ОБРАБОТКА СОБЫТИЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РЕАЛЬНОГО ВРЕМЕНИ С ИСПОЛЬЗОВАНИЕМ ПОДХОДА, ОСНОВАННОГО НА АНАЛИЗЕ ДЕРЕВЬЕВ АТАК

Чечулин А.А., Котенко И.В.

Лаборатория проблем компьютерной безопасности Санкт-Петербургского Института Информатики и Автоматизации РАН

Санкт-Петербург, Россия

РусКрипто'2014, 25-28 марта 2014 г.

Зачем это нужно?

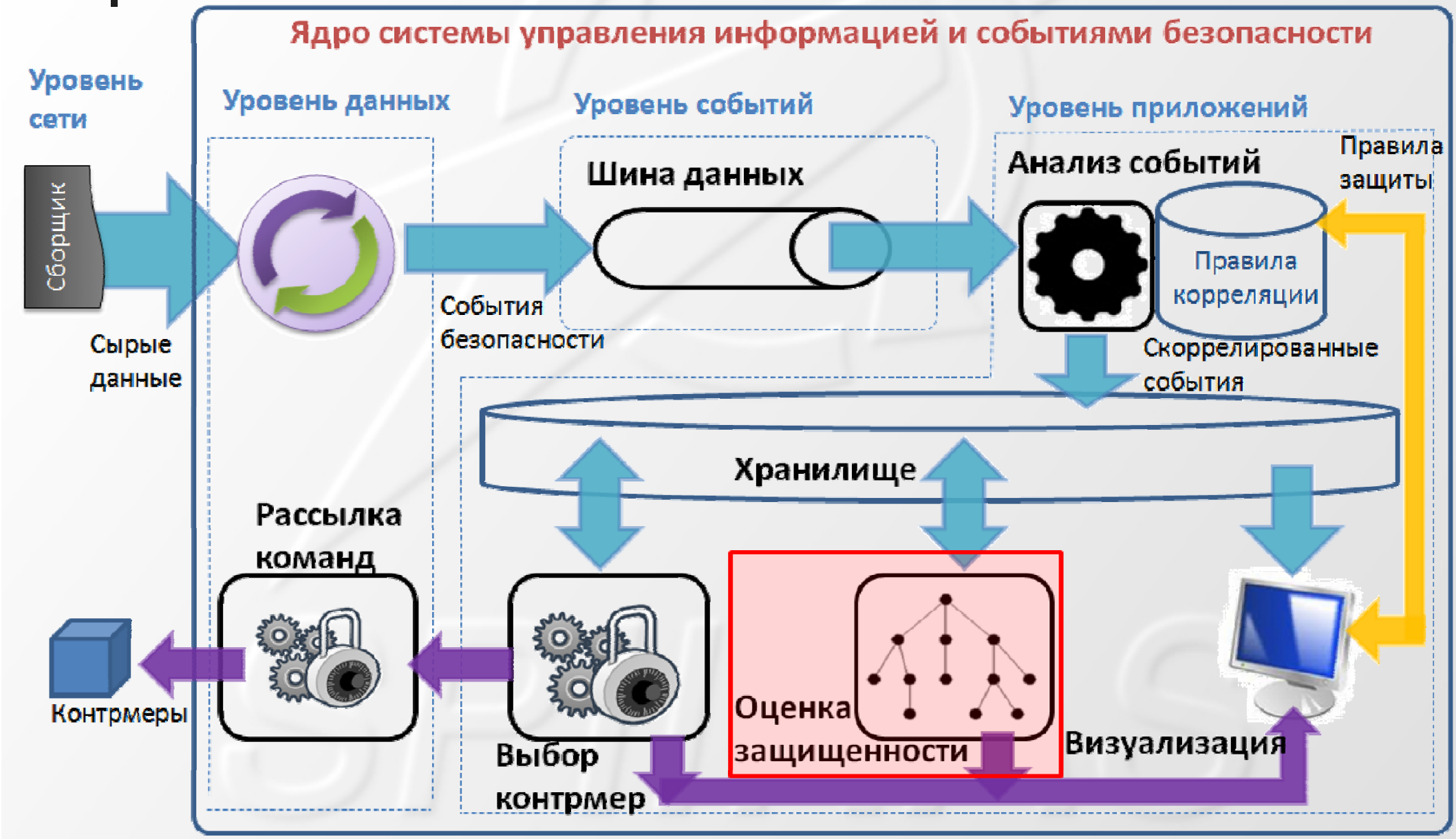
- Аналитическое моделирование атак - это медленный и ресурсоемкий процесс…
- Модель не может полностью описать реальную систему…
- Нарушитель не будет двигаться по заданному алгоритму, он придумает что-то свое…
- Моделирование не может точно предсказать эксплуатацию уязвимостей нулевого дня…
- Анализ деревьев атак может выдать только вероятностные значения возможных атак

– что с этим можно делать?

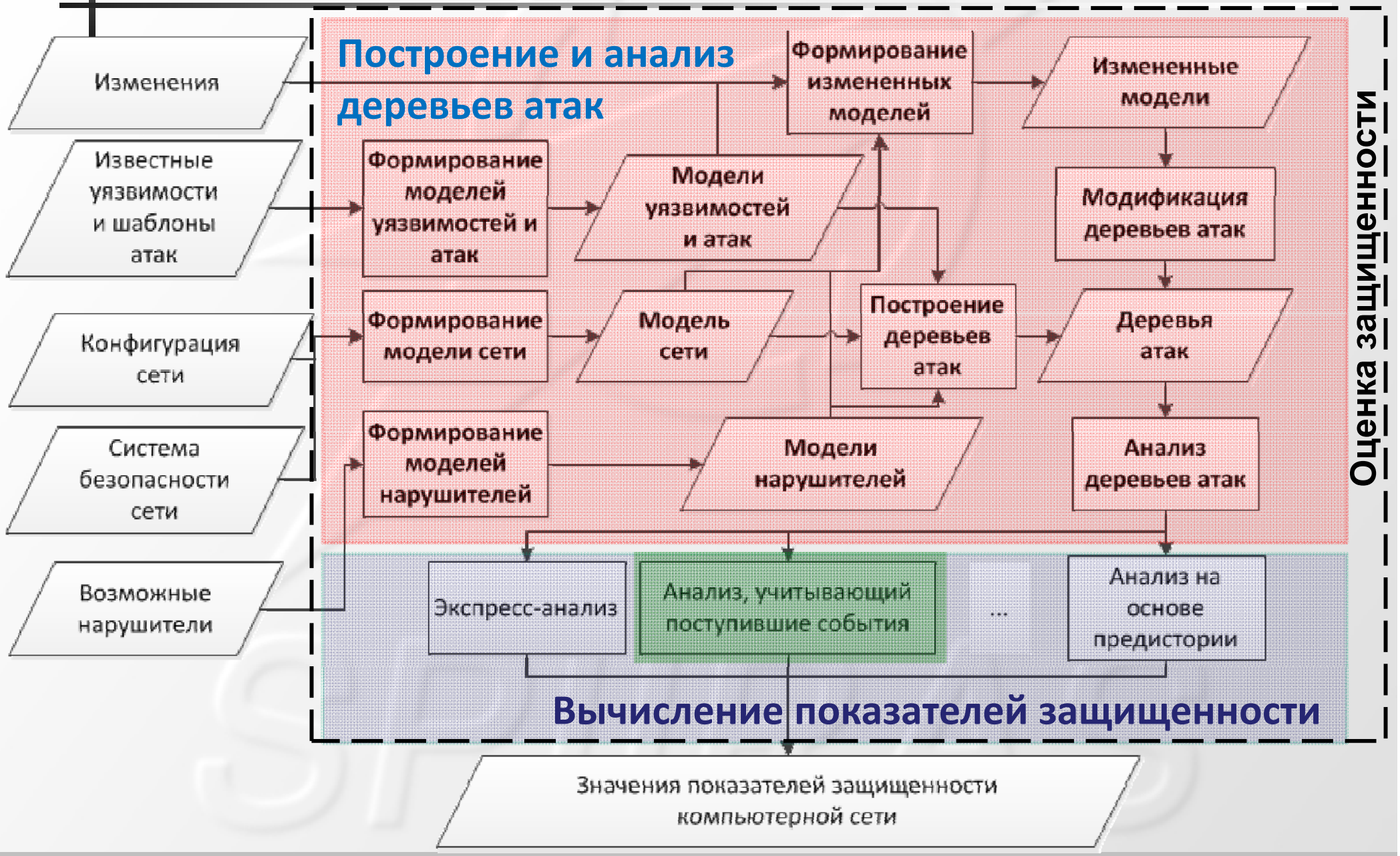
Основные подходы к построению и анализу деревьев атак

- Стандарты представления **уязвимостей, шаблонов атак** и **программно-аппаратных платформ** **[Мартин, 2013; …]**
- Подходы, описывающие различные **активные и пассивные способы сбора информации** о проблемах в системе защиты компьютерных сетей **[Nessus, 2013; Nmap, 2013, …]**
- Общая концепция построения и применения **деревьев атак** **[Шнайер, 1999;…]**
- Анализ возможных атак и их последствий с помощью **дискретного моделирования событий** **[Шоров, 2012,…]**
- Представление атак и активности легитимных пользователей как **упорядоченных во времени действий** **[Хейнеман, 2011,…]**
- Подход, основанный на автоматическом построении **деревьев атак** для автоматизированной оценки защищенности компьютерных сетей **[Степашкин, 2007; …]**
- …

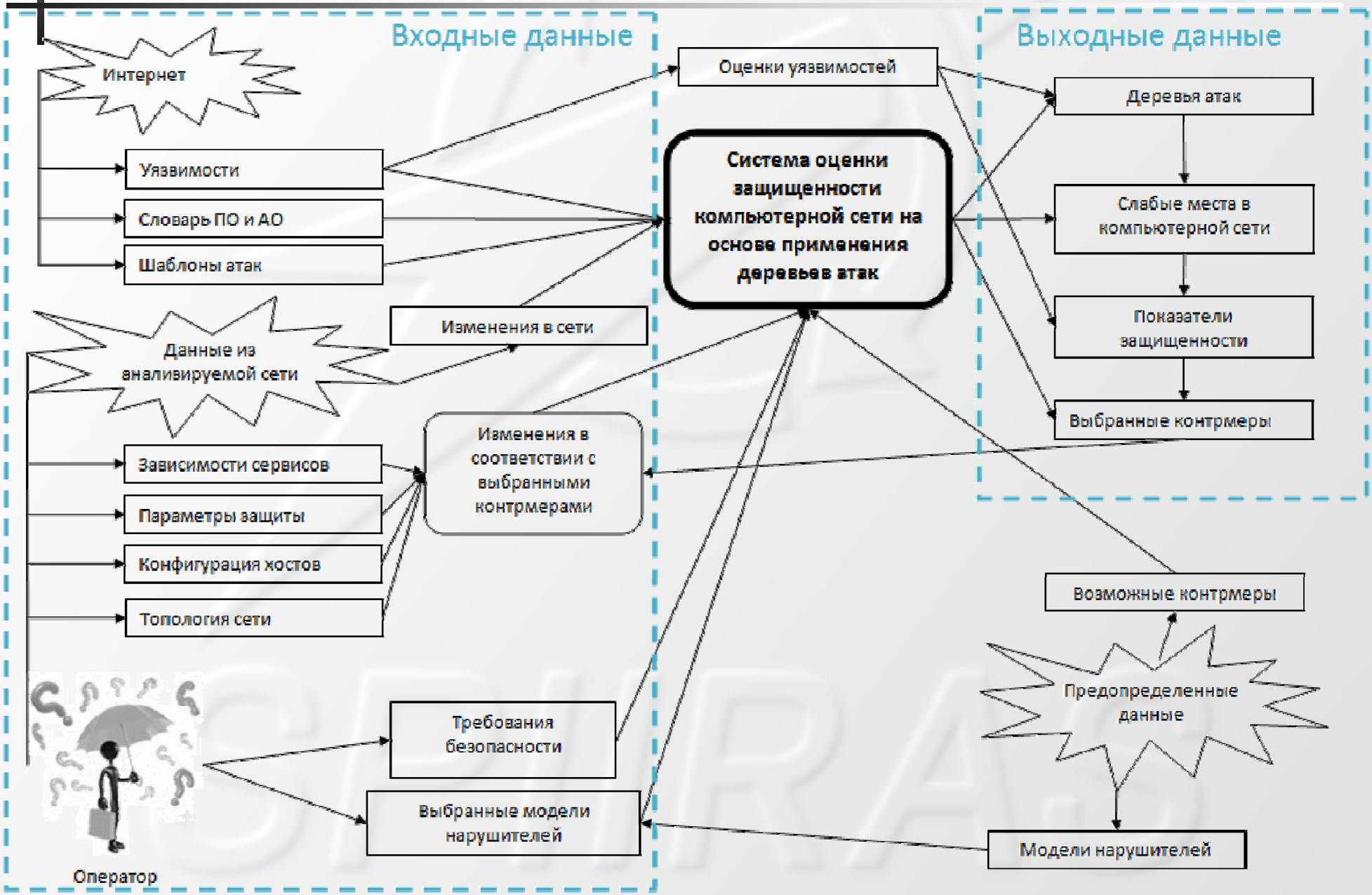
Общая схема процесса мониторинга и управления безопасностью



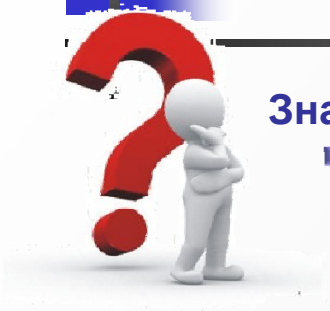
Место и роль обработки событий безопасности



Основные информационные потоки



Режимы работы прототипа



Не real-time режим

Знания оператора

Модель сети

Спецификация

Расчет базовых метрик

Уязвимости

Деревья атак

Результаты моделирования

Базовые метрики

Режим anytime

События в реальном времени

Обновленные деревья атак

Деревья атак

Расчет метрик защищенности

Сценарии

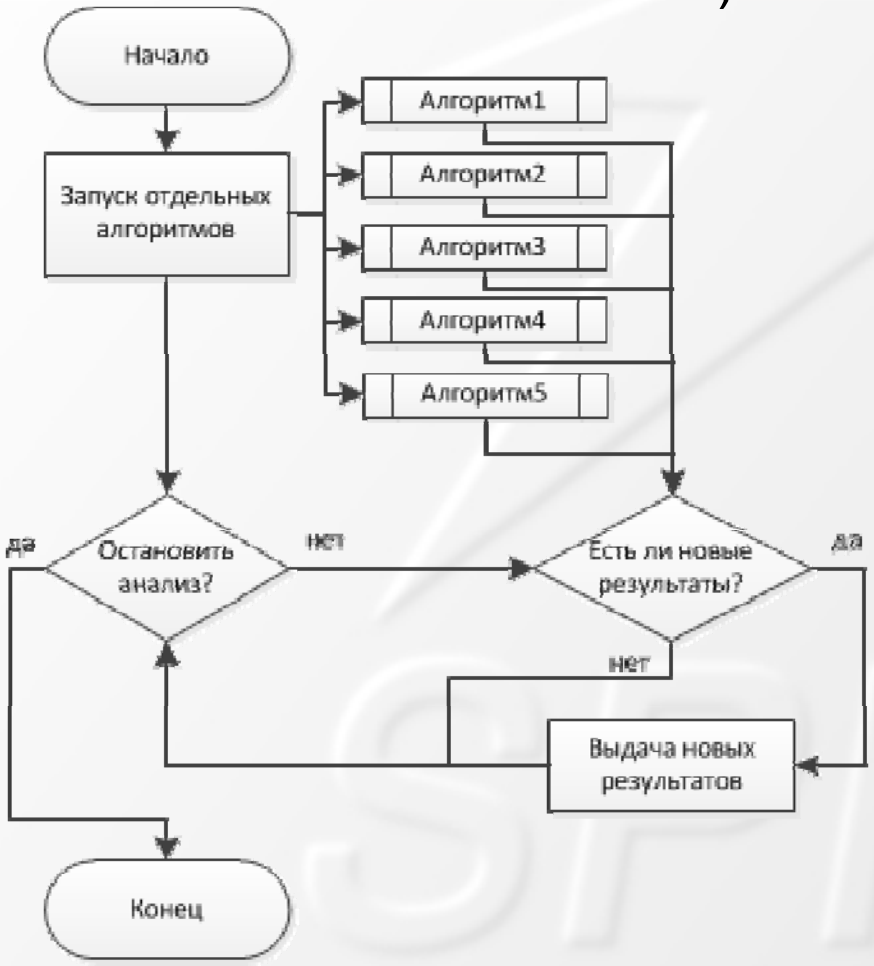
События в реальном времени

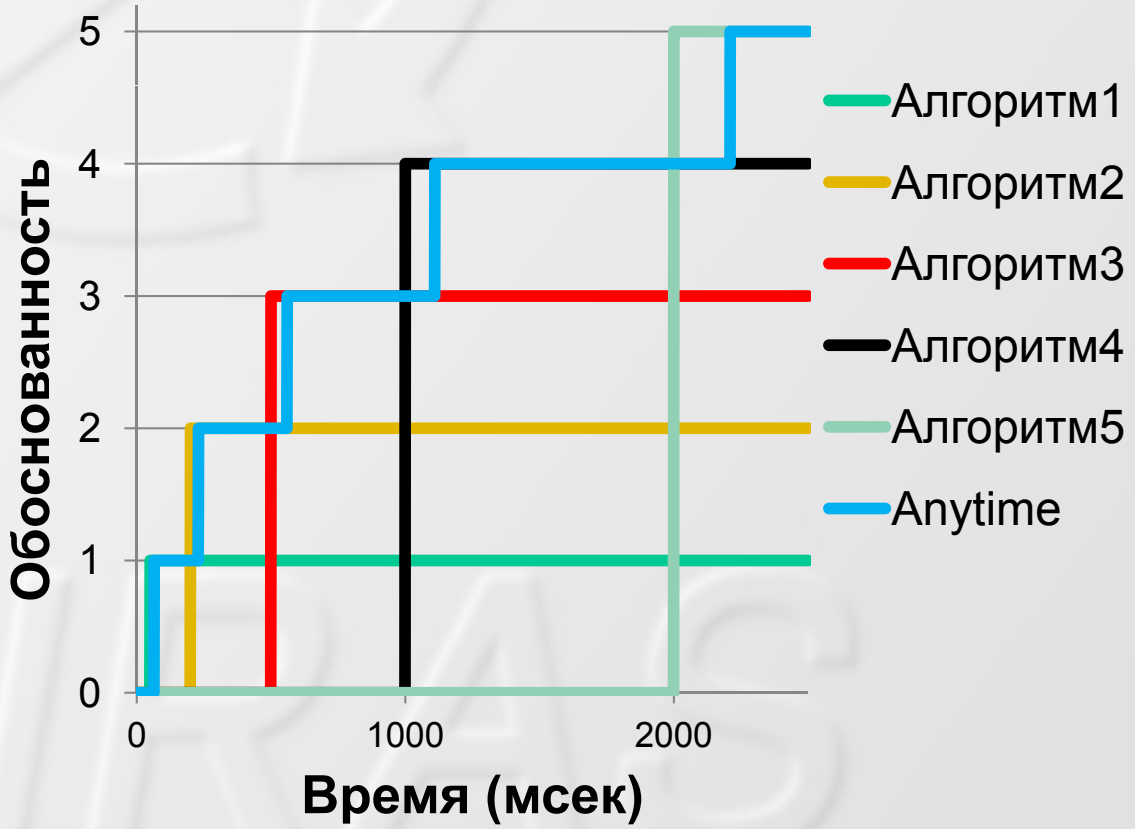
Определение сценариев атак

Рекомендации

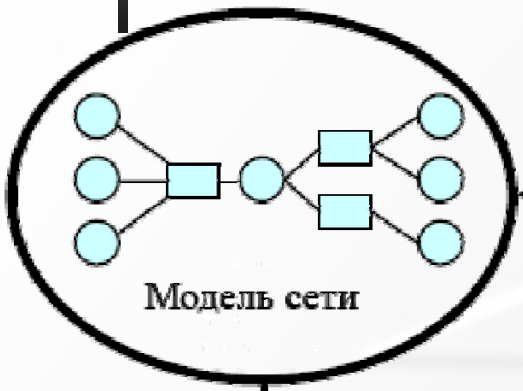
Anytime-алгоритмы

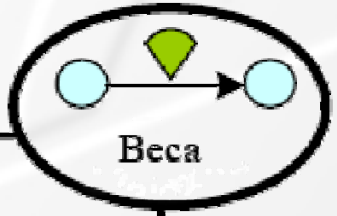
- Особенности подхода, основанного на **anytime-алгоритмах**
  - возможность получения решения в любой момент времени
  - улучшение решения с течением времени (повышение обоснованности)

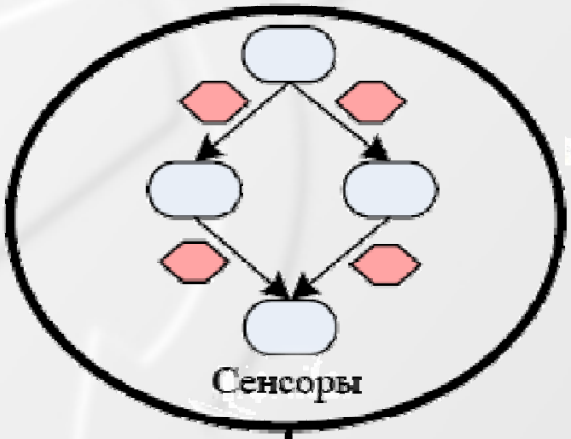


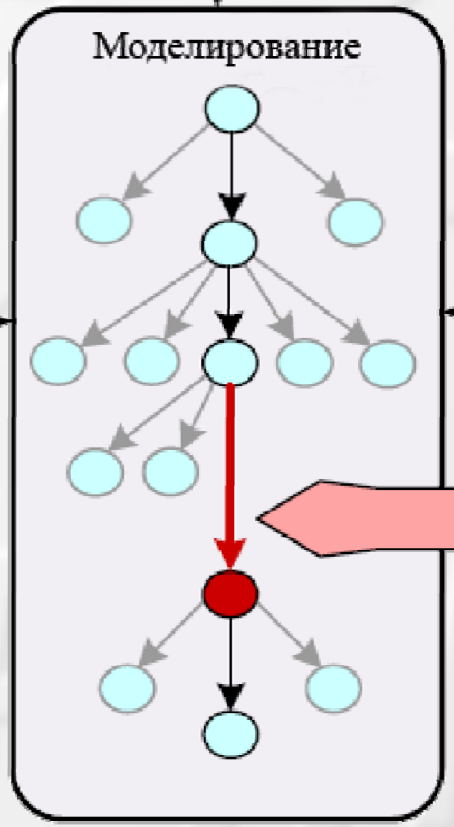


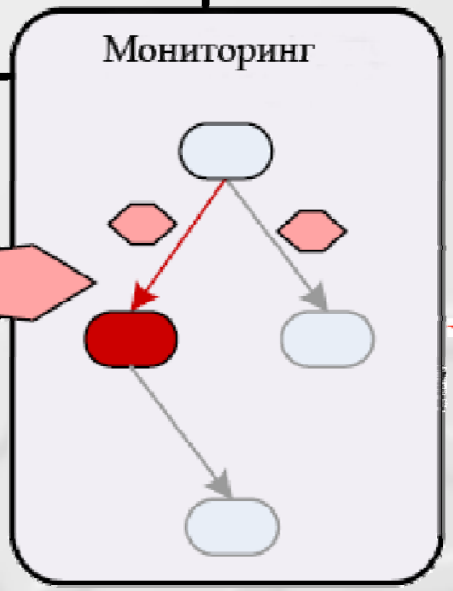
Анализ событий



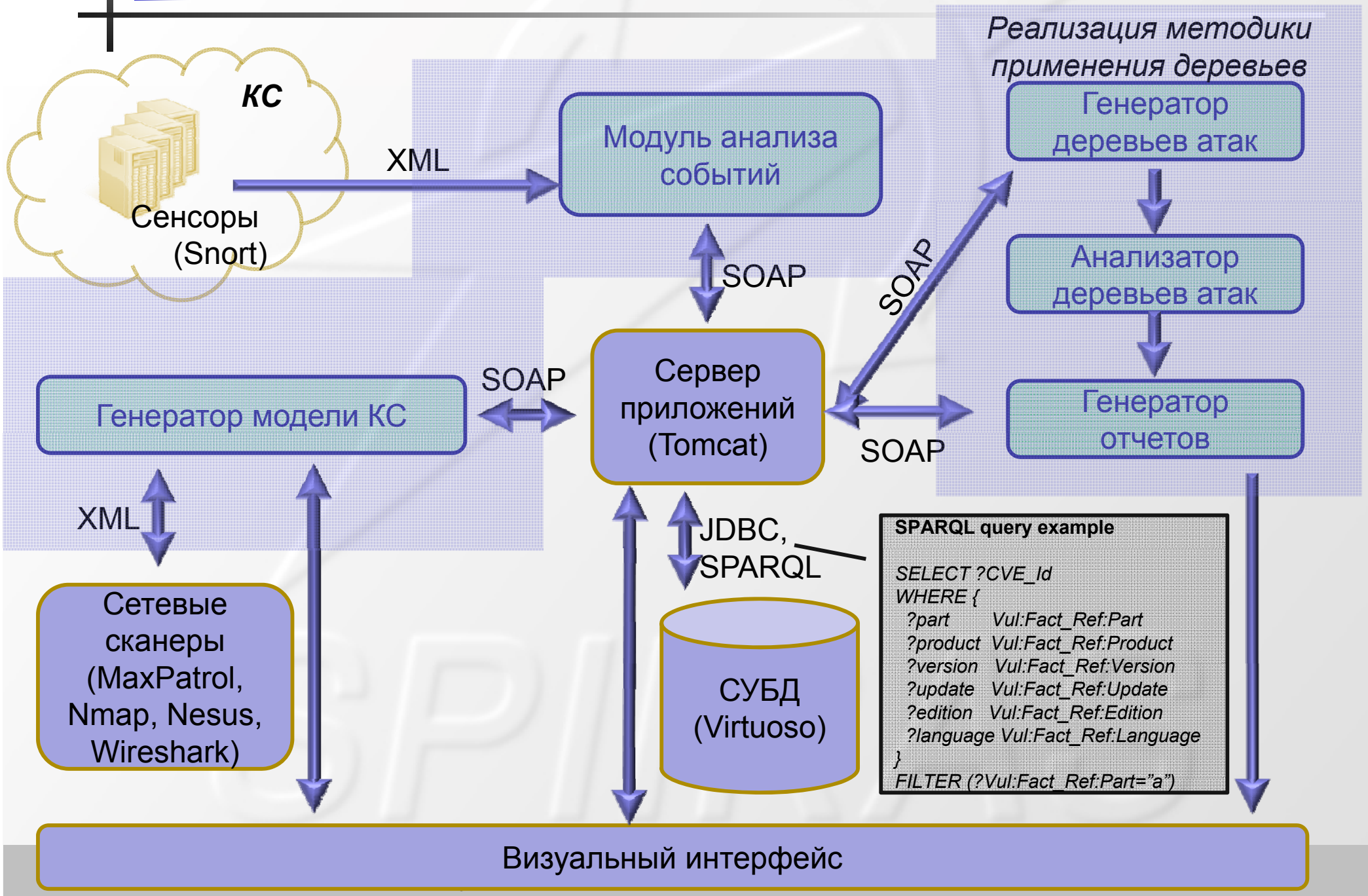




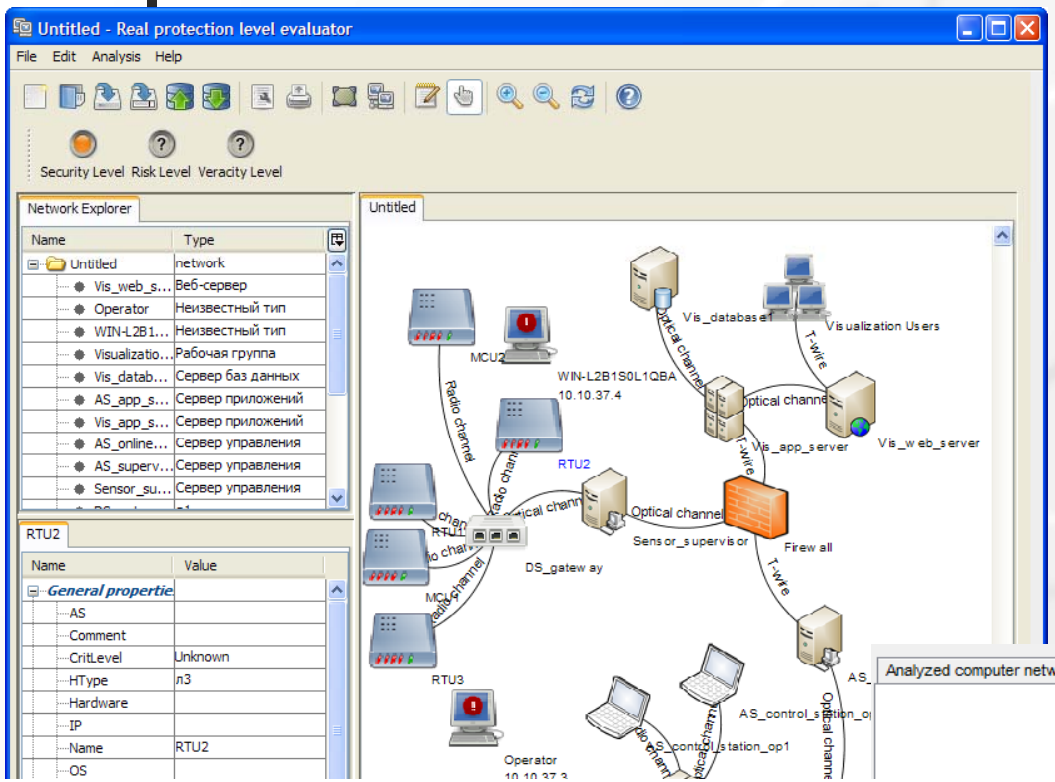


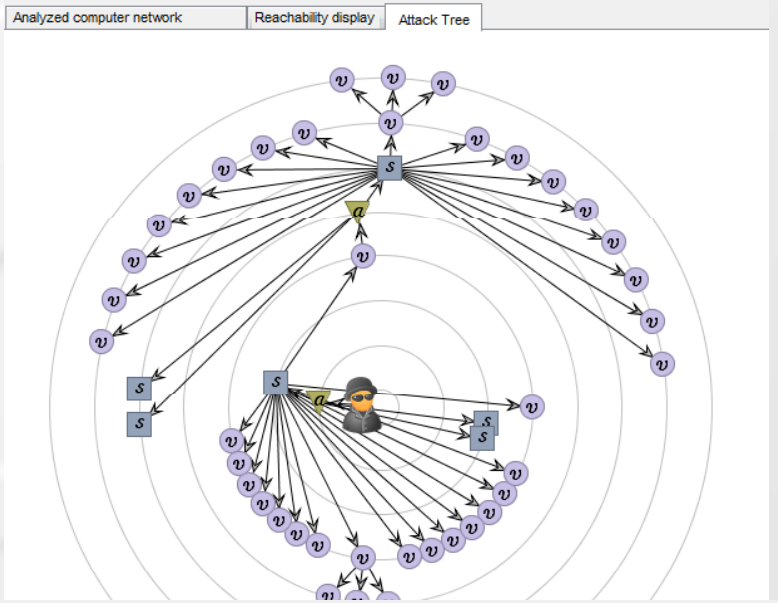


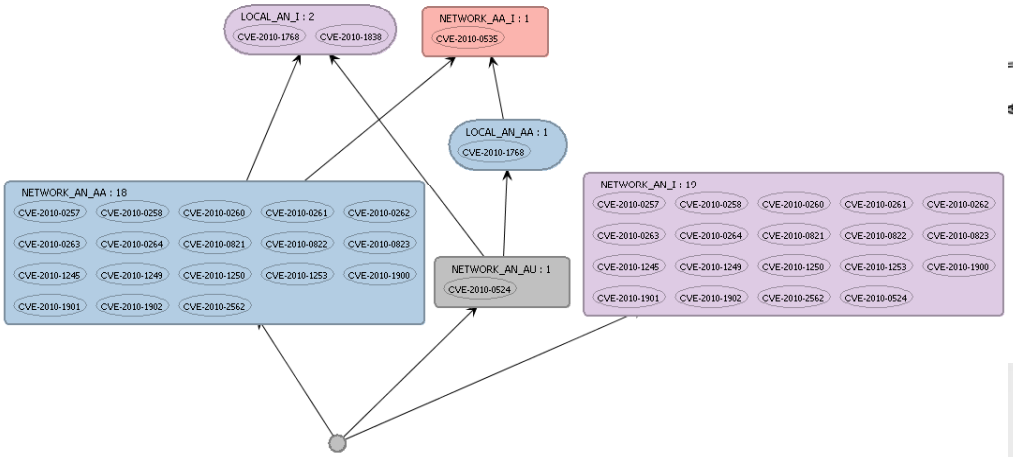
Архитектура и программная реализация (1/2)

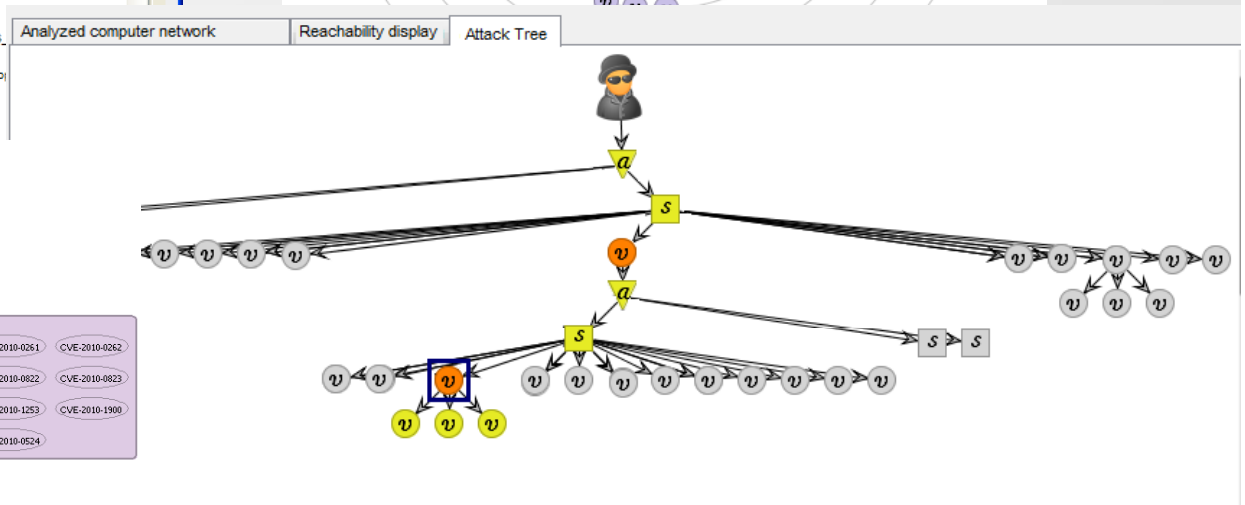


Архитектура и программная реализация (2/2)

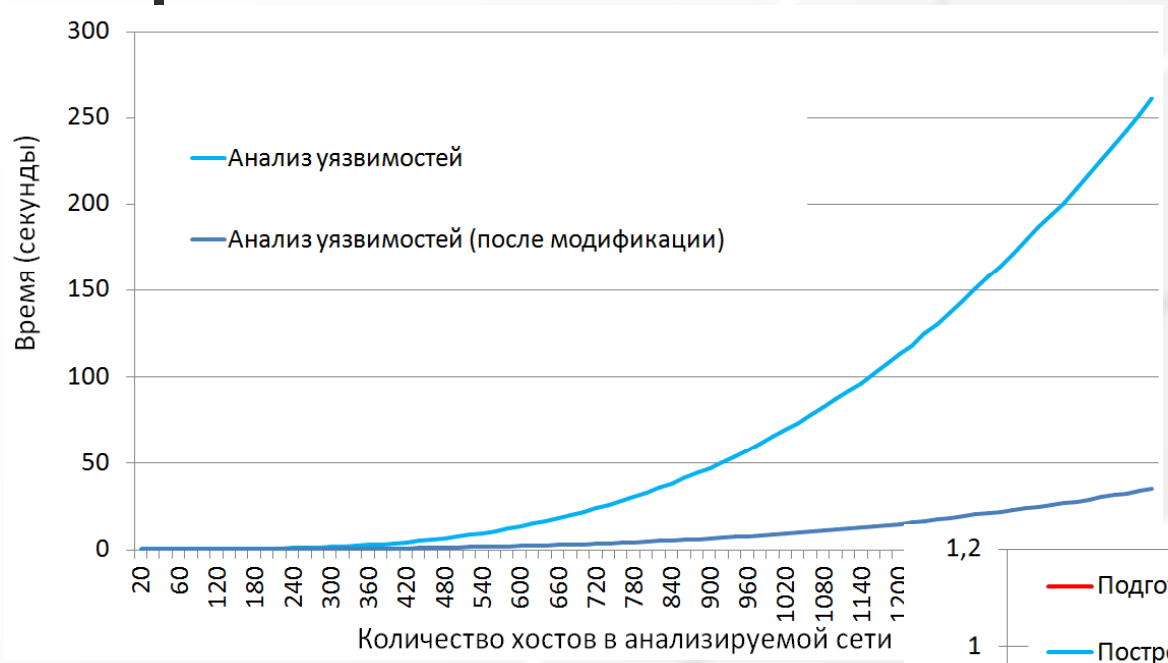








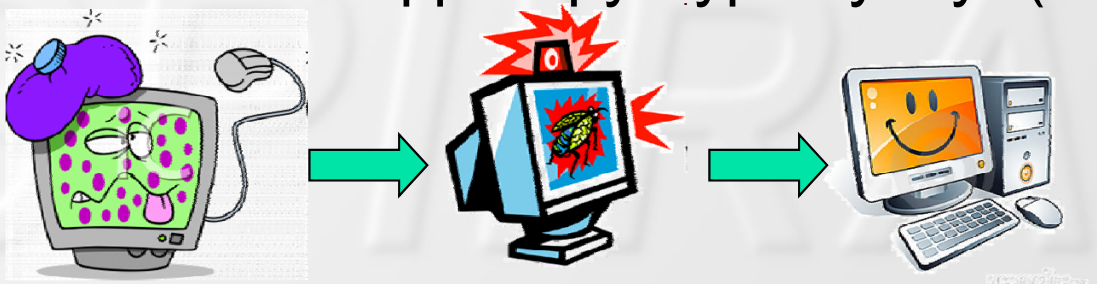
Оценка и сравнение показателей методики



- При обработке событий, для каждого события формируется список маршрутов атак;
- Для каждого маршрута рассчитываются показатели рисков и вероятности того, что нарушитель будет использовать именно этот маршрут.

Выводы

- Аналитическое моделирование атак может быть использовано при мониторинге событий безопасности в реальных компьютерных сетях;
- Известные проблемы:
  - Сбор исходных данных;
  - Выявление деталей проведенной атаки, а лучше конкретный идентификатор проэксплуатированной уязвимости;
  - Ошибки первого и второго рода.
- Данный подход был успешно использован в проекте Седьмой рамочной программы (FP7) Европейского Сообщества “Управление информацией и событиями безопасности в инфраструктурах услуг (MASSIF)”.



Контактная информация

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

Котенко Игорь Витальевич
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko

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.