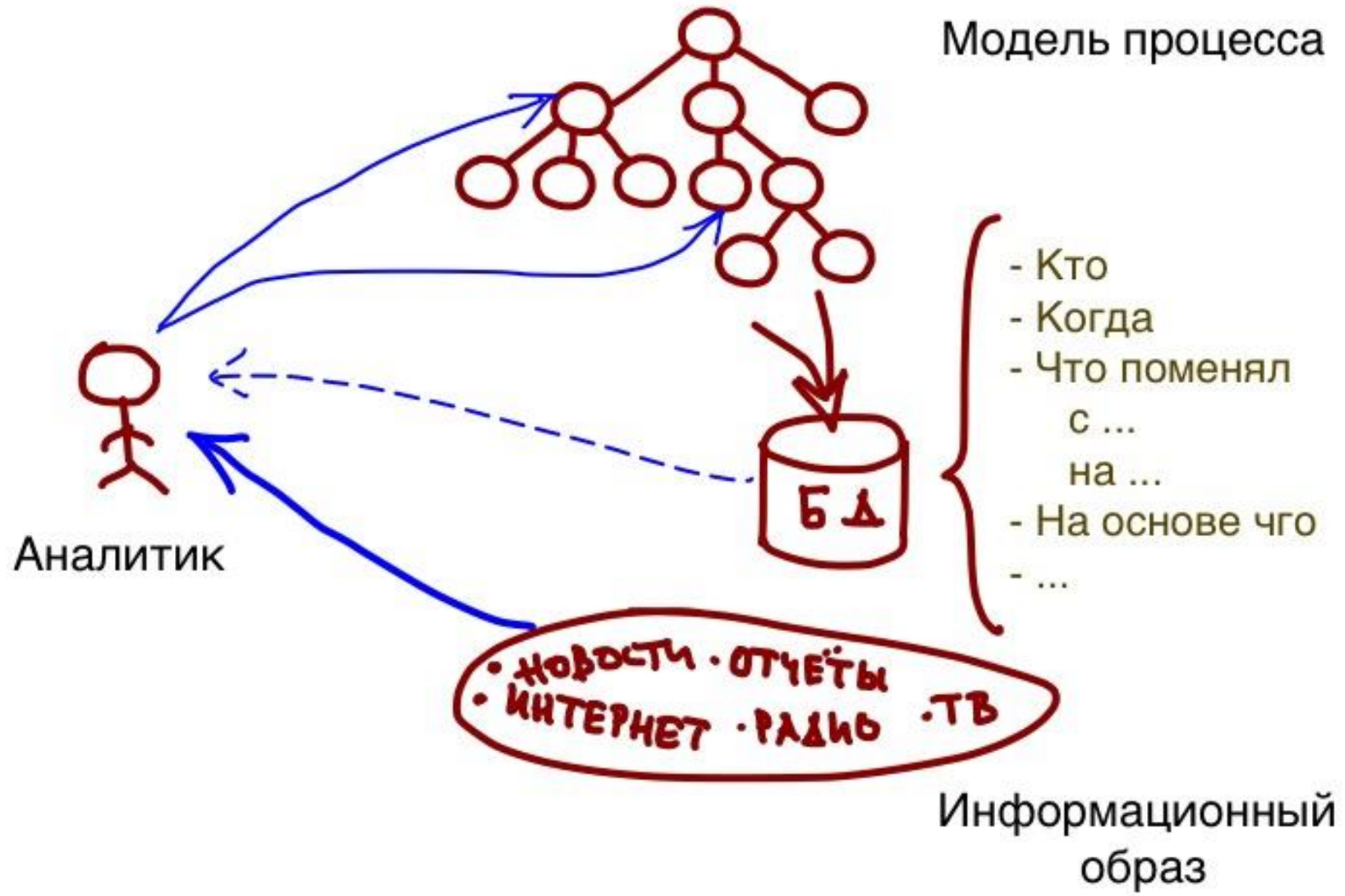
Как может работать/мониторинг

Уровни системы		Уровни контроля и управления	Уровни мониторинга
“Кластер”		CoMУ/ Ситуационный центр	Системный мониторинг
"Система"		ERP	
"Механизм"		SCADA	
"Узел"		АСУ ТП	
"Блок"		Контроллеры	
		Датчики	Технический мониторинг



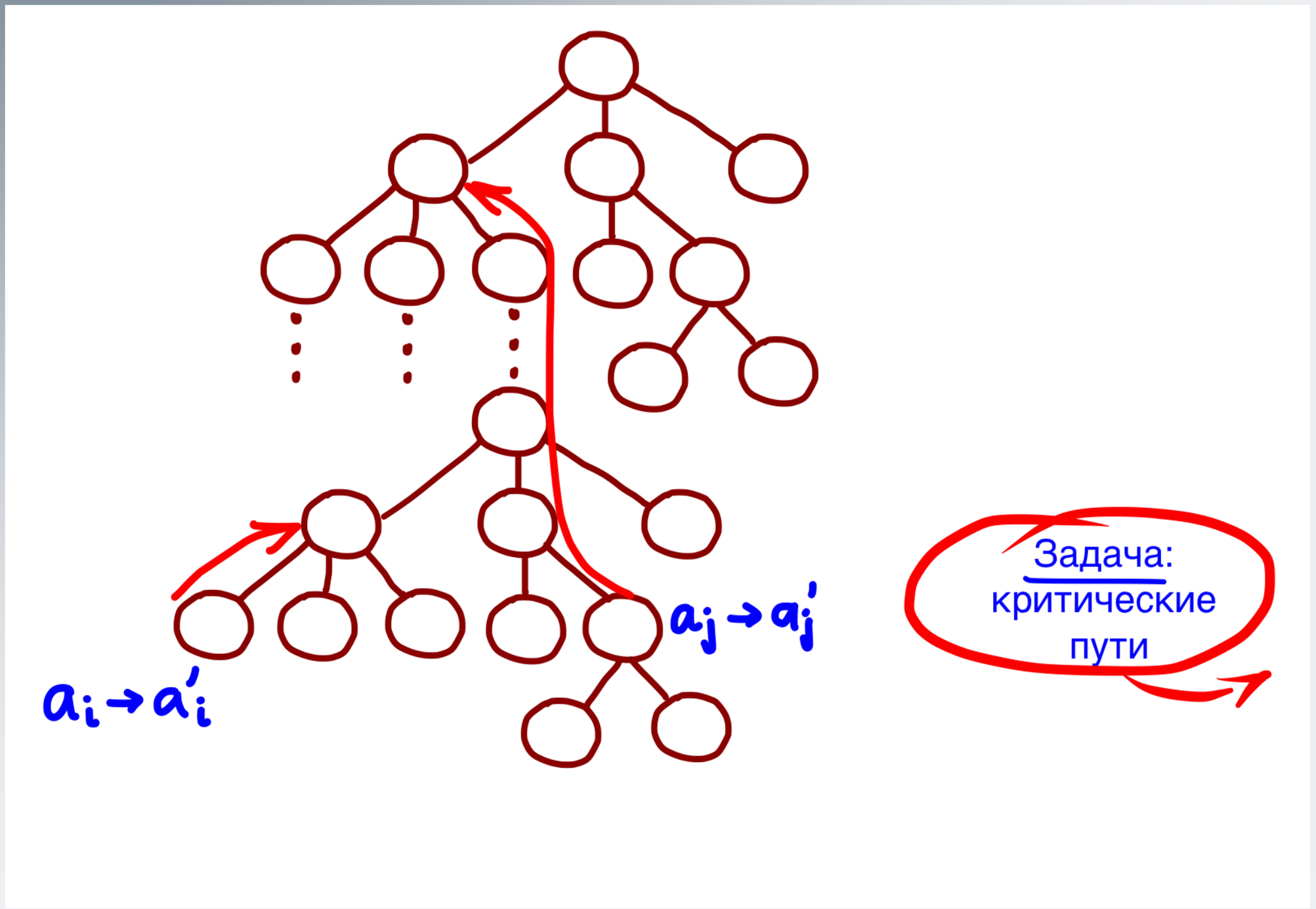


СОМУ: ввод информации

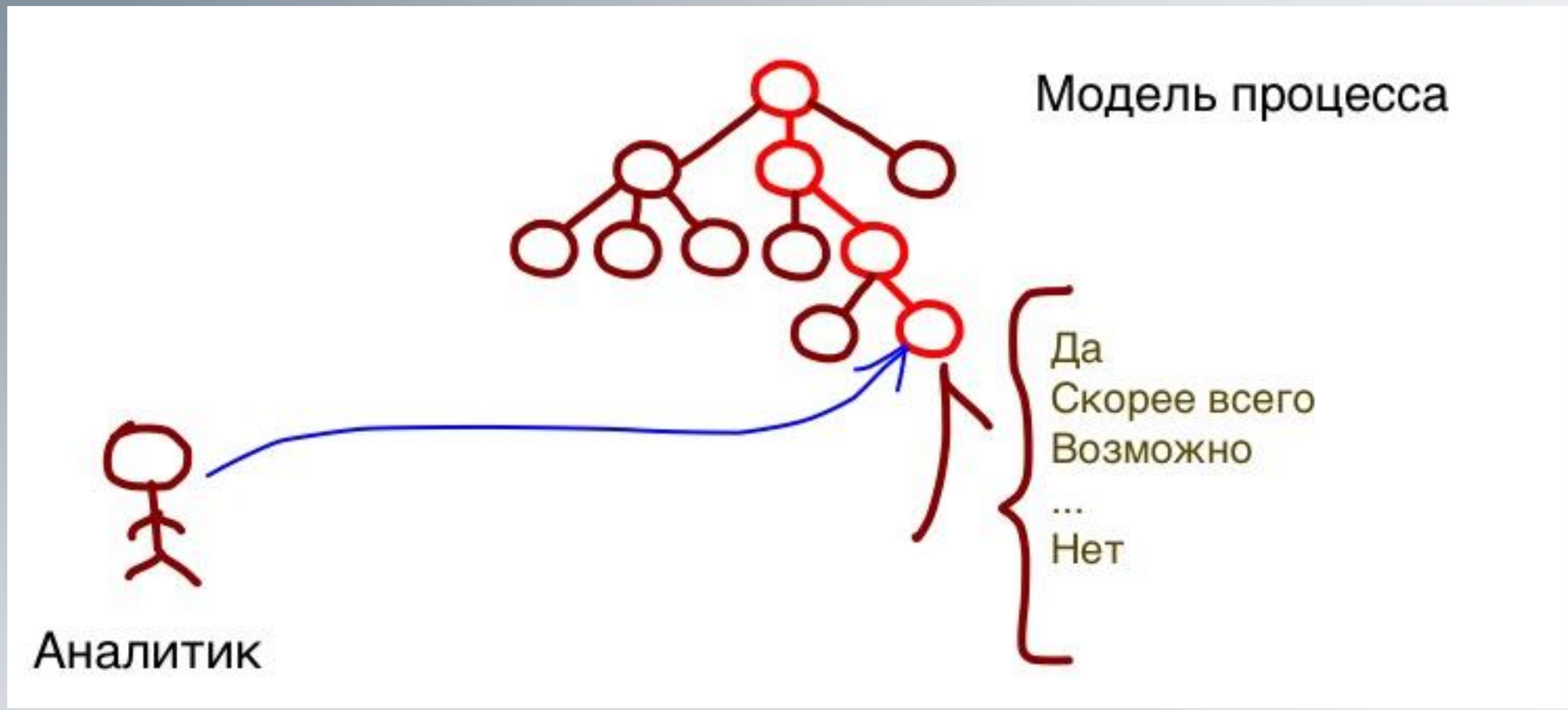


Результат:
Актуальные состояние процесса, подтвержденное ссылками на все доступные информационные материалы и измерения.

Анализ: прямая задача.



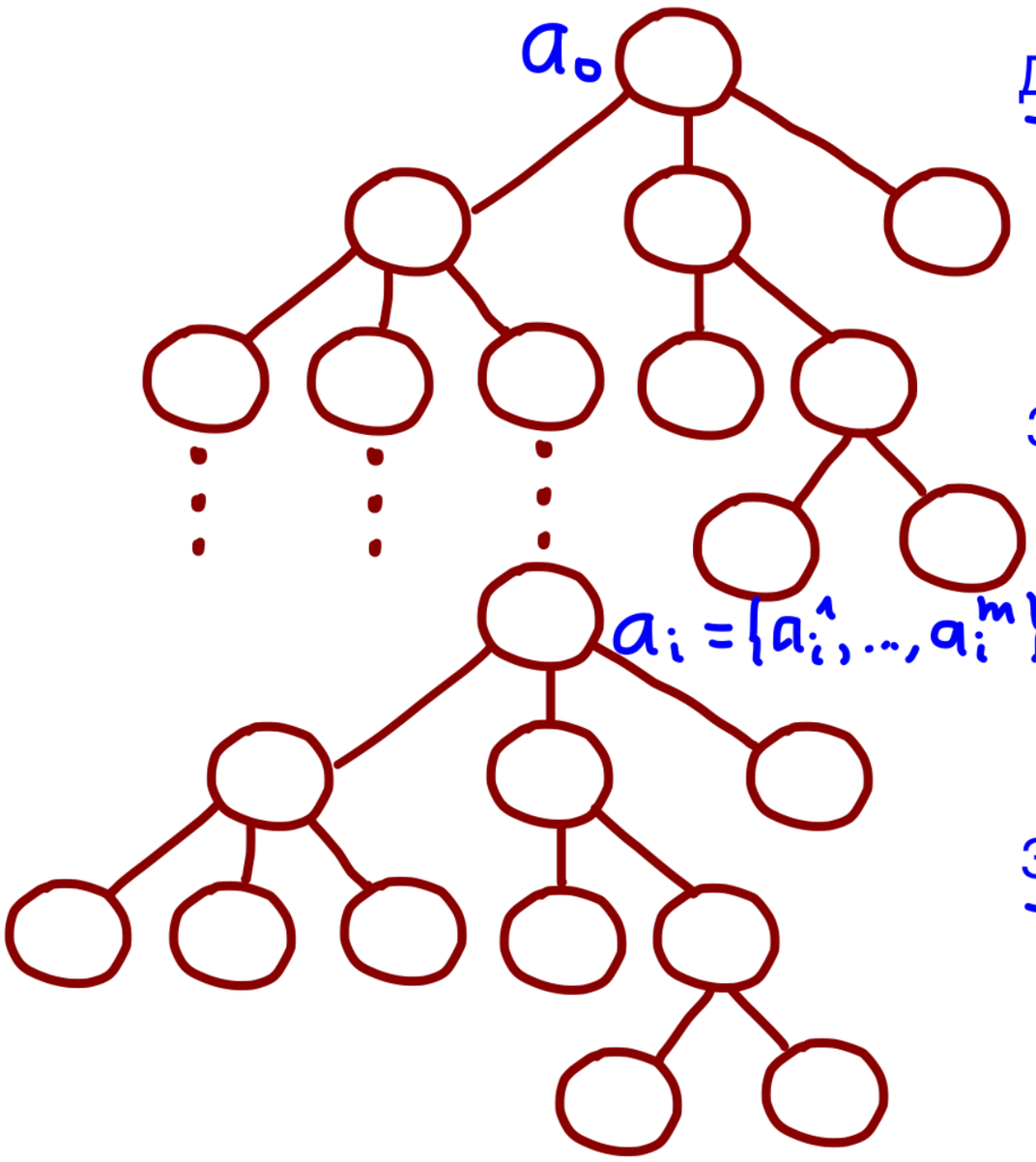
Прямая задача: критические пути.



Критический путь – малое изменение значения элемента вызывает изменение состояния всего процесса/проблемы.

Знание таких элементов имеет большое практическое значение и позволяет выявить "слабые места" в процессе/проблеме на текущий момент времени, разработать мероприятия по блокированию нежелательных ситуаций или провоцированию желательных, т.е. управлять развитием процесса/проблемы обеспечения безопасности IoT.

Анализ: обратная задача.



Дано: (1) X - бюджет

(2) $\Delta C_i = C(a_i^k \to a_i^{k+1})$

- стоимость изменения

Задача 1: Найти $\{a_{i_1}, .., a_{i_n}\}$:

$$\Delta a_0 \to max,$$

$$\sum_{j=1}^{n} \Delta c_{ij} \leq X$$

Максимальный эффект за данный бюджет

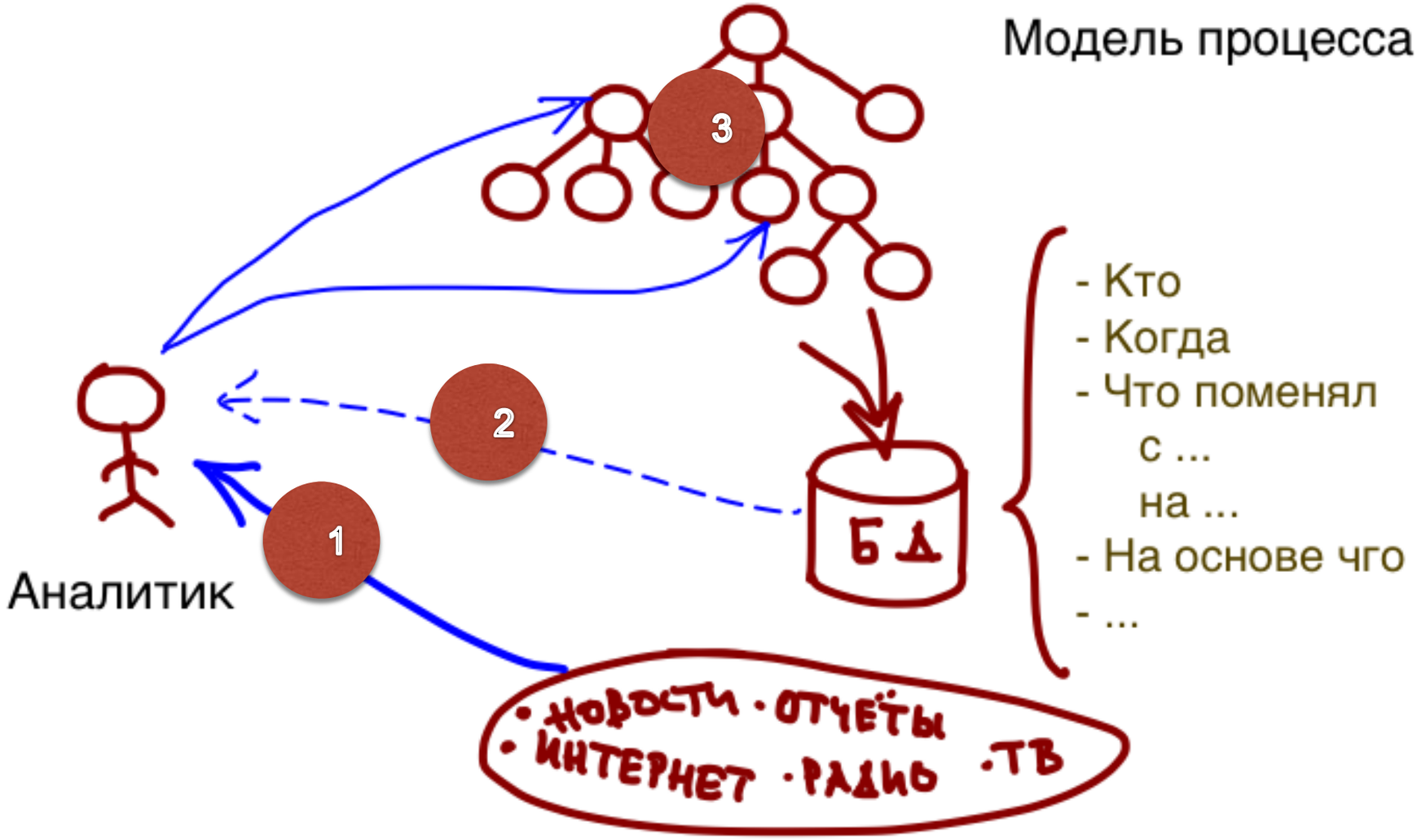
Задача 2: Найти $\{a_{i_1}, .., a_{i_n}\}$:

$$\sum_{j=1}^{n} \Delta c_{ij} \to min$$

$$\Delta a_0 \geqslant \Delta a_0^*$$

Заданный эффект за минимальный бюджет

Проблемы разработки СОМУ



Проблемы 1-3 решены.
Доказана устойчивость – можно применять в практических задачах.

Проблема 1

Можно ли, учитывая некоторые особенности восприятия человеком объектов реального мира и их описания, сформулировать правило выбора оптимального множества значений признаков, по которым описываются эти объекты? Возможны два критерия оптимальности:

- Критерий 1. Под оптимальными понимаются такие множества значений, используя которые человек испытывает минимальную неопределенность при описании объектов.

- Критерий 2. Если объект описывается некоторым количеством экспертов, то под оптимальными понимаются такие множества значений, которые обеспечивают минимальную степень рассогласования описаний.

Проблема 1: результаты

- Показано [Рыжов, 1985] , что мы можем сформулировать методику выбора оптимального множества значений качественных признаков.
- Более того, показано [Рыжов, 1991] , что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений.
- Множества, оптимальные по критериям 1 и 2 совпадают.

http://intsys.msu.ru/staff/ryzhov/FuzzySetsTheoryApplications.htm

Проблема 2

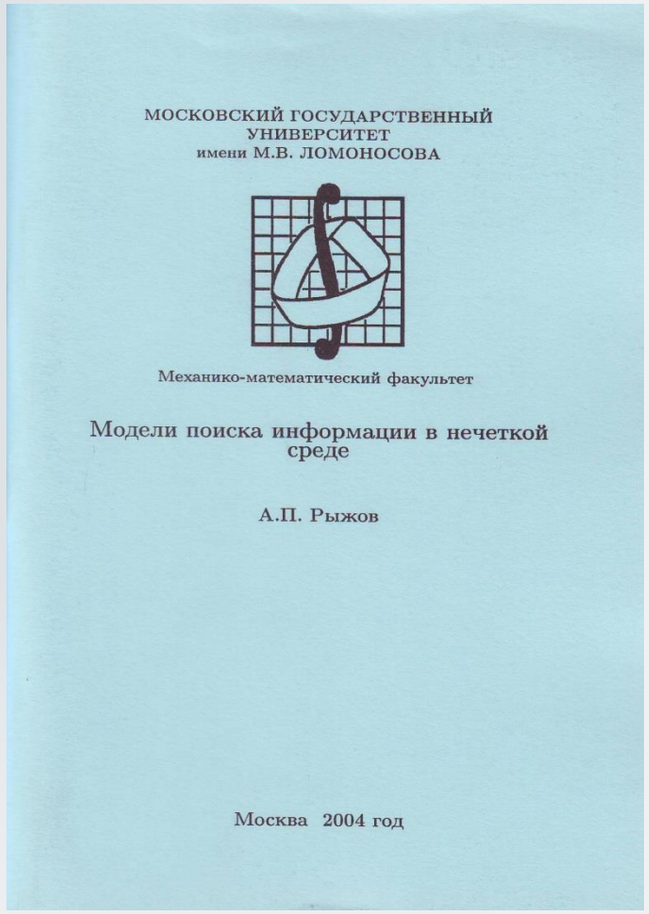
Можно ли определить показатели качества поиска информации в нечетких (лингвистических) базах данных и сформулировать правило выбора такого множества лингвистических значений, использование которого обеспечивало бы максимальные показатели качества поиска информации?

Проблема 2: результаты

- Показано [Рыжов, 1992] , что можно ввести показатели качества поиска информации в нечетких (лингвистических) базах данных и формализовать их.

- Показано [Рыжов, 1992], что возможно сформулировать методику выбора оптимального множества значений качественных признаков, которое обеспечивает максимальные показатели качества поиска информации.

- Более того, показано [Рыжов, 1993], что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений.


МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Механико-математический факультет

Модели поиска информации в нечеткой среде

А.П. Рыжов

Москва 2004 год

http://www.intsys.msu.ru/staff/ryzhov/FuzzyRetrieval2010.htm

Проблема 3

Можно ли предложить алгоритмы выбора операторов агрегирования информации в системах информационного мониторинга, обеспечивающие «настройку» системы на конкретную предметную область?

Проблема 3: результаты

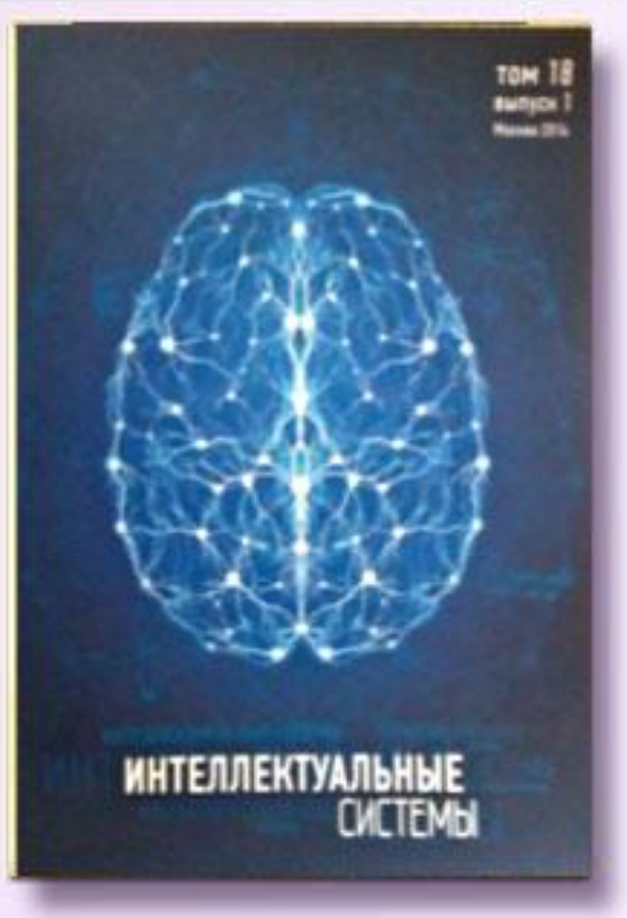
Разработаны подходы синтеза компонент облачного кластера на технологии Hadoop для решения задач идентификации и мониторинга кибер-атак [Назаров, 2015-2016 гг.]:

- Сформулированы требования к софту;
- Исследованы аспекты достаточности измерений.

Проблема 3: результаты

Выделяются следующие подходы к решению этой проблемы, базирующиеся на различных интерпретациях операторов агрегирования информации [Рыжов, 1996]:

- геометрический;
- логический;
- на основе обучения:
  - обучение на основе генетических алгоритмов
  - обучение на основе нейронных сетей.



Рыжов А.П. Об агрегировании информации в нечетких иерархических системах. Интеллектуальные системы, Том 6, Вып. 1-4, 2001, с. 341 - 364 - http://www.intsys.msu.ru/magazine/archive/v6(1-4)/ryzhov.pdf

Технология разработки СОМУ

СОМУ - совместный продукт

- Экспертов (Э),
- Математиков и аналитиков (М)
- Разработчиков ПО (Р)

Включает следующие этапы:

- концептуальная модель;
- исследовательский демонстратор;
- демонстратор СОМУ IoT;
- система.

Технология разработки СОМУ: этапы

СОМУ - совместный продукт

- Экспертов (Э),
- Математиков и аналитиков (М)
- Разработчиков ПО (Р)

- Э / М / Р = 2 / 3 / 2
- Цель: система, способная решать реальную (возможно, упрощенную) задачу на основе реальной информации
- Результаты:
  - Прототип
  - Оценка применимости технологии
  - Уточненный план проекта
  - Начало пилотного использования
  - 30% - 40% стоимости проекта

- Э / М / Р = 1 / 1 / 3
- Цель: полномасштабная система
- Результат:
  - Внедренная система
  - Документация
  - Обученные пользователи
- 25% - 30% стоимости проекта

Концептуальная модель

Исследовательский прототип

Демонстрационный прототип

Система

- Э / М / Р = 3 / 2 / 1
- Цель: Постановка задачи
- Результаты:
  - Проект модели
  - Сценарии использования СИМ в организации заказчика
  - План проекта (этапы, ресурсы, сроки, и т.п.)
- 10% - 15% стоимости проекта

- Э / М / Р = 2 / 3 / 3
- Цель: система, реализующая все необходимые функции на всей модели проблемы
- Результаты:
  - Прототип
  - Организация опытной эксплуатации прототипа системы
  - Уточненный план проекта
  - 20% - 25% стоимости проекта

Резюме

- Функционал СОМУ:
  - Решают задачу оценки, мониторинга и управления рисками
  - Позволяют аналитику вводить информацию из всех доступных источников естественным образом
  - Хранят историю развития процесса, оценивают его текущее состояние, прогнозируют и моделируют будущее
- СОМУ эффективны:
  - Когда нет/ нельзя построить математическую модель процесса в виде уравнений, автоматов и пр.
  - Когда есть аналитики, решающие задачу оценки и мониторинга на систематической основе
- Разработка СОМУ возможна:
  - Когда можно построить семантическую модель процесса в виде набора понятий и их взаимосвязей
  - Поступает и анализируется реальная информация - возможны обучение и на стройка
- Возможна разработка оптимальных СОМУ с точки зрения (1) удобства ввода; (2) согласованности оценок (3) информационной поддержки ввода и моделирования

Предложение

- Использовать для решения задачи синтеза облачного сервиса класса IaaS для развертывания Интеллектуальной сети устройств защиты информации, предназначенной для контролируемого, защищённого взаимодействия устройств различных классов, относящихся к «Интернету вещей», с другими аналогичными устройствами или иными объектами «Интернет», технологию оценки и мониторинга сложных процессов:
  - Обеспечивает решение задач оценки и мониторинга рисков
  - Не требуется дорогой инфраструктуры (суперкомпьютеров и пр.)
  - Есть примеры использования этой технологии на международном и федеральном уровнях, в ведущих международных компаниях
  - Положительные заключения ведущих мировых экспертов

Примеры СОМУ в части мониторинга и оценки:

- Система мониторинга и оценки мирной ядерной деятельности стран в интересах управления обеспечения международных гарантий МАГАТЭ (Development of an Intelligent System for Monitoring and Evaluation of Peaceful Nuclear Activity, IAEA, Vienna, STR-310);
- Система «Мониторинг - 1» (НИЦ «Контур» ФАПСИ).
- Система оценки и мониторинга производства изделий микроэлектроники (Cadence Design Systems)

Новые аспекты кибербезопасности

МАГАТЭ

Microsoft Excel - Модель.МАГАТЭ.XLS

Файл Правка Вид Вставка Формат Сервис Данные Окно Справка Введите вопрос

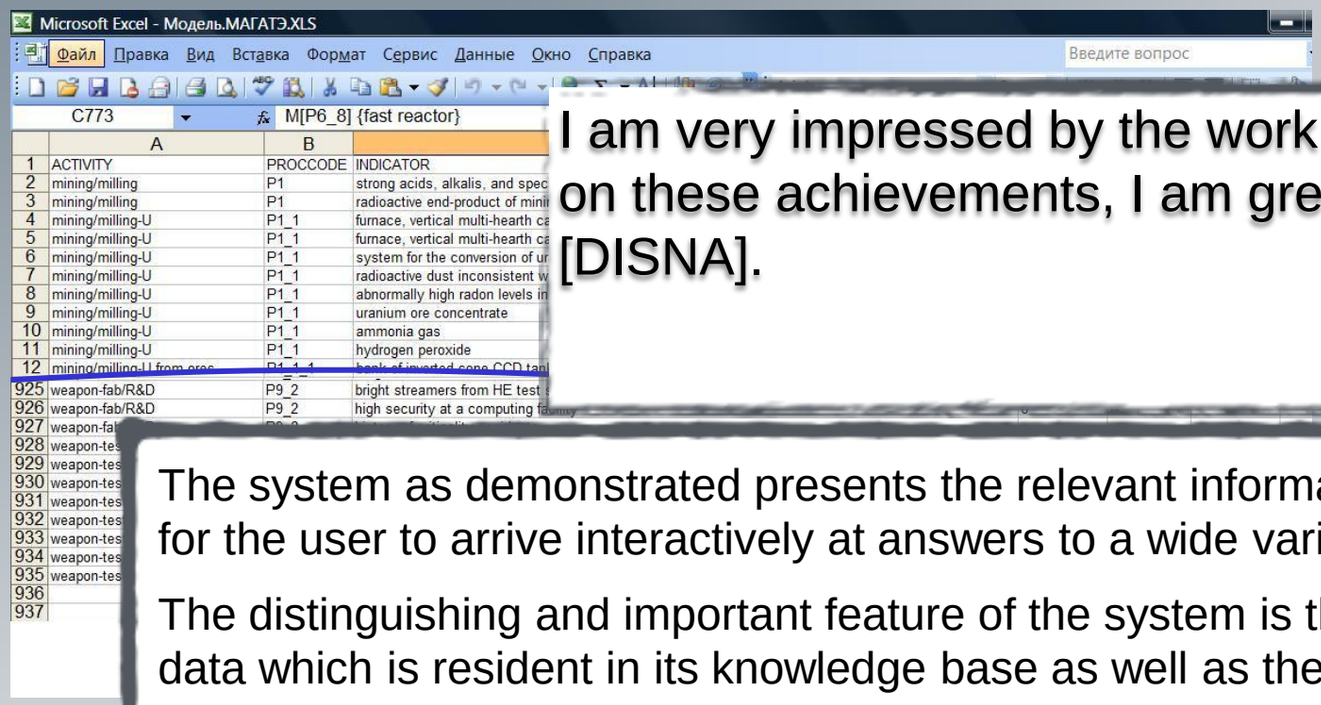
Arial 8

C773 M[P6_8] {fast reactor}

	A	B	C	D	E	F	
1	ACTIVITY	PROCCODE	INDICATOR	TYPE	STRENGTH	REFDOC	REF
2	mining/milling	P1	strong acids, alkalis, and specialized solvents	env	m		
3	mining/milling	P1	radioactive end-product of mining/milling process	nm	s	254/pt 1a	1.1
4	mining/milling-U	P1_1	furnace, vertical multi-hearth calciner	d	m		
5	mining/milling-U	P1_1	furnace, vertical multi-hearth calciner (if no known Al industry)	d	s		
6	mining/milling-U	P1_1	system for the conversion of uranium ore concentrate	e	w	254/pt 1b	7.1
7	mining/milling-U	P1_1	radioactive dust inconsistent with local soils	env	m		
8	mining/milling-U	P1_1	abnormally high radon levels in air	env	w		
9	mining/milling-U	P1_1	uranium ore concentrate	nm	s	254/pt 1a	1.1
10	mining/milling-U	P1_1	ammonia gas	nnm	w		
11	mining/milling-U	P1_1	hydrogen peroxide	nnm	w		
12	mining/milling-U from ores	P1_1_1	bank of inverted-cone CCD tanks	d	m		
925	weapon-fab/R&D	P9_2	bright streamers from HE test shots indiating the use of DU as a dummy core				
926	weapon-fab/R&D	P9_2	high security at a computing facility	o	w		
927	weapon-fab/R&D	P9_2	history of criticality accidents	o	w		
928	weapon-test	P9_3	coaxial or fiber optic cable, large quantities	d	m	na	
929	weapon-test	P9_3	electronic streak or framing camera	d	m	254/pt 2	5.4
930	weapon-test	P9_3	oscilloscopes, large quantity	d	m	na?	
931	weapon-test	P9_3	photomultiplier tube	d	m	254/pt 2	7.2
932	weapon-test	P9_3	pulse generator, high-speed	d	m	254/pt 2	7.3
933	weapon-test	P9_3	oscilloscope or tansient recorder	d	w	254/pt 2	7.1
934	weapon-test	P9_3	vibration test equipment	d	w	254/pt 2	1.7
935	weapon-test	P9_3	drilling rigs or mining operations under tight security in remote location	o	s		
936							
937							

Новые аспекты кибербезопасности

МАГАТЭ



I am very impressed by the work done up to now in a rather short time and, base on these achievements, I am greatly in favor of a continuation of this project [DISNA].

E.E. Kerre, University of Ghent

The system as demonstrated presents the relevant information in a user-friendly form and makes it possible for the user to arrive interactively at answers to a wide variety of queries.

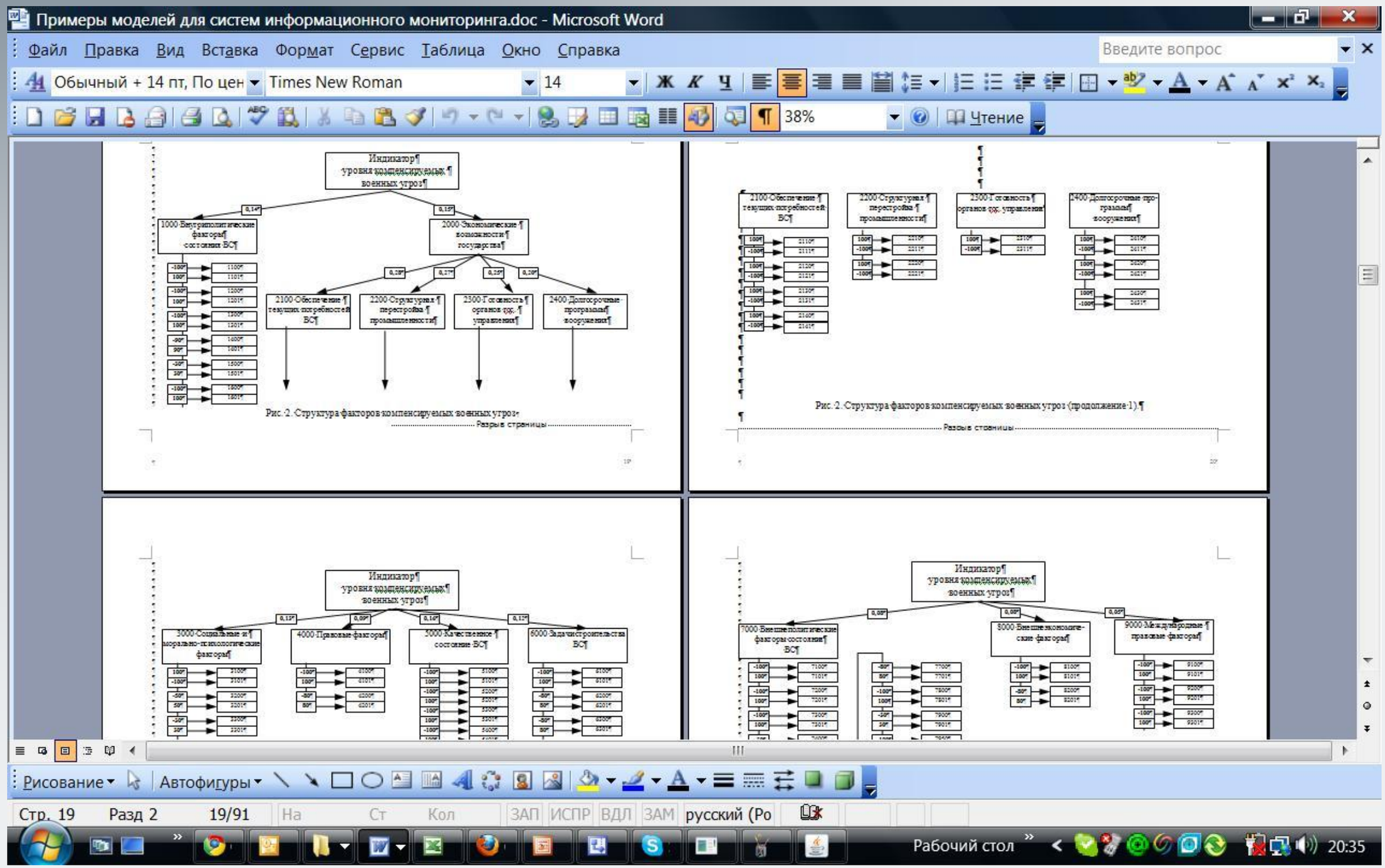
The distinguishing and important feature of the system is that it can process both numerical and linguistic data which is resident in its knowledge base as well as the data supplied by the user. The underlying theory reflects latest advances in methods of processing and aggregation of information which is uncertain, imprecise, incomplete or lacking in reliability.

This system is certainly not a toy system. In summary, my assessment of the DISNA Program is very positive. It gives me great pleasure to have an association with it.

Lotfi Zadeh,
Professor in the Graduate School and Director
Berkeley Initiative in Soft Computing (BISC)
Computer Science Division
Department of EECS
729 Soda Hall # 1776
Berkeley, CA 94720-1776, USA

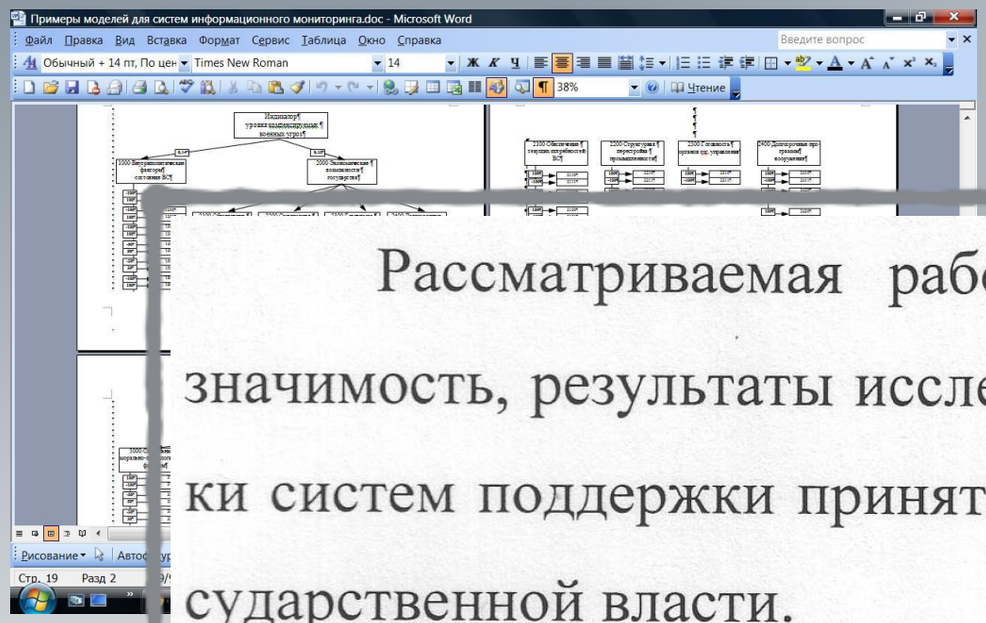
Новые аспекты кибербезопасности

Оценка и мониторинг рисков…



Новые аспекты кибербезопасности

Оценка и мониторинг рисков…



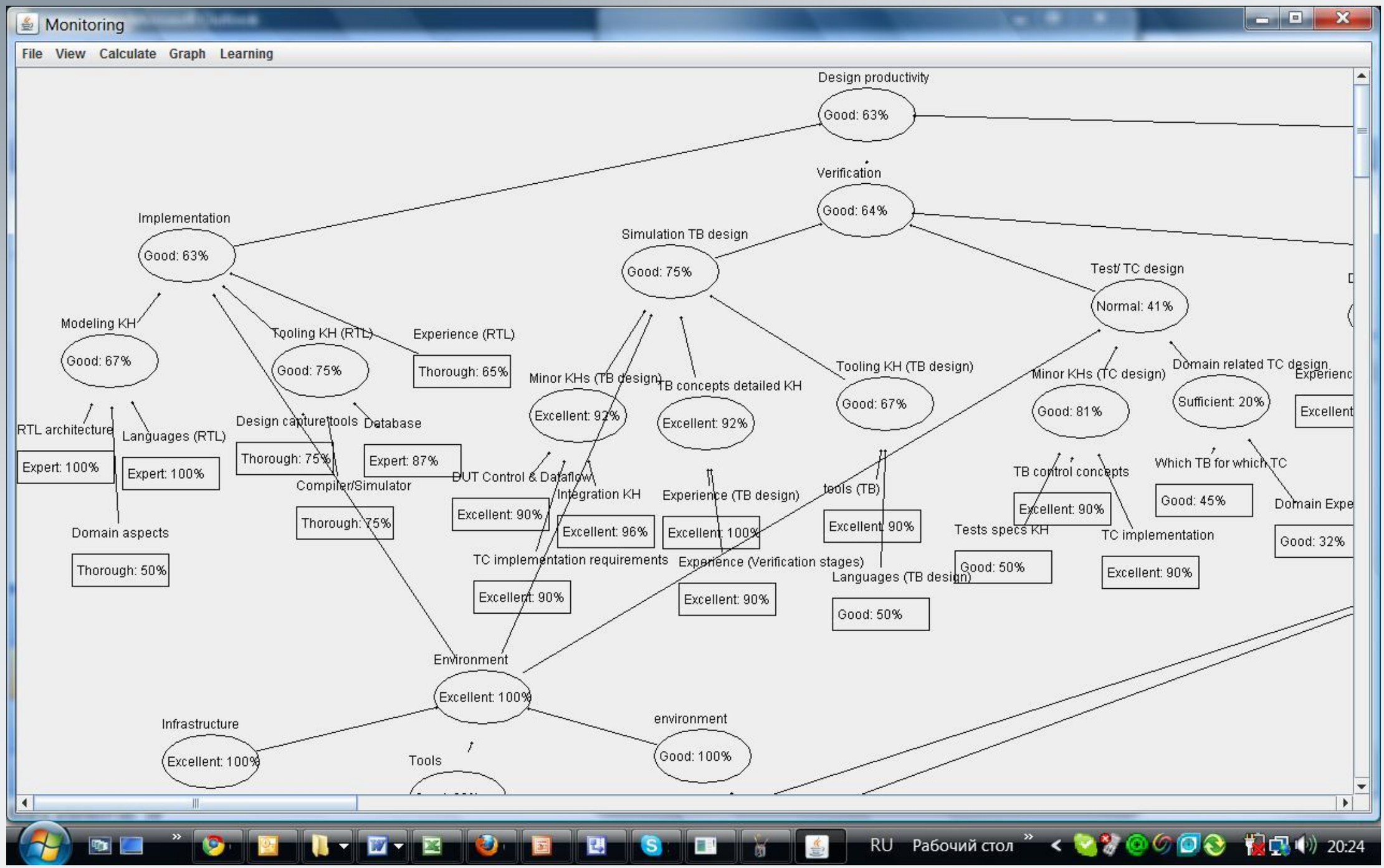
Рассматриваемая работа имеет значительную научно-практическую значимость, результаты исследования могут быть использованы для разработки систем поддержки принятия решений в ситуационных центрах органов государственной власти.

Советник Управления информационных систем
Спецсвязи ФСО России,
доктор технических наук

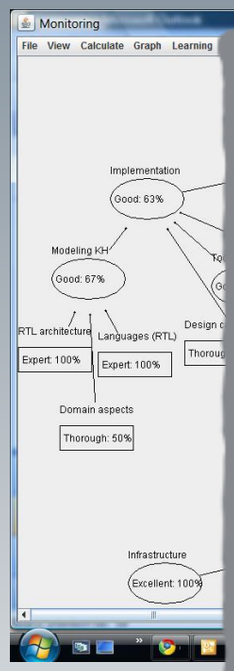
Н.Н. Демидов

16.10.2007г.

Оценка и мониторинг проектов в микроэлектронике



Оценка и мониторинг проектов в микроэлектронике



В течение 2005-2006 гг. Российским и Германским отделениями компании проводились работы по проекту «Оценка и мониторинг проектирования изделий микроэлектроники» в интересах группы Cadence VCAD (виртуальный САПР Cadence). Целью работ была разработка автоматизированной системы оценки способности конкретного коллектива разработчиков выполнить проект в необходимое время с требуемым качеством при заданном ресурсном обеспечении и сопровождения процесса проектирования.

Экспертами компании были проанализированы различные технологии для разработки такой системы и в качестве базовой выбрана технология информационного мониторинга, разработанная А.П. Рыжовым.

мов. Успешный ход проекта подтвердил их адекватность и применимость в области оценки и мониторинга разработки высокотехнологических изделий.

Генеральный директор
Cadence Design Systems Russia А.Н. Комков

Новые аспекты кибербезопасности

Иерархия уровней интеллектуальной системы анализа и противодействия бот-атакам.

Иерархические уровни разработанной в рамках Сколковского проекта «Глобальная система противодействия неправомерным действиям в киберпространстве» (Соглашение по гранту Сколково № 87 от 02.11.2012г.) автоматизированной системы (АС) противодействия бот-атакам содержат следующие модули:

- системы нечётких продукционных правил, описывающих работу идентификатора с учётом экспертных оценок;
- нейронечёткую сеть, в структуре которой отражена система нечётких продукционных правил; чёткую самообучаемую нейросеть (НС) для решения задач классификации и кластеризации входных векторов.

Уровень идентификации деструктивных воздействий (ДВ), предназначенный для классификации по вектору признаков ДВ на элементы и узлы IoT, формируемых датчиками этих ДВ.

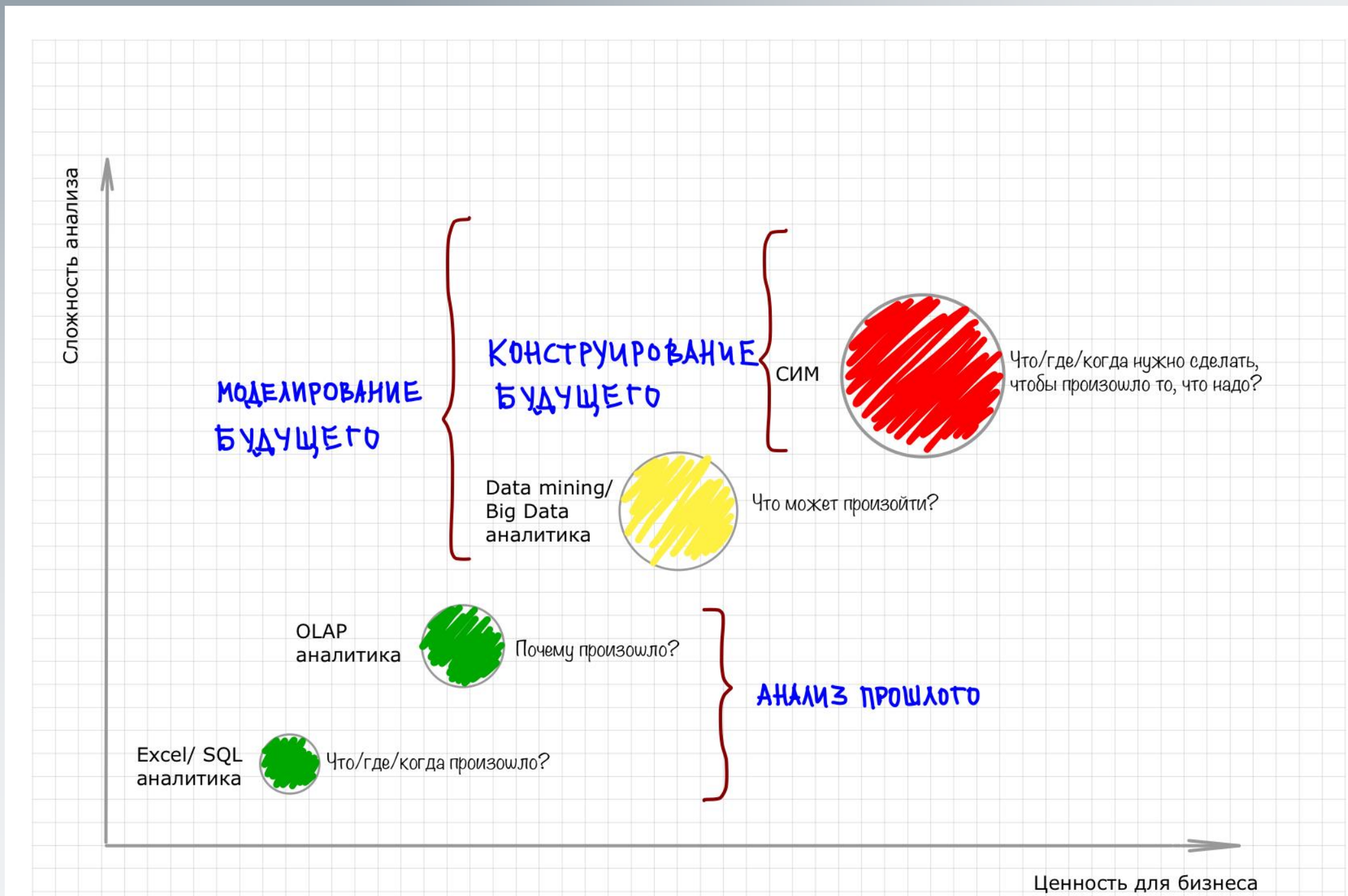
Новые аспекты кибербезопасности

Галушкин А.И.,Назаров А.Н. и др. Проект РФФИ №14-47-01574 2014г. по теме «Исследование вопросов автоматизации процедур мониторинга в web-пространстве на основе нейро-нечеткого формализма».

Приложение.
Близкие технологии

- Системная динамика
  - Автором является проф. Джей Форрестер (Jay Wright Forrester), MIT.
  - Трудоемкость разработки, настройки и верификации (параметрические модели элементов)
  - Нет обработки информационного потока (модель верхнего уровня)
- Нечеткие когнитивные карты
  - Автором является проф. Барт Кошко (Bart Andrew Kosko), USC
  - Нет обработки информационного потока (только подсистема моделирования)

Приложение. СОМУ и аналитика



Новые аспекты кибербезопасности

Личный состав лаборатории № 79

Зав. лабориторией - д.т.н., профессор Назаров Алексей Николаевич, эксперт ВАК, РАН, ITU.

Ведущий научный сотрудник – д.т.н., профессор Рыжов Александр Павлович, MBA.

Ведущий эксперт – Михалевич Игорь Феодосьевич, к.т.н., с.н.с.

Сакрутина Екатерина Алексеевна– научный сотрудник.

Аникина Евгения Владимировна, ведущий инженер

Новые аспекты кибербезопасности

Текущее планирование деятельности лаборатории № 79

Проект «Разработка технологии идентификации физических устройств и пользователей на основе анализа «следов», оставляемых ими в информационном пространстве». Заказчик Фонд перспективных исследований. Стадия доработки заявки.

Проект СВБУ АСУ ТП АЭС «Бушер». Главному конструктору представлены технические предложения по мониторингу кибер-атак. Стадия рассмотрения у Заказчика.

Программа фундаментальных исследований президиума РАН «Фундаментальные основы прорывных технологий в интересах национальной безопасности». Проект «Разработка методов, моделей и технологий интеллектуального анализа данных в сложных автоматизированных системах управления». Стадия подготовки отчётных материалов по этапу».

НИОКР по основам создания ведомственного сегмента ГосСОПКА Минтранса России. Стадия подготовки предложений по участию.

Спасибо за внимание.
Вопросы ?

Москва
2017