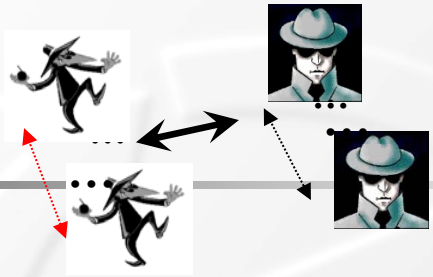


Аналитическое моделирование и анализ событий в системах управления информацией и событиями безопасности

И.В. Котенко

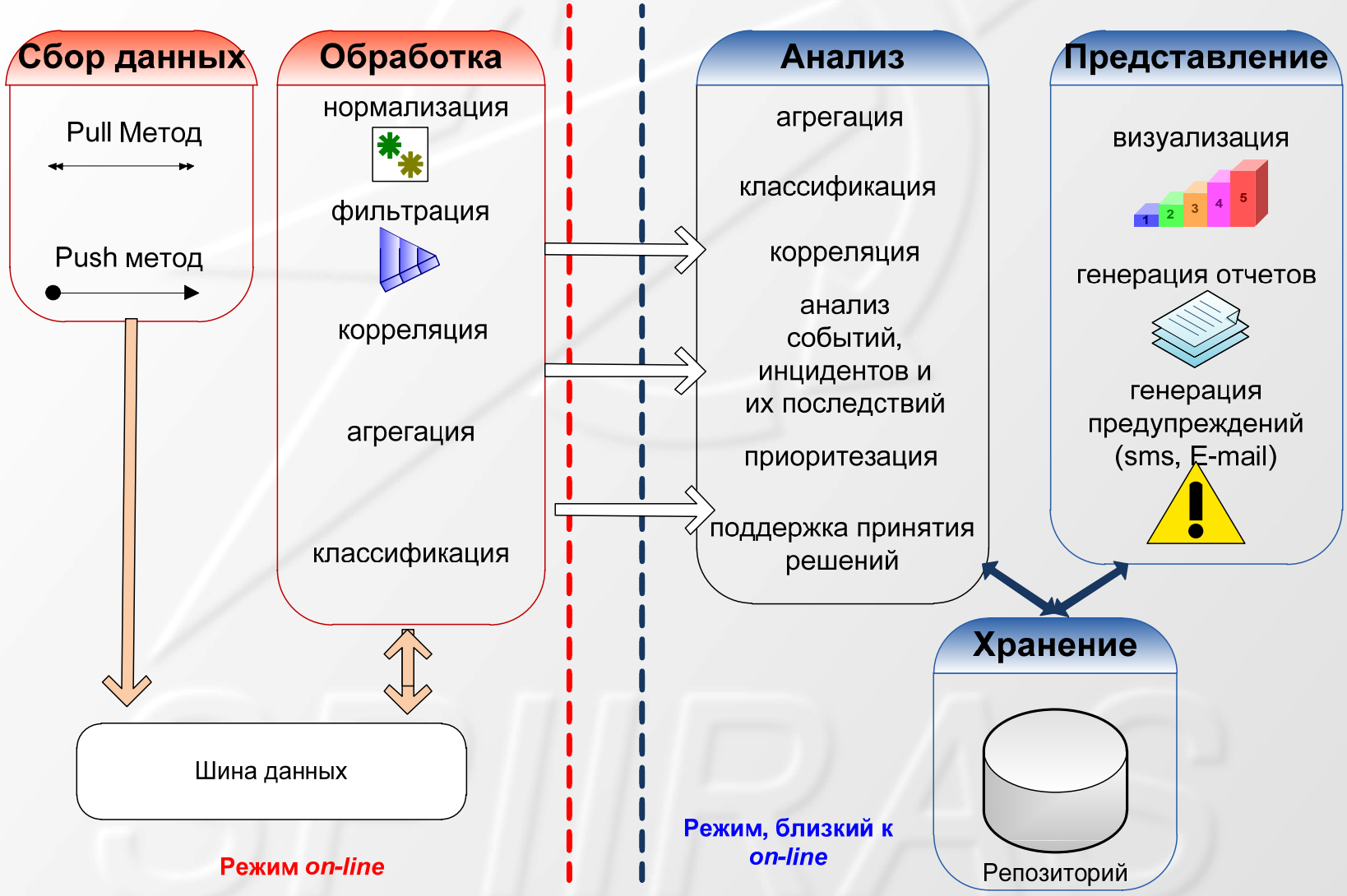
Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто'2012, 28-31 марта 2012 г.

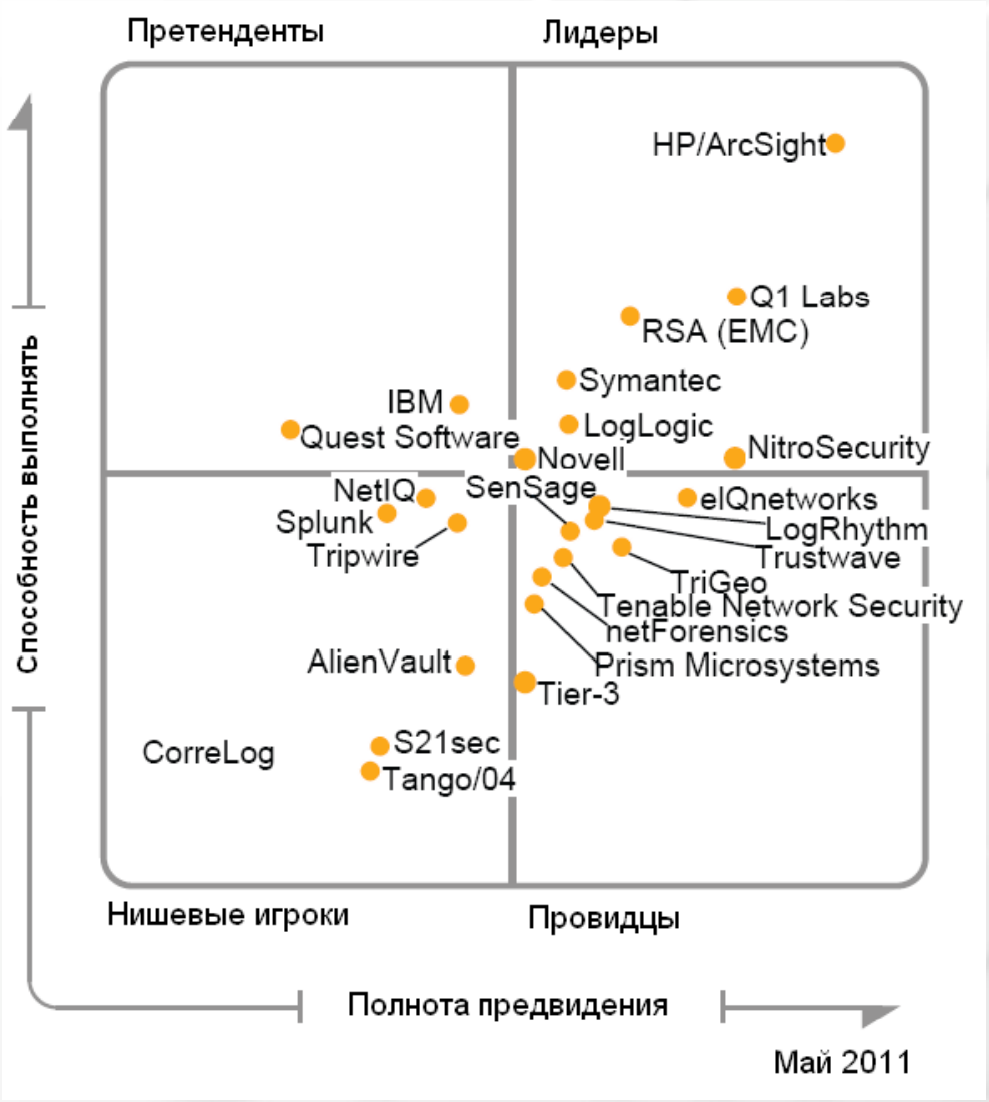
План доклада

- Введение
- SIEM-системы
- Подход к аналитическому моделированию
- Пример фрагмента сценария моделирования
- Заключение

Функциональная модель SIEM-системы

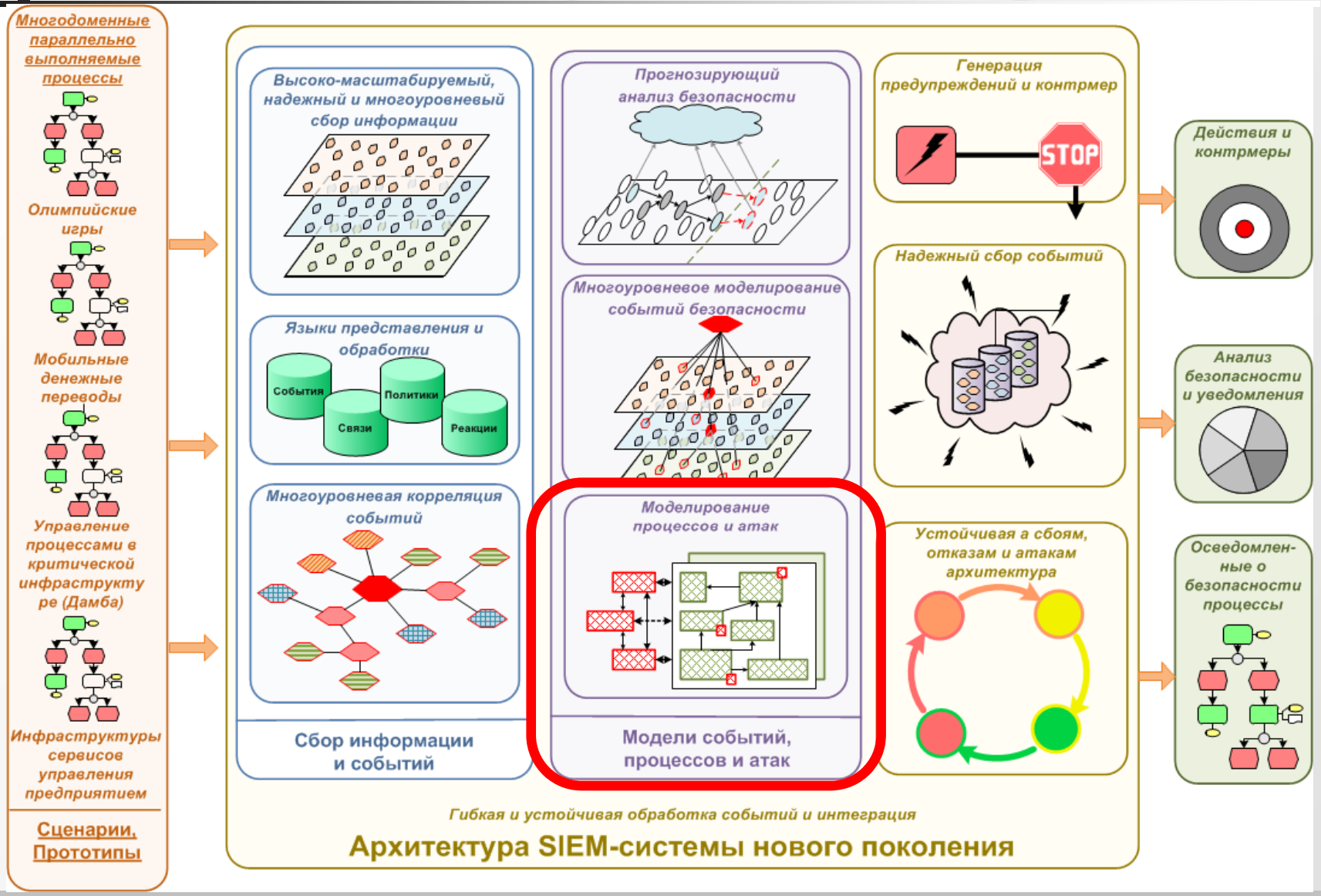


Сравнение SIEM-решений (*Gartner, 2010*)



- **ArcSight**
- **RSA (EMC)**
- **Symantec Security Information Manager (SIM)**
- **LogLogic**
- IBM Tivoli Security Information and Event Manager (TSIEM)
- CA
- Novell
- LogRhythm
- netForensics Open Security Platform
- Tenable
- LogMatrix
- …

Место и роль моделирования атак и механизмов защиты в проекте MASSIF (1/2)



План доклада

- Введение
- SIEM-системы
- **Подход к аналитическому моделированию**
- Пример фрагмента сценария моделирования
- Заключение

Основные причины использования моделей атак в SIEM-системах

- Вычисление возможных последовательностей (трасс) атак, и упреждающее определение целей безопасности, которые с наибольшей вероятностью станут мишенью для нарушителя
- Корреляция последовательностей событий безопасности, т.к. они относятся к определенным действиям внутри модели атак
- Определение показателей защищенности
- Определение соответствующих наборов контрмер, т.е. действий, предпринимаемых системой, чтобы разрушить непрерывную последовательность действий атакующего
- Динамическое вычисление воздействия атак и контрмер; атак - когда они нарушают политику безопасности, и контрмер - когда они изменяют конфигурацию системы

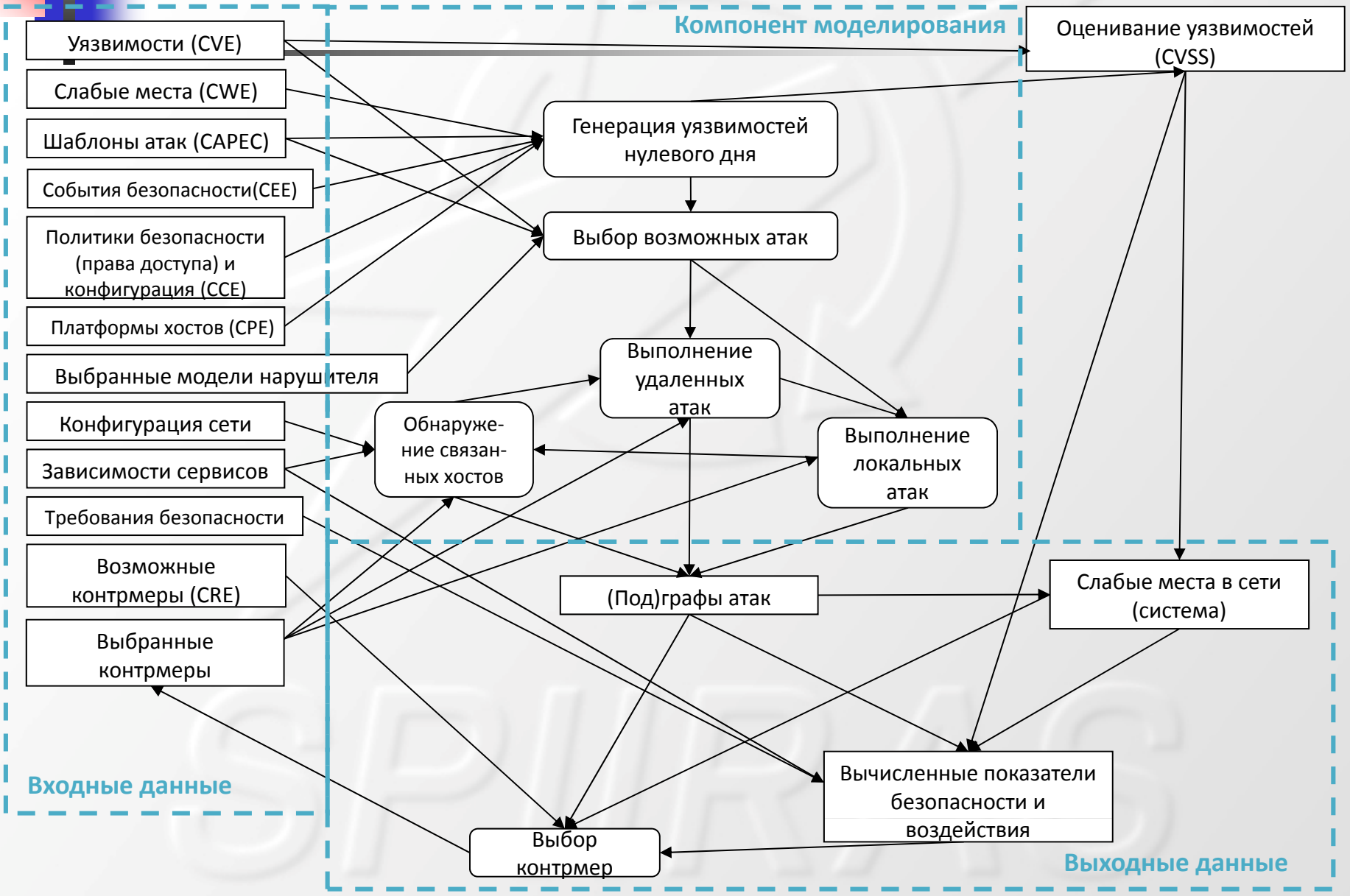
Особенности предлагаемых решений (1/2)

- Использование репозитория безопасности (содержащего данные о конфигурации системы, моделях нарушителя, уязвимостях, атаках, оценках, контрмерах и др.)
- Эффективные методики генерации графов атак и зависимостей сервисов, базирующиеся на методиках топологического анализа уязвимостей (TVA), которые формируют потенциальные последовательности использования уязвимостей для построения графов атак
- Учет как известных, так и новых атак, основанных на уязвимостях 0-го дня
- Применение anytime-алгоритмов для обеспечения близкого к реальному времени генерации подграфов атак и процедур анализа защищенности (anytime-алгоритм - итерационный вычислительный алгоритм, который способен выдать наилучшее на данный момент решение)

Особенности предлагаемых решений (2/2)

- Комбинированное использование графов атак и графов зависимостей сервисов
- Вычисление комплекса разнообразных показателей защищенности, включая следующие показатели:
  - уровень защищенности,
  - уровень воздействия и потенциал атаки,
  - уровень навыков нарушителя,
  - эффективность контрмер,
  - степень побочных потерь при реализации контрмер и др.
- Стохастическое аналитическое моделирование и интерактивная поддержка принятия решений для выбора предпочтительных решений по безопасности на основе определения предпочтений относительно различных типов целей и требований (рисков, стоимости, выигрыша) и установления компромиссов между высокоуровневыми целями защиты информации

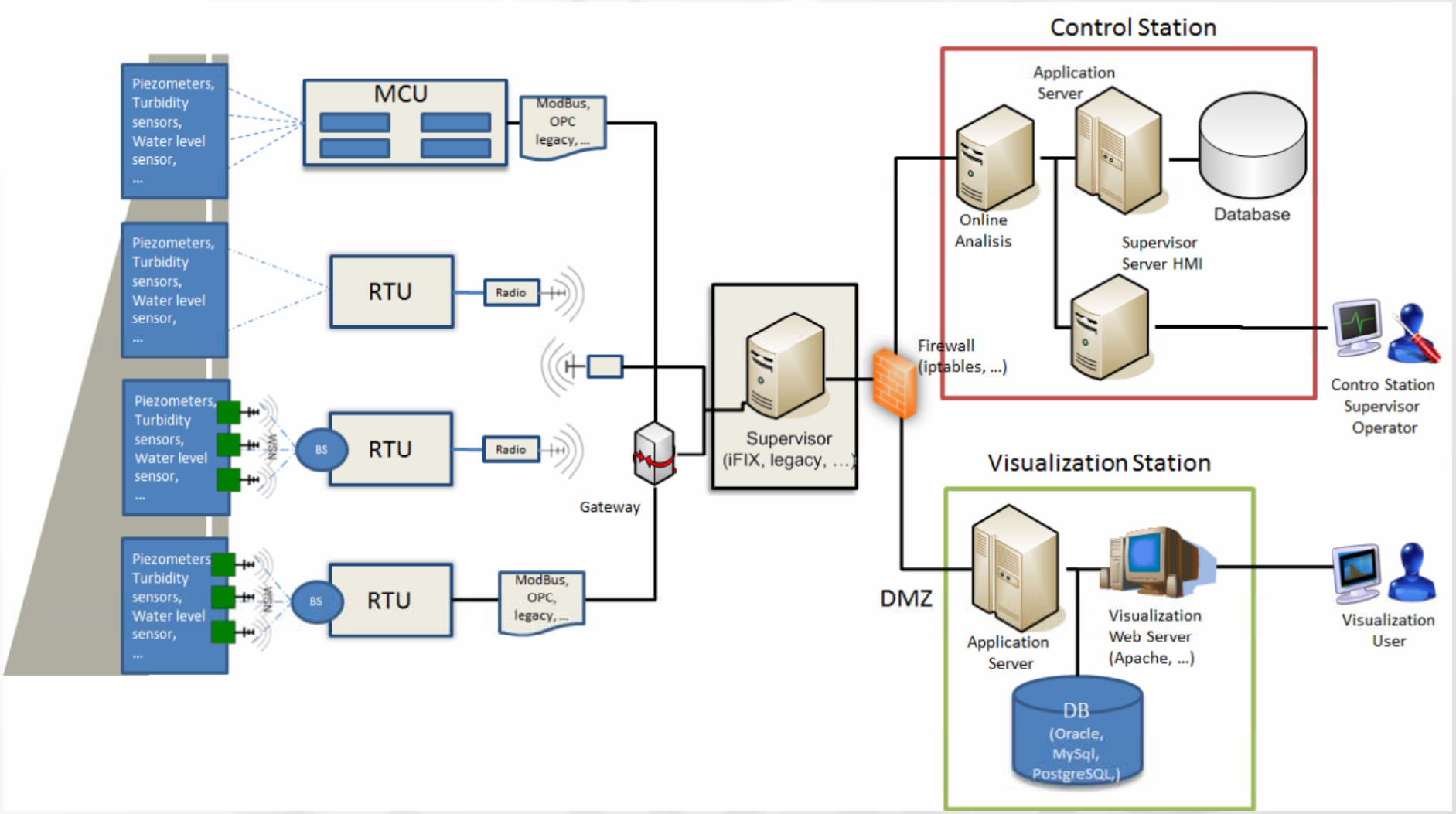
Основные процессы при моделировании



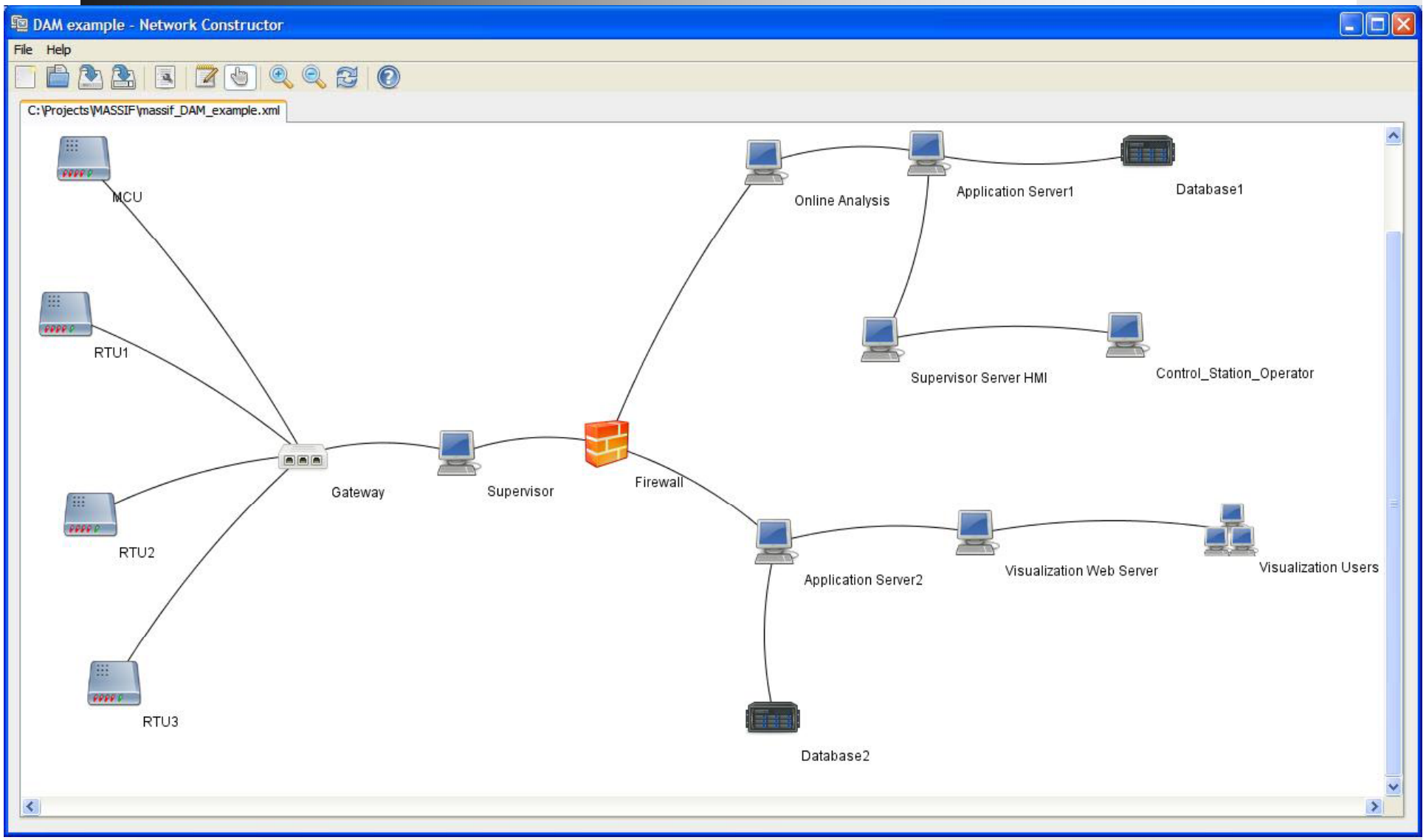
План доклада

- Введение
- SIEM-системы
- Особенности моделирования механизмов защиты информации
- Подход к аналитическому моделированию
- **Пример фрагмента сценария моделирования**
- **Заключение**

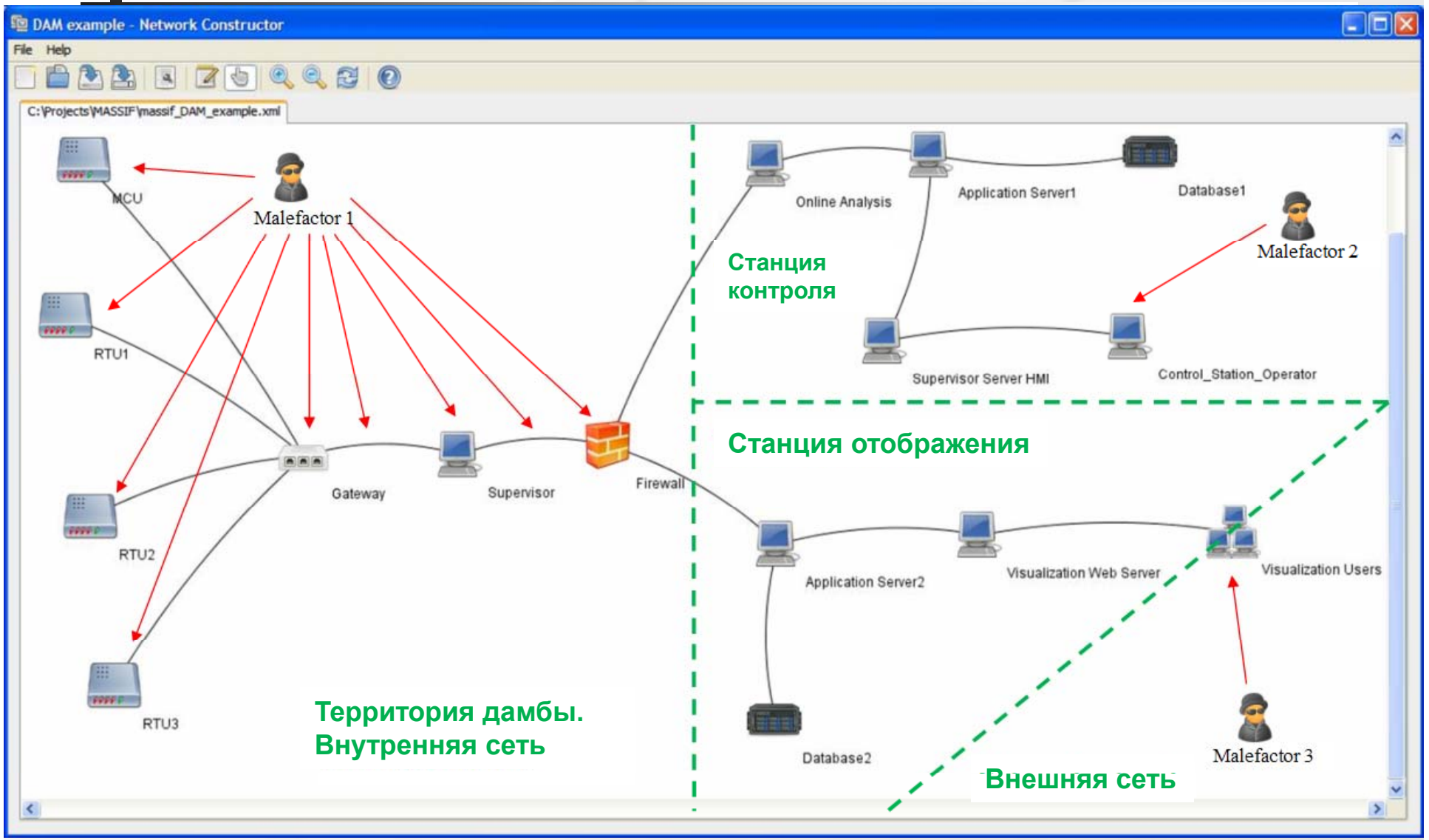
Пример моделирования для сценария “Управление процессами в критических инфраструктуре (Дамба)”



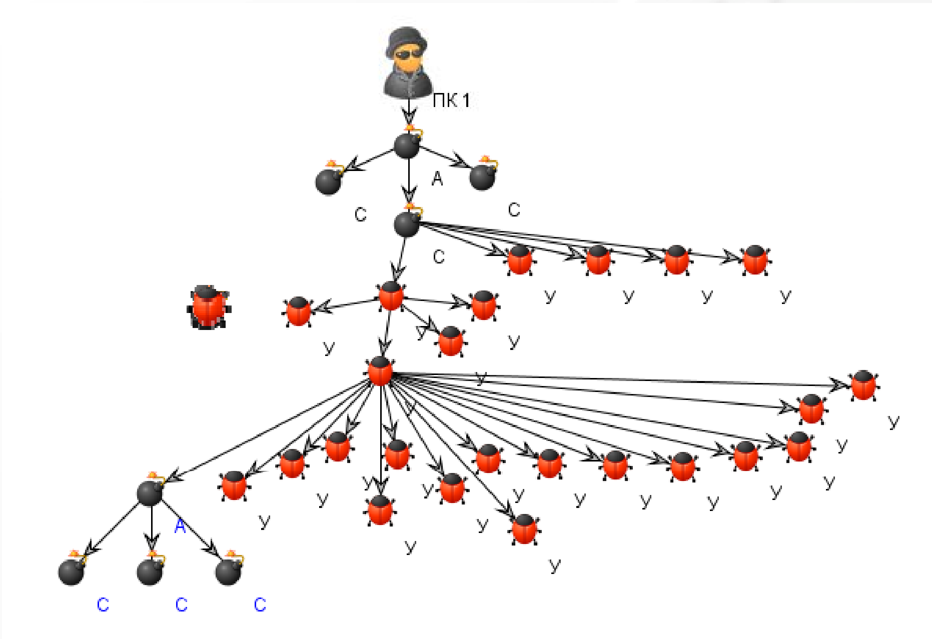
Топология сети

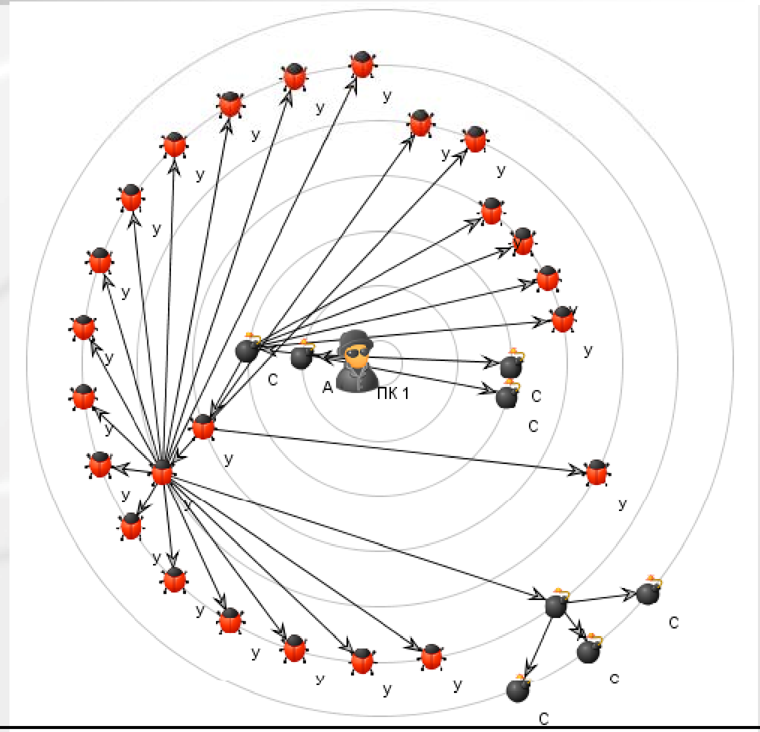


Модель нарушителя



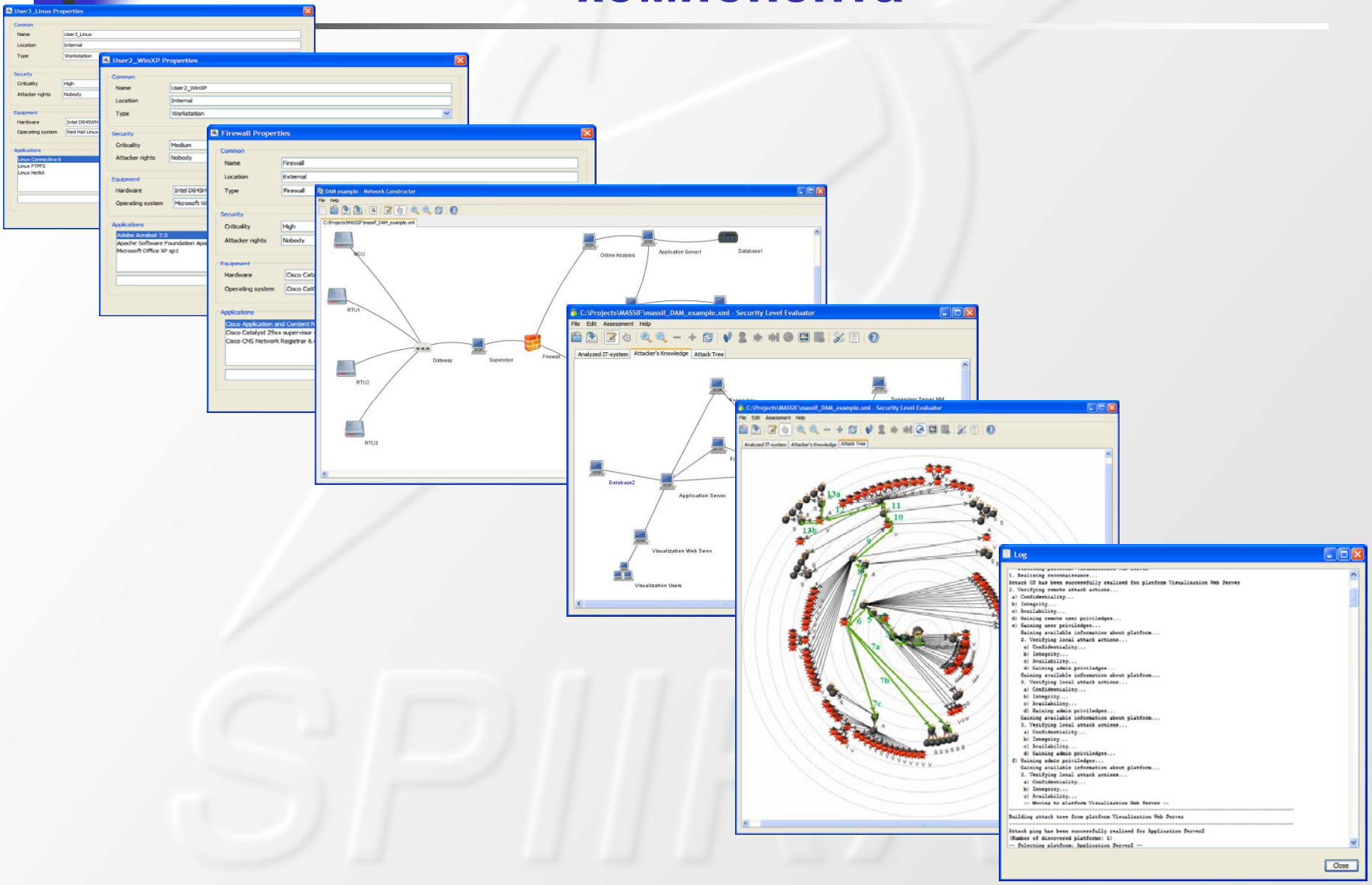
Интерфейс среды моделирования (3/3)



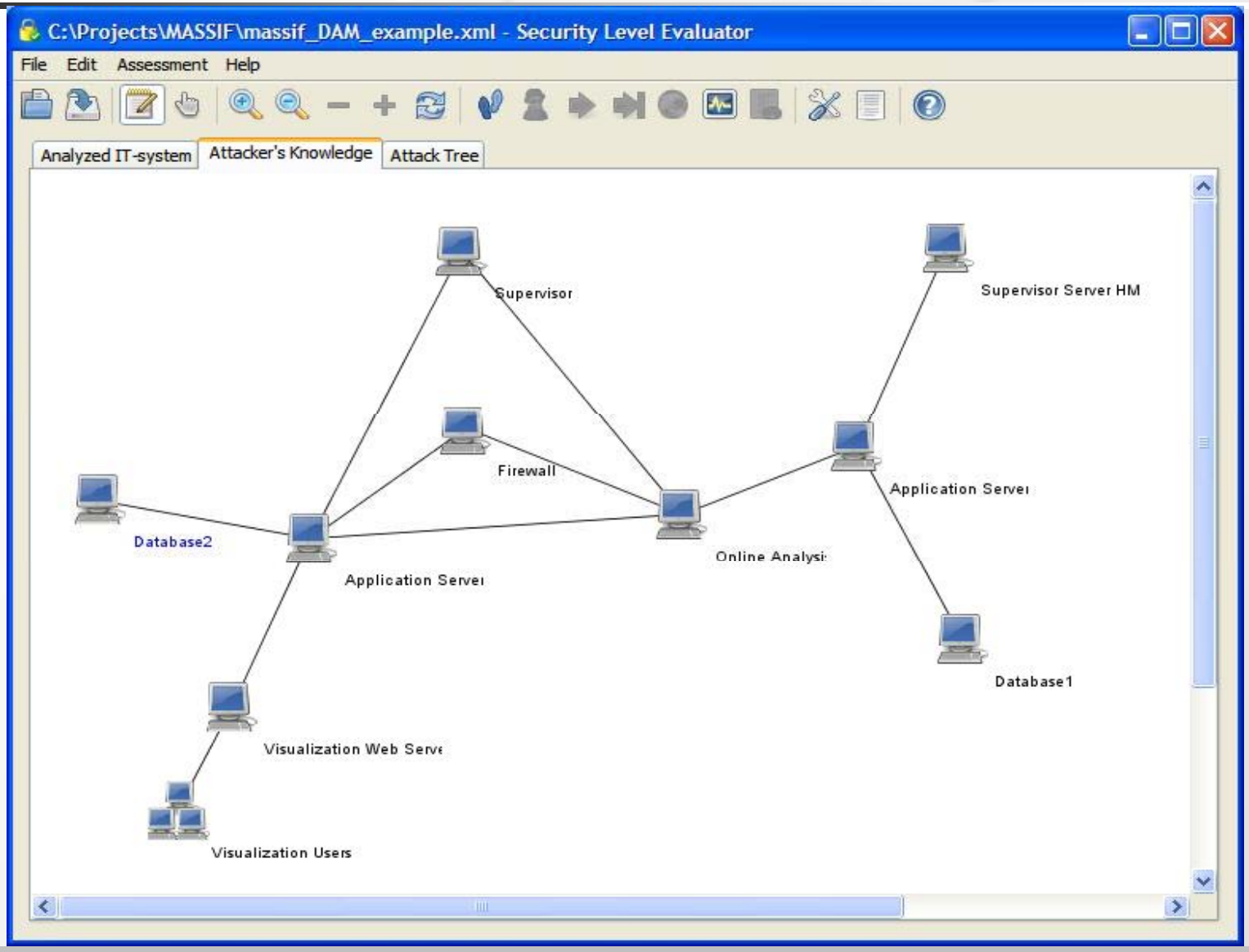


Обозначение	Описание
	Исходное положение нарушителя (рядом со значком отображается имя платформы, используемой нарушителем в качестве исходной для реализации атакующих действий)
	Специфическое атакующее действие (рядом со значком используется символ «А») или сценарий (рядом со значком используется символ «С»), не использующие уязвимости, например, обнаружение «живых» хостов (PING)
	Атакующее действие, использующее уязвимость (рядом со значком используется символ «У»)

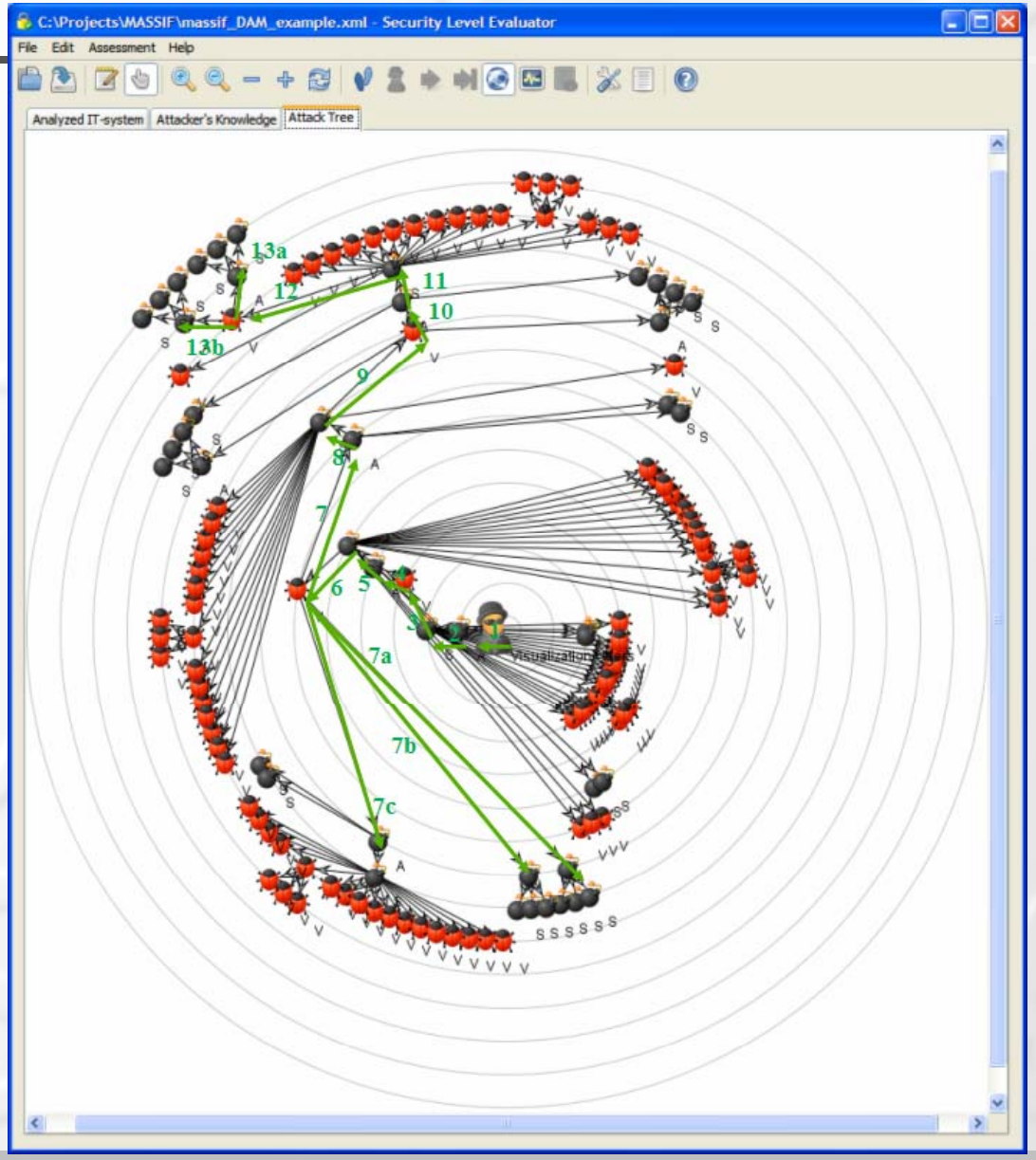
Последовательность функционирования компонента



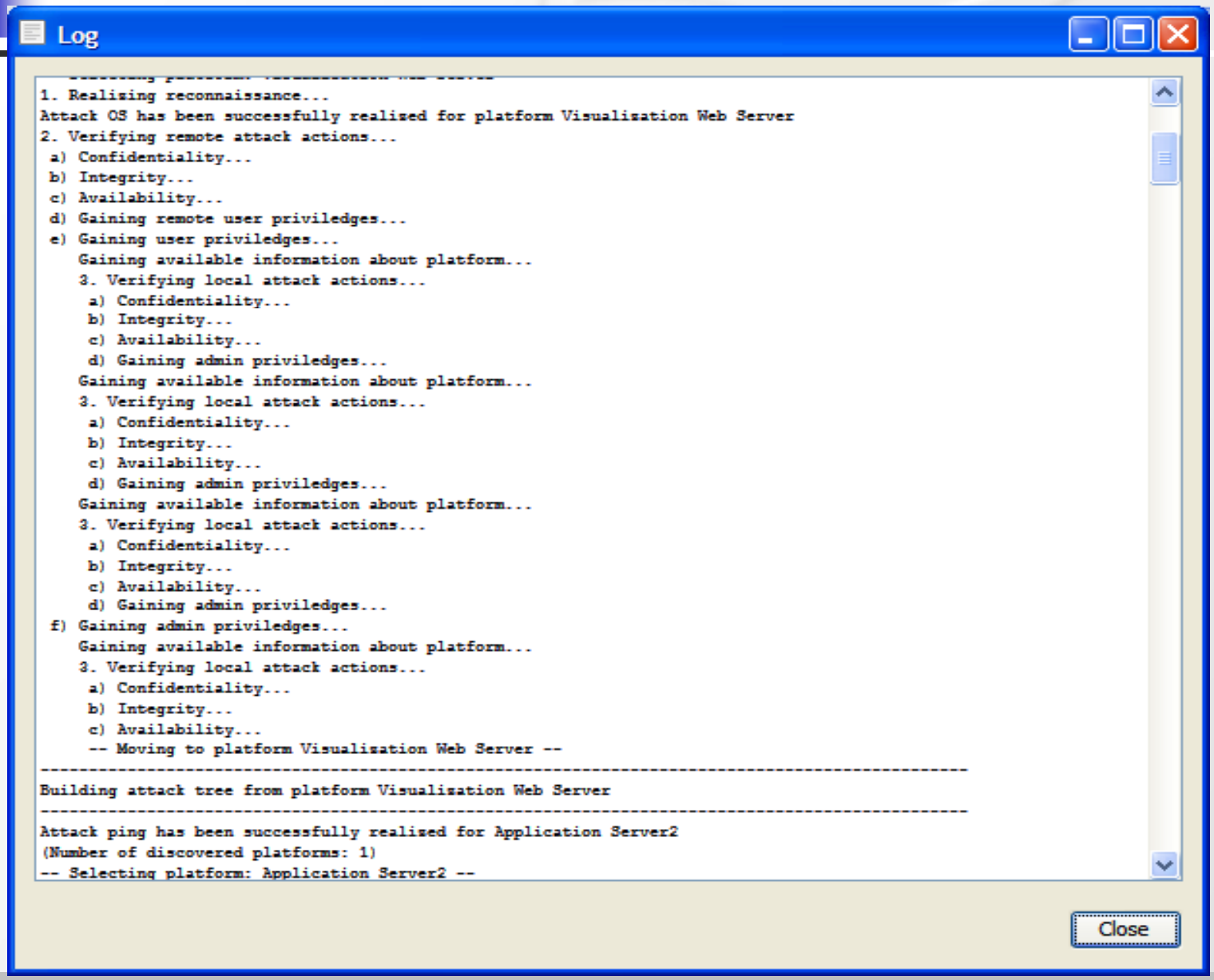
Знания нарушителя при реализации атак



Граф атак


C:\Projects\MASSIF\massif_DAM_example.xml - Security Level Evaluator
File Edit Assessment Help
Analyzed IT-system
Attacker's Knowledge
Attack Tree
13a
12
11
10
13b
9
8
7
6
5
7a
7b
7c

Журнал построения дерева атак



План доклада

- Введение
- SIEM-системы
- Особенности моделирования механизмов защиты информации
- Подход к аналитическому моделированию
- Пример фрагмента сценария моделирования
- **Заключение**

Основные результаты работы

- Представлен подход к моделированию атак и механизмов защиты в SIEM-системах на основе аналитического анализа графов атак, построения сервисов зависимостей, учета уязвимостей нулевого для и др.
- Разработаны средства аналитического моделирования, реализующие данный подход.
- Проведено большое количество экспериментов, показавших возможность использования предложенного подхода для моделирования механизмов защиты информации, а также анализа защищенности проектируемых и функционирующих сетей.
- Предлагаемый подход к моделированию позволяет исследовать различные механизмы построения защищенных сетей, отвечать на вопросы “Что, если…”, определять наиболее эффективные механизмы защиты, осуществлять анализ защищенности в режиме, близком к реальному времени.

Направления дальнейших исследований

- Совершенствование моделей базовых компонентов и их реализация
- Улучшение масштабируемости и адекватности аналитического моделирования
- Разработка подхода и стенда моделирования, основанных на “многорезолюционных” методах моделирования. Данный подход позволяет интегрировать макро- и микро- уровневые модели атак и механизмов защиты *(аналитические, основанные на пакетах, базирующиеся на эмуляции) и реальные сети небольшого размера для исследования масштабных атак и механизмов защиты.*

Контактная информация

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

Благодарности

- Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект № 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

РОССИЙСКАЯ АКАДЕМИЯ НАУК