КОРРЕЛЯЦИЯ ДАННЫХ БЕЗОПАСНОСТИ В СЕТЯХ «ИНТЕРНЕТ ВЕЩЕЙ»

Д. Б. Смирнов[1], А. А. Чечулин[2]

[1]ЗАО «НПП «ТЕЛДА», [2]СПИИРАН,
Санкт-Петербург, Россия

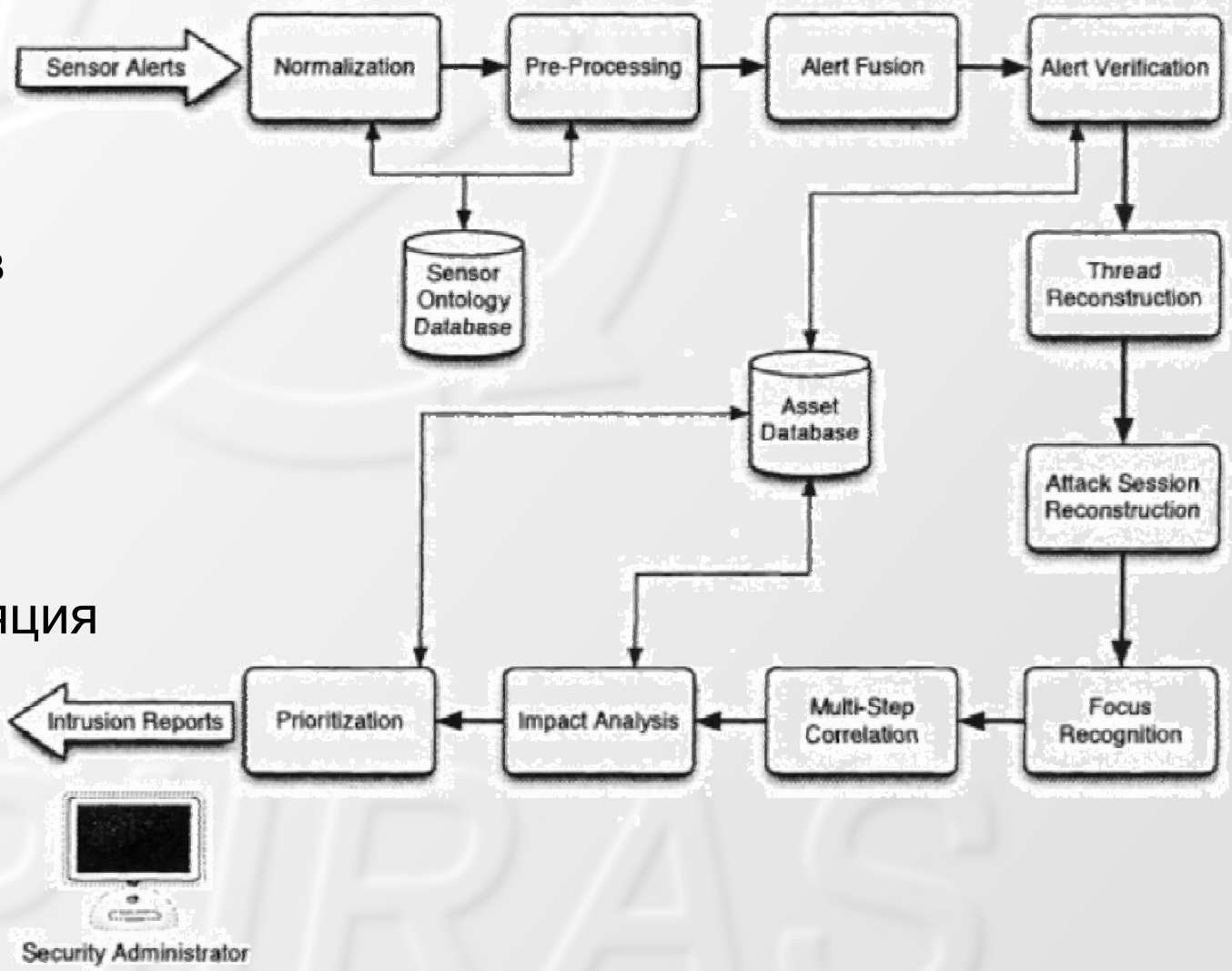
РусКрипто'2015, 17-20 марта 2015 г.

Интернет вещей

- Автомобили
  - Контроль двигателя, АКП, АБС …
- Связь
  - Коммутация, мобильные телефоны, маршрутизаторы, IP телефония, КПК …
- Бытовая техника
  - Телевизоры, холодильники, СВЧ печи …
- Коммерческая техника
  - Автоматизированный контроль, кассовые аппараты, системы управления запасами…
- Системы защиты
  - Контроль периметра, видеокамеры, проверка пропусков…

Общая последовательность действий при корреляции данных

- Нормализация
- Предобработка
- Генерация инцидентов
- Проверка инцидентов
- Выявление угроз
- Выявление атаки
- Определение целей
- Многошаговая корреляция
- Оценка ущерба
- Приоритезация

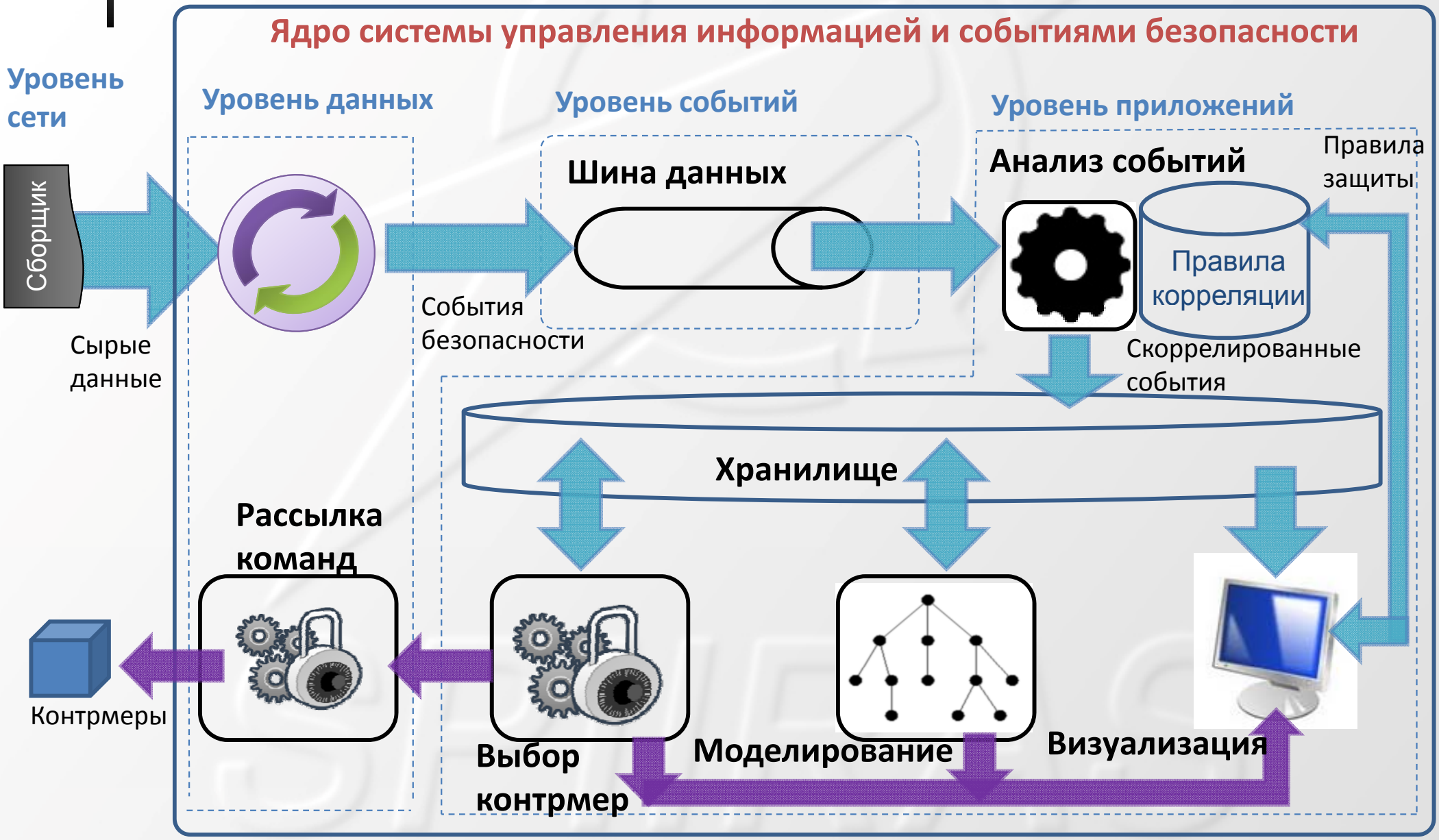


[Saeid Dadkhah, M. R. Khalili Shoja, Hassan Taheri, Alert Correlation through a Multi Components Architecture, 2013]

Действия выполняемые SIEM системой

- Получение и предобработка данных безопасности
  - Сбор данных от разнородных источников
  - Фильтрация и нормализация данных
- Корреляция данных безопасности
  - Детерминированные подходы
    - Правила
    - Конечные автоматы
    - Матрицы
  - Аномалии
    - Статистические подходы
    - Вероятностные подходы
- Контрмеры
  - Политики безопасности
  - Методы искусственного интеллекта
  - Онтологии

Общая архитектура SIEM системы

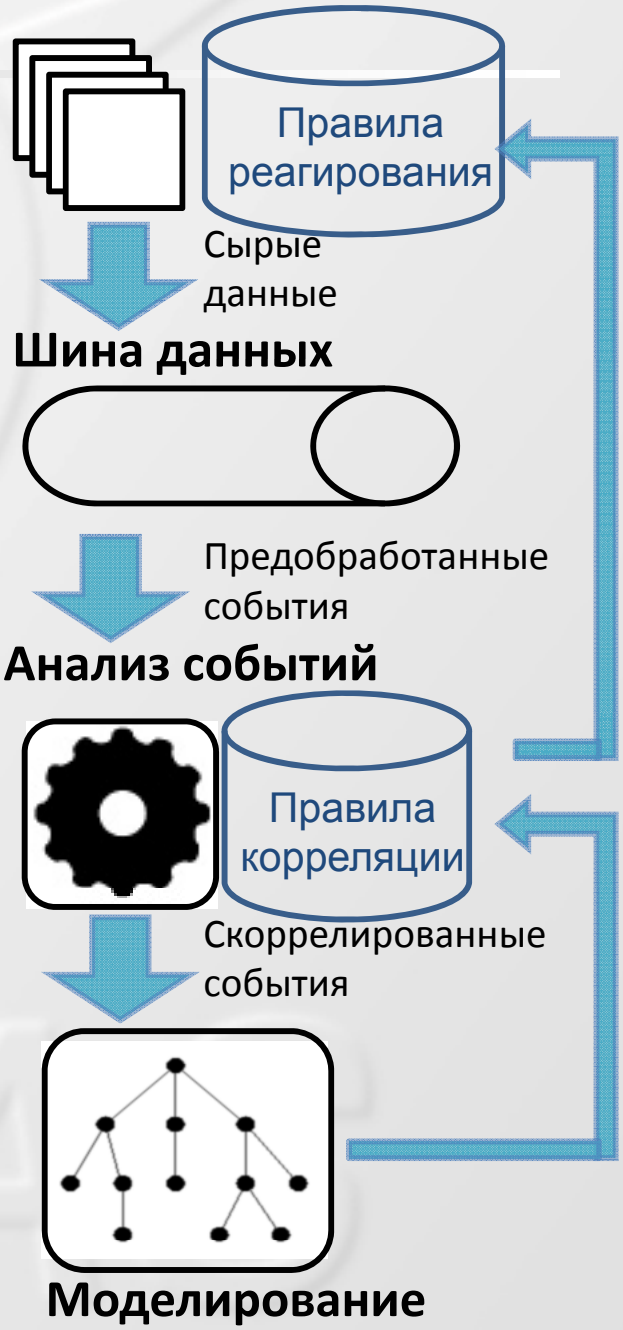


Дополнительные особенности Интернета вещей

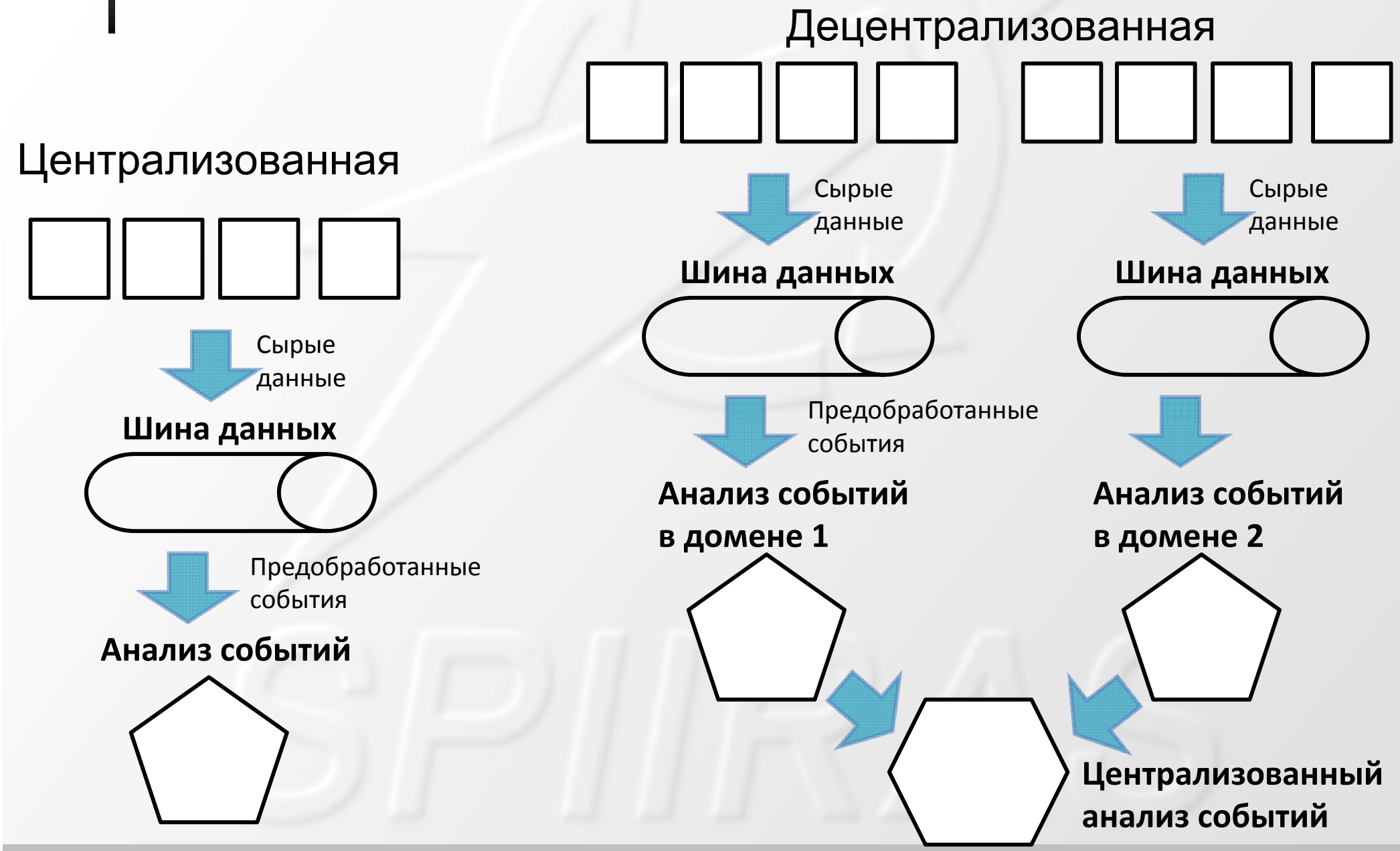
- Распределенная структура
  - Ограниченные возможности передачи данных
  - Необходимость верификации сообщений о событиях безопасности
- Недостаток вычислительных ресурсов на встроенных устройствах
  - Невозможность комплексного анализа событий безопасности на конечных устройствах
- Разнородность конечных устройств
  - Наличие устройств, которые невозможно перепрограммировать
  - Наличие узлов требующих непосредственного доступа в Интернет
  - Различная критичность узлов

Структура корреляции данных безопасности

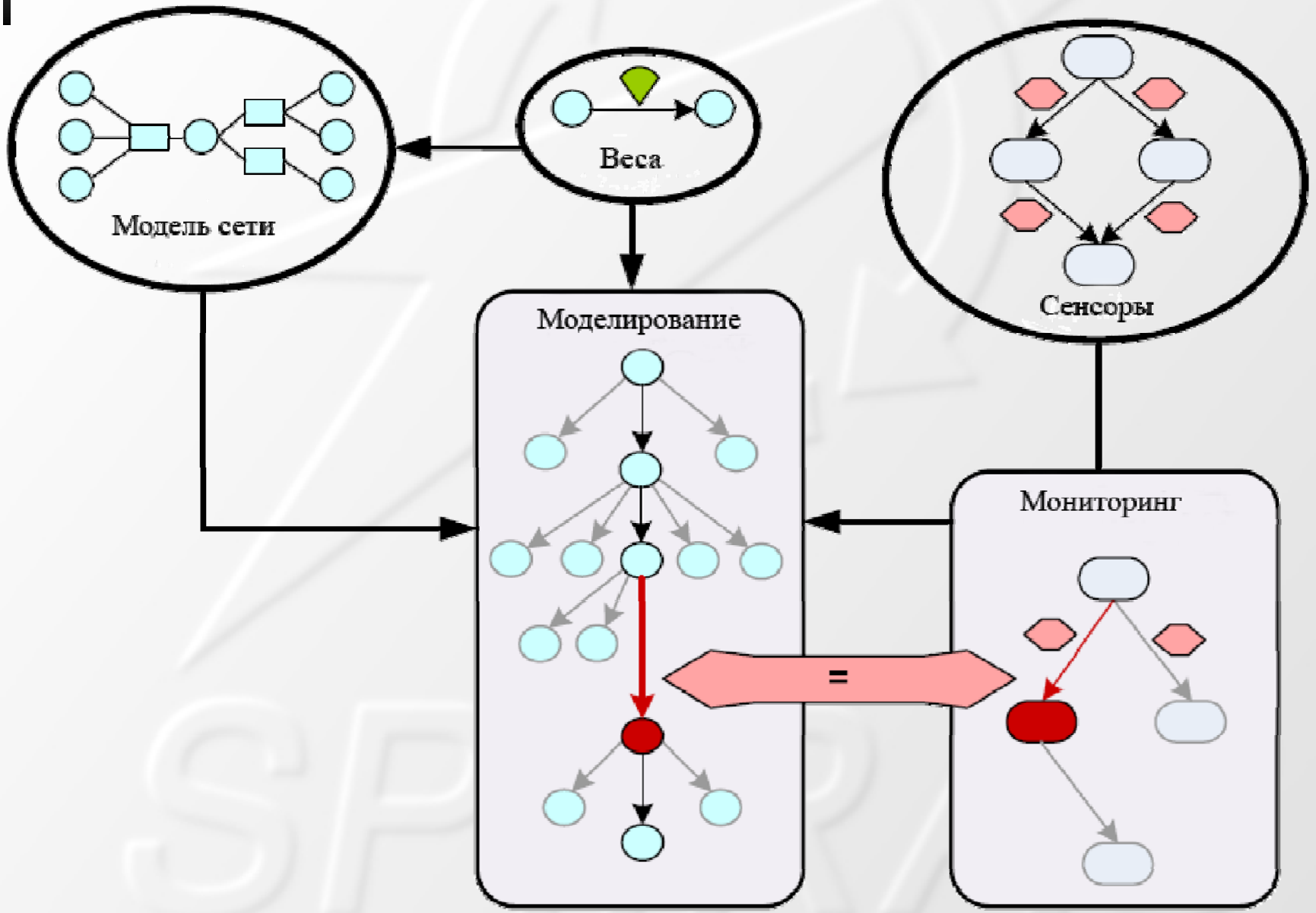
- Четыре уровня обработки событий
  - На уровне встроенного устройства
    - Фильтрация
    - Применение простых правил
    - Отправка в шину данных
  - В шине данных
    - Нормализация
    - Агрегация
    - Верификация
  - В подсистеме корреляции
    - Корреляция
    - Создание инцидентов безопасности
  - В подсистеме моделирования атак
    - Расширенный анализ инцидентов безопасности на основе сопоставления с графами атак
    - Обратная связь с системой корреляции



Архитектура системы корреляции



Анализ событий с помощью аналитического моделирования



Заключение

- Рассмотрены основные проблемы корреляции событий безопасности в сетях “Интернет вещей”
- Описан подход, позволяющий использовать моделирование атак для задачи корреляции событий безопасности
- Применение данного подхода позволит повысить уровень защищенности существующих сетей Интернета вещей

Контактная информация

Чечулин Андрей Алексеевич
chechulin@comsec.spb.ru
http://comsec.spb.ru/chechulin

Благодарности

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0033, уникальный идентификатор соглашения RFMEFI60414X0033; соглашение № 14.604.21.0137, уникальный идентификатор соглашения RFMEFI60414X0137; соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).