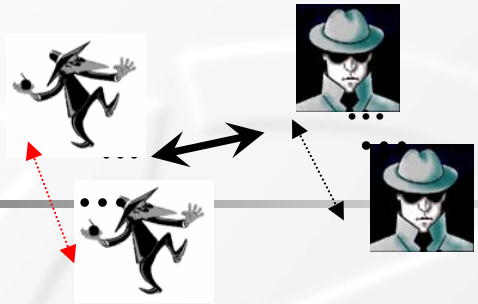


Моделирование и анализ механизмов кибербезопасности

И.В. Котенко

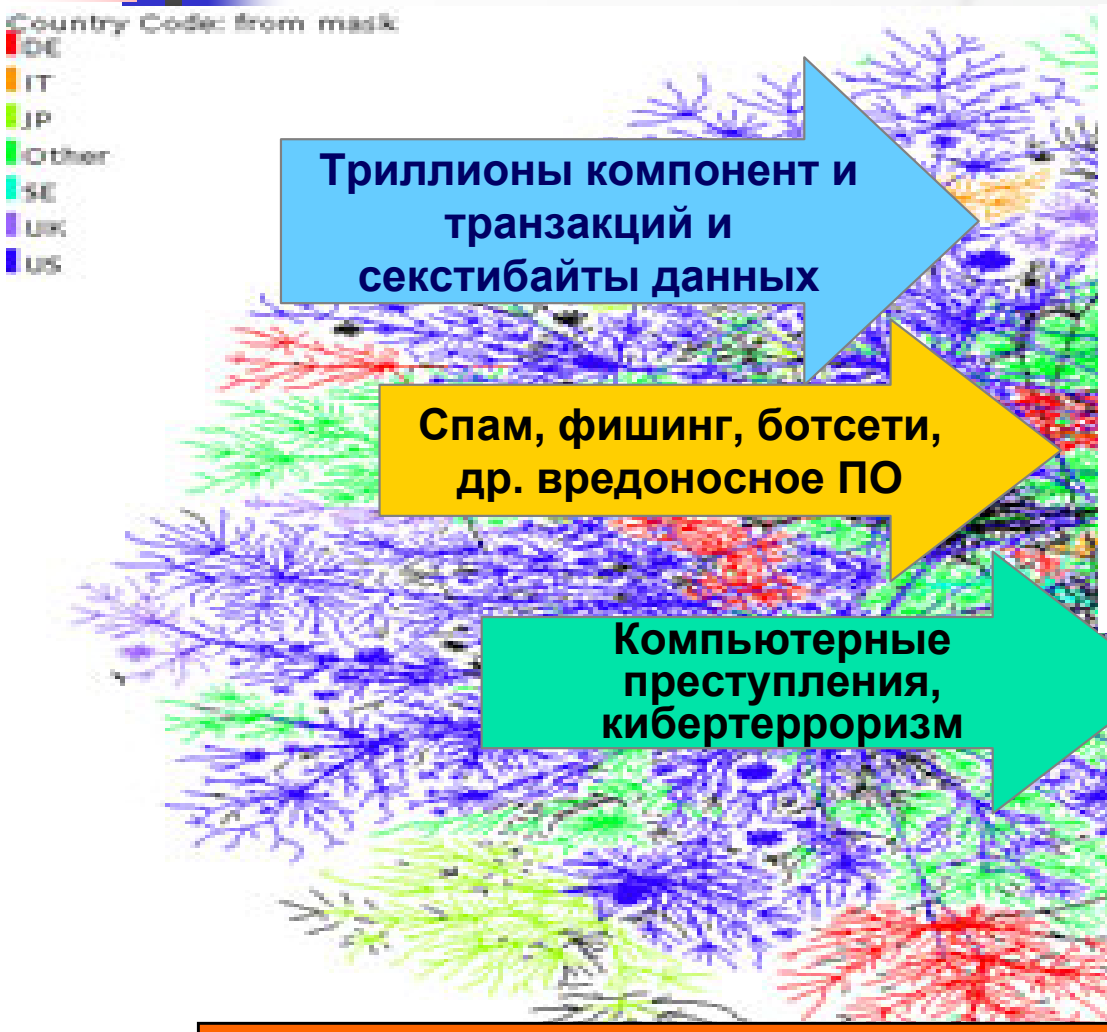
Учреждение Российской академии наук
Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто-2011, 30 марта – 2 апреля 2011 г.

План доклада

- Введение
- Особенности моделирования механизмов кибербезопасности
- Подход к моделированию на уровне пакетов
- Подход к аналитическому моделированию
- Заключение

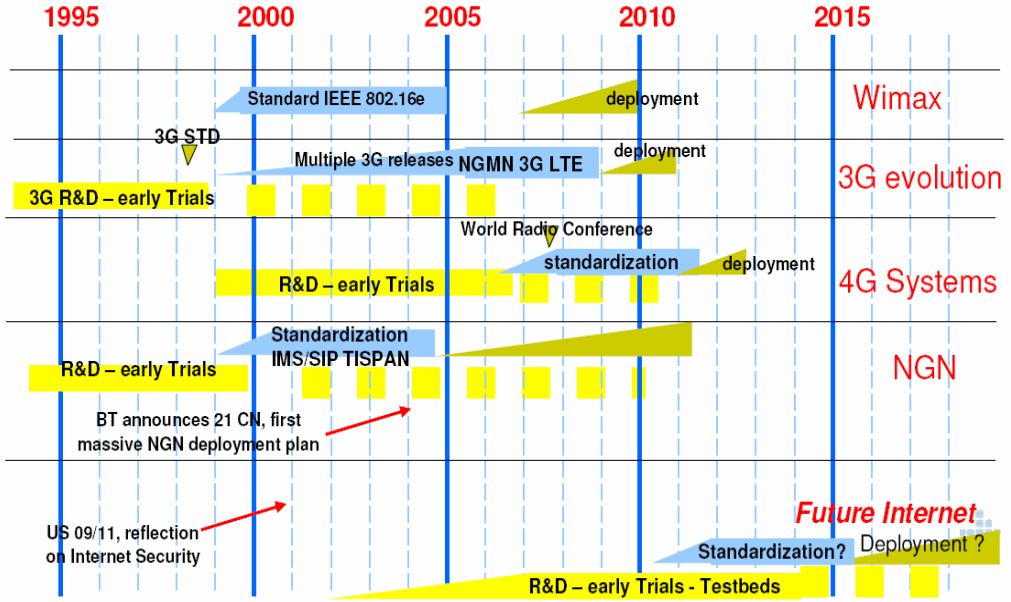
Будущие системы: проблема сложности!



Триллионы компонент и транзакций и секстибайты данных

Спам, фишинг, ботсети, др. вредоносное ПО

Компьютерные преступления, кибертерроризм



- Безопасность
- Масштабируемость
- Надежность
- Устойчивость
- …

Collaborative Security!

“Сквозная” безопасность и доверие в сетях, компонентах и сервисах!

Решаемая задача

- В связи с большой сложностью компьютерных сетей и невозможностью воспроизведения реальных исследуемых событий в сети Интернет, в том числе в силу возможных негативных событий, исследовательское моделирование играет важную роль в исследованиях, связанных с защитой от компьютерных атак и разработкой (выбором) механизмов и средств кибербезопасности.
- Доклад посвящен разработке общего подхода и программно-аппаратных средств для исследования компьютерных атак и механизмов кибербезопасности на основе интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического анализа графов атак, методов эмуляции и виртуализации сетевых процессов и др.

План доклада

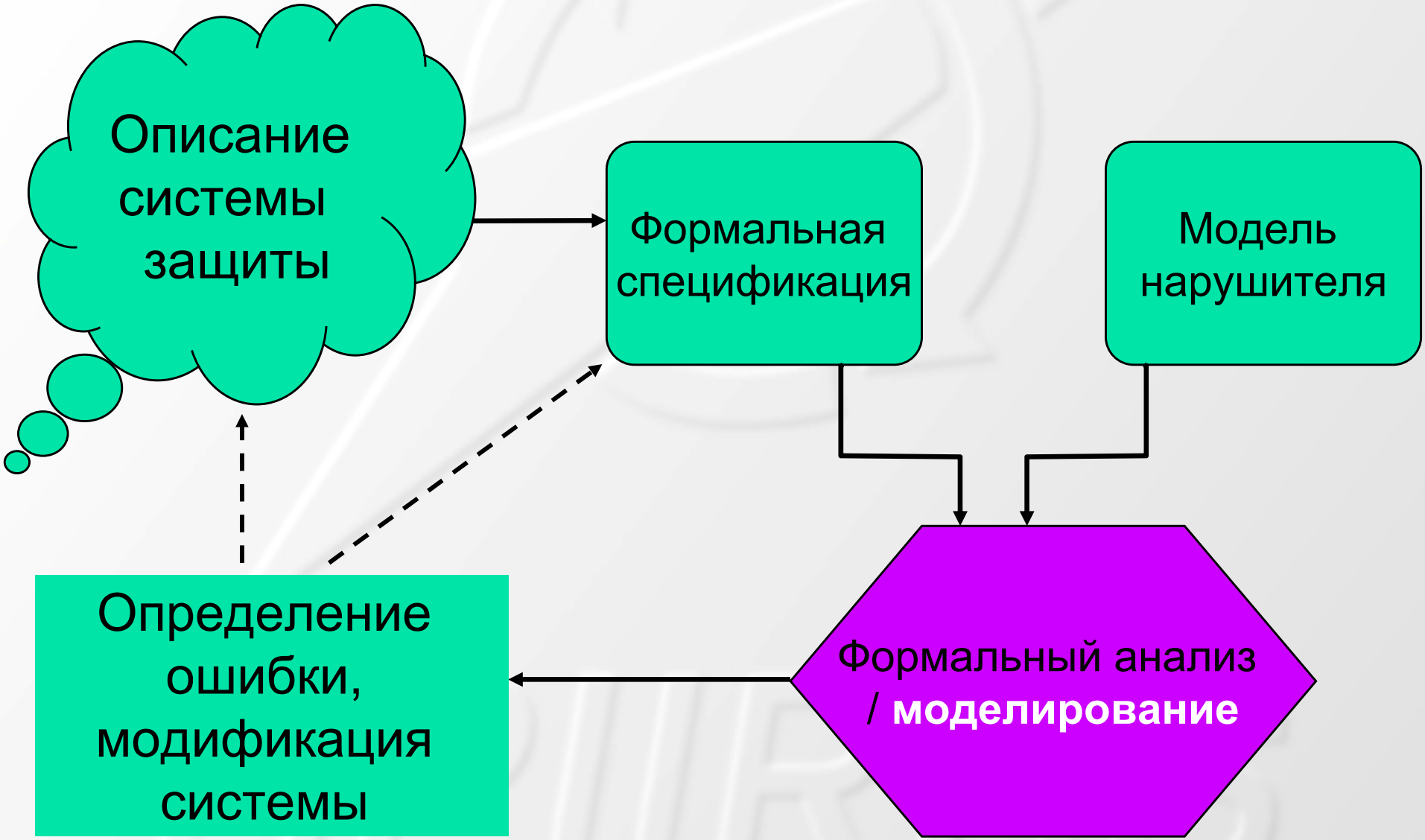
- Введение
- **Особенности моделирования механизмов кибербезопасности**
- Подход к моделированию на уровне пакетов
- Подход к аналитическому моделированию
- Заключение

Общие этапы моделирования для решения задач защиты информации

- Построение модели защищаемой системы
- Построение модели противника (нарушителя)
- Определение свойств компонентов защиты
- Моделирование и анализ выполнения этих свойств при реализации атак противника (нарушителя)

- Проверка результата моделирования
  - При данных допущениях реализация атак не приведет к нарушению заданных свойств
  - Не существует “абсолютной” защищенности

Метод явного учета нарушителя



Фундаментальный компромисс между сложностью модели и ее адекватностью

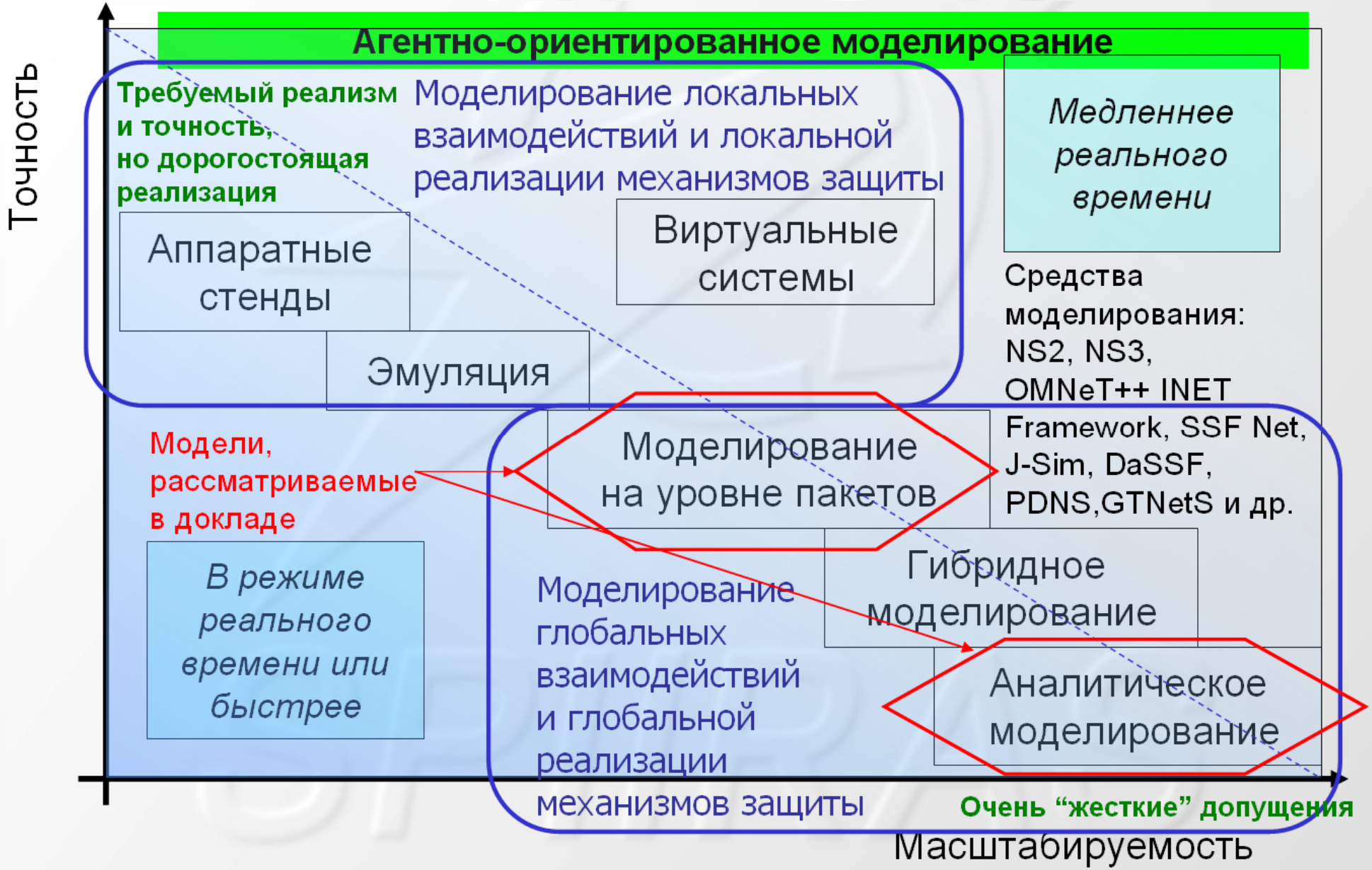
- **Модели абстрактны и сильно упрощены**
  - Отдельные компоненты моделирования представляются, как правило, как конечные автоматы
  - Функции защиты, как правило, моделируются как абстрактные типы данных
  - Свойства защиты формулируются, как правило, как недостижимость “плохого” состояния
  - Существует множество методов анализа свойств, многие из них автоматизированы …, но не являются полностью надежными
  - Доказательства в модели выполняются на основе ряда упрощающих допущений, которые игнорируют некоторые возможности нарушителя
- *Атака в формальной или имитационной модели “влечет” реальную атаку*

/В.Шматиков/

Области использования моделирования для задач защиты информации

- **Анализ влияния (Impact assessment)** для определения, каким образом механизмы защиты воздействуют на защищаемую систему и ее целевые свойства (безопасность, производительность, надежность и др.) [D.Nicol, S.Smith, M.Zhao-04 ; S.Kent, C.Lynn, K.Seo-00 (Secure BGP); M.Zhao, S.Smith, D.Nicol-05 и др.]
- **Эмуляция**, при которой реальные и виртуальные компоненты (“миры”) комбинируются для изучения взаимодействия между системами защиты и нарушителем и выявления уязвимостей системы защиты [G.Bakos, V.Berk-02 (Worm activity by metering ICMP); M. Liljenstam et al-03 (Simulating worm traffic) и др.]
- **Тренировки по реализации атак** и сценарии обучения [M. Liljenstam et al-05 (RINSE); B. Brown et al-03 и др.]
- **Анализ рисков**, базирующихся как на известных уязвимостях и параметрах конфигурации системы [R. Ortalo, Y.Deswarte, M.Kaaniche-99; Sheyner et al-02; B.Madam, K.Goseva-Popstojanova-02 и др.], так и новых (0-day) уязвимостях [Ingols et al., 2009], [Wang et al., 2010]

Спектр используемых моделей

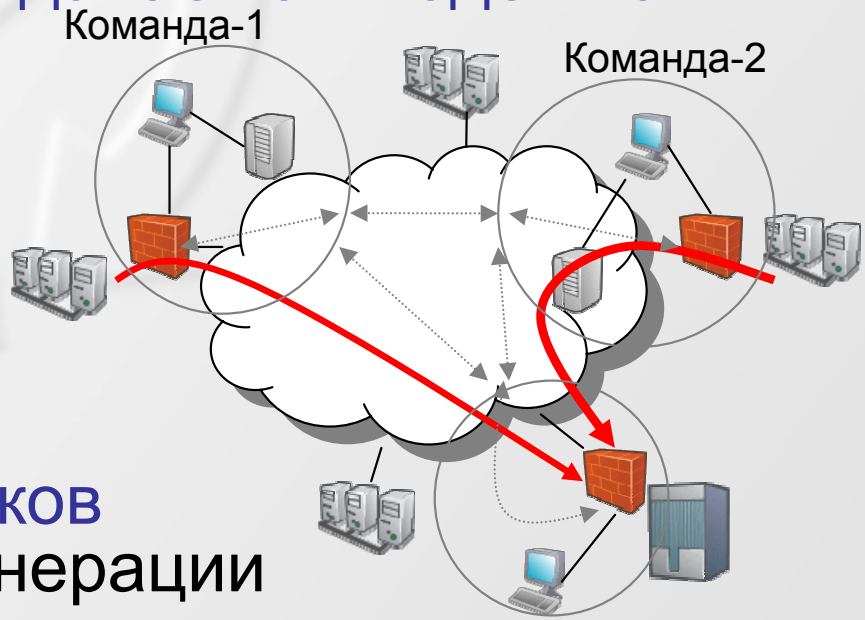


План доклада

- Введение
- Особенности моделирования механизмов кибербезопасности
- **Подход к моделированию на уровне пакетов**
- Подход к аналитическому моделированию
- Заключение

Основные положения подхода (1/3)

- Кибернетическое противоборство представляется в виде взаимодействия различных команд программных агентов
- Процессы происходят в среде, задаваемой моделью Интернета
- Выделяются команды агентов атаки, защиты и пользователей
- Команды взаимодействуют между собой: противоборствуют, кооперируются, адаптируются



- Команда агентов-злоумышленников эволюционирует посредством генерации новых экземпляров и типов атак, а также сценариев их реализации с целью преодоления подсистемы защиты.
- Команда агентов защиты адаптируется к действиям злоумышленников путем изменения исполняемой политики безопасности, формирования новых экземпляров механизмов и профилей защиты.

Основные положения подхода (3/3)

- Предлагаемый подход базируется на **комбинировании** элементов теории общих намерений, теории разделяемых планов и комбинированных подходов
- **Структура команды агентов** описывается в терминах иерархии групповых и индивидуальных ролей в различных сценариях действий
- **Спецификация иерархии планов** действий осуществляется для каждой из ролей. Для каждого плана описываются:
  (1) начальные условия, когда план предлагается для исполнения;
  (2) условия, при которых план прекращает исполняться;
  (3) действия, выполняемые на уровне команды, как часть общего плана
- **Назначение ролей и распределение планов** между агентами выполняется в два этапа: (1) сначала план распределяется в терминах ролей, (2) каждой из ролей ставится в соответствие агент

Процедуры поддержки командной работы

1. **Процедуры обеспечения согласованности действий агентов в команде** *(группе, индивидуально)* по некоторому общему плану.
2. **Процедуры мониторинга и восстановления функциональности команды** *(группы, индивидуально)* за счет переназначения “утерянных” ролей тем членам команды, которые в состоянии выполнить эту работу
3. **Процедуры обеспечения селективности коммуникаций**; основываются на расчете важности того или иного сообщения с учетом его “стоимости” и выгоды, получаемой при этом.

Команда защиты

$C_{defense} = \{S, D, F, L, I\}$

Агент “сэмплер”

- Сбор модельных данных для каждого узла по сетевым пакетам
- Выдача модельных данных на запрос «детектора»

Агент “детектор”

- Прием сообщения о работоспособности других агентов
- Запрос данных от «сэмплеров»
- Прием решения об атаке
- Посылка сообщения со списком подозрительных узлов «фильтру» и агенту «расследования», директиву ограничивать трафик

Агент «фильтр» – прием данных от «детектора» и фильтрация

Агент «расследования» – отслеживание источника атаки и его обезвреживание

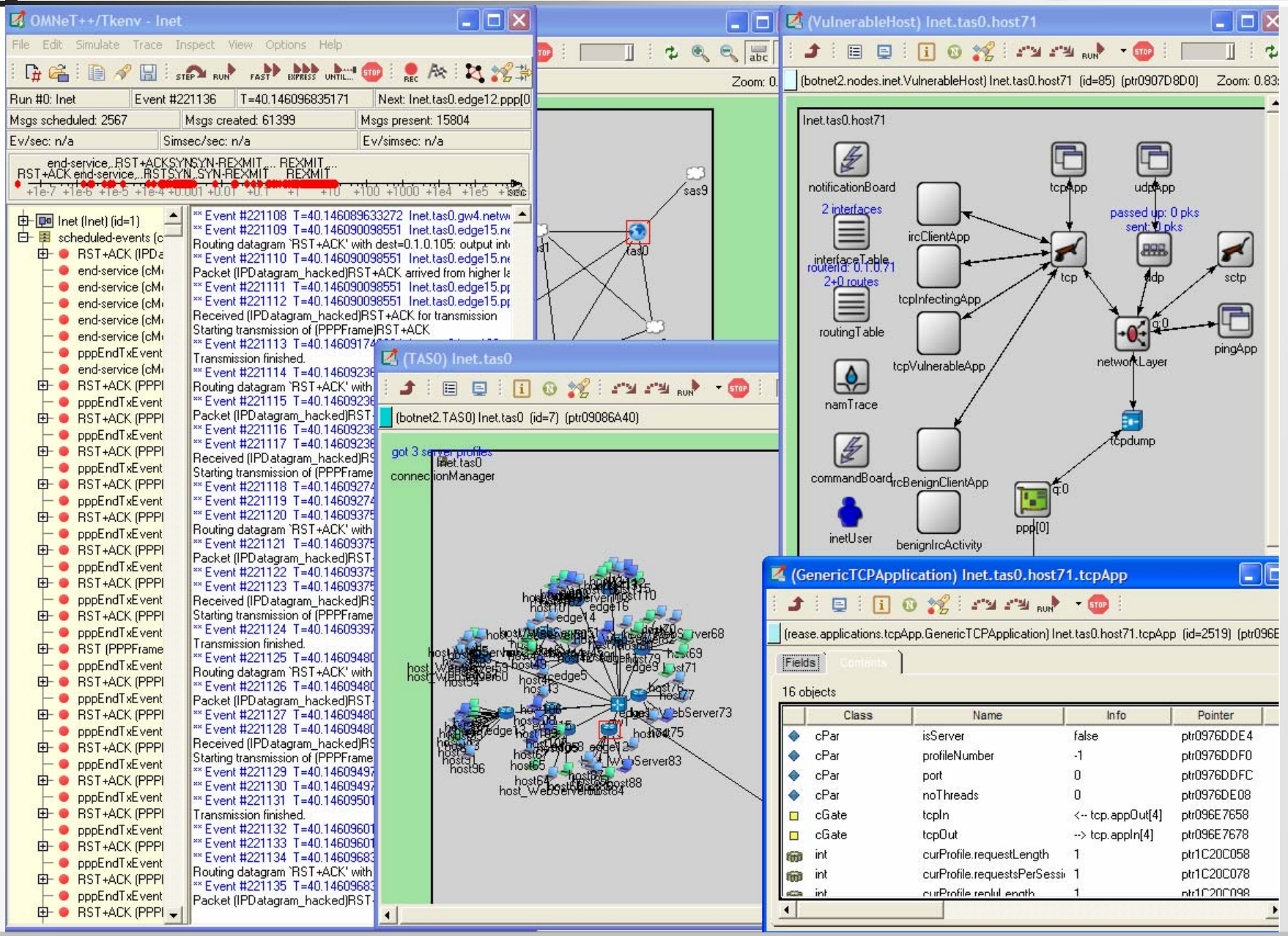
Агент «ограничитель» – ограничение трафика

Параметры моделирования

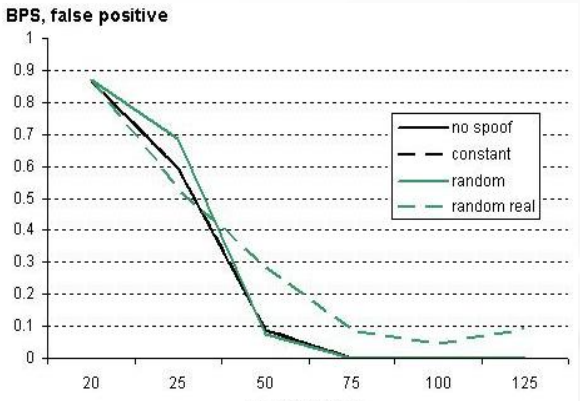
- *Топология и конфигурация сети:* количество и типы хостов и каналов связи между ними, характеристики каналов и хостов.
- *Конфигурация команд атаки:* количество демонов; адрес и порт мастера для взаимодействия; порт демона для посылки пакетов атаки; адрес и порт цели атаки; время атаки; интенсивность атаки; метод подмены адреса отправителя.
- *Параметры команд защиты*: адрес защищаемого узла, адрес и порт “детектора” для взаимодействий, размер ответа на запрос и время обработки запроса сервером; схема адаптации и т.п.
- *Параметры команды пользователей*: количество пользователей; адрес и порт сервера; время начала работы; количество, запросов, интервал между запросами, размер запросов к серверу в одном соединении; интервал между соединениями.
- *Параметры кооперации агентов защиты:* схема кооперации.
- *Параметры моделирования*: продолжительность моделирования, количество экспериментов и др.
- *Параметры атак*
- *Параметры механизмов защиты*

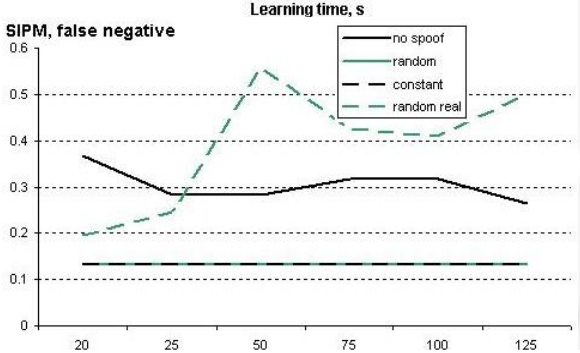
Архитектура среды моделирования на уровне пакетов

Интерфейс среды моделирования

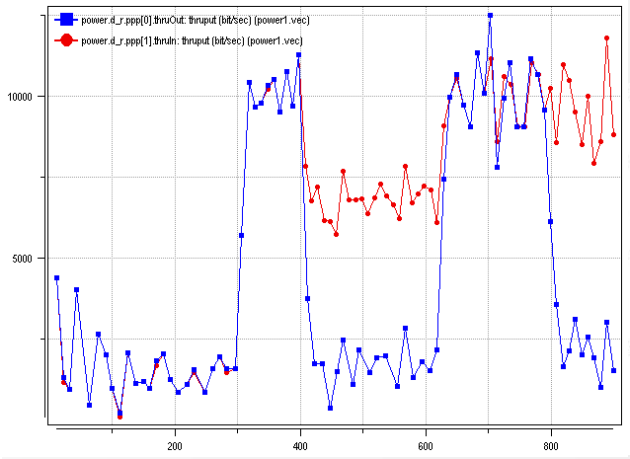


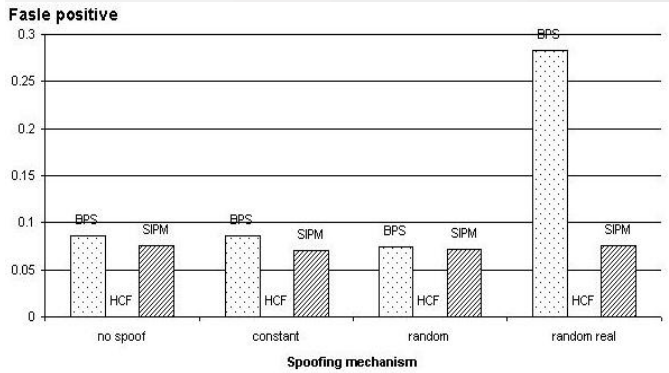
Виды экспериментов

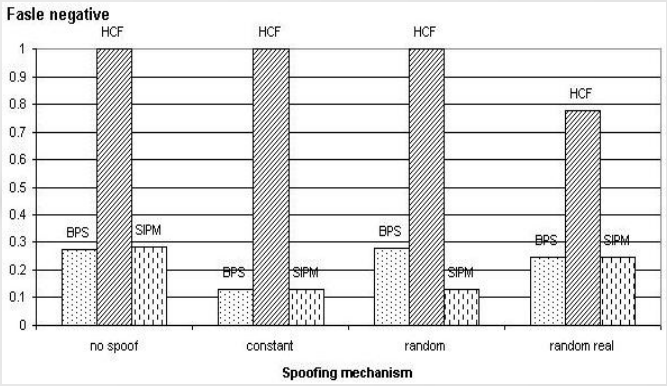




- Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак и перспективных методов защиты.
- В процессе экспериментов можно варьировать
  - топологию и конфигурацию сети;
  - структуру и конфигурацию команд атаки и защиты;
  - механизмы реализации атак и защиты;
  - параметры кооперации команд и др.







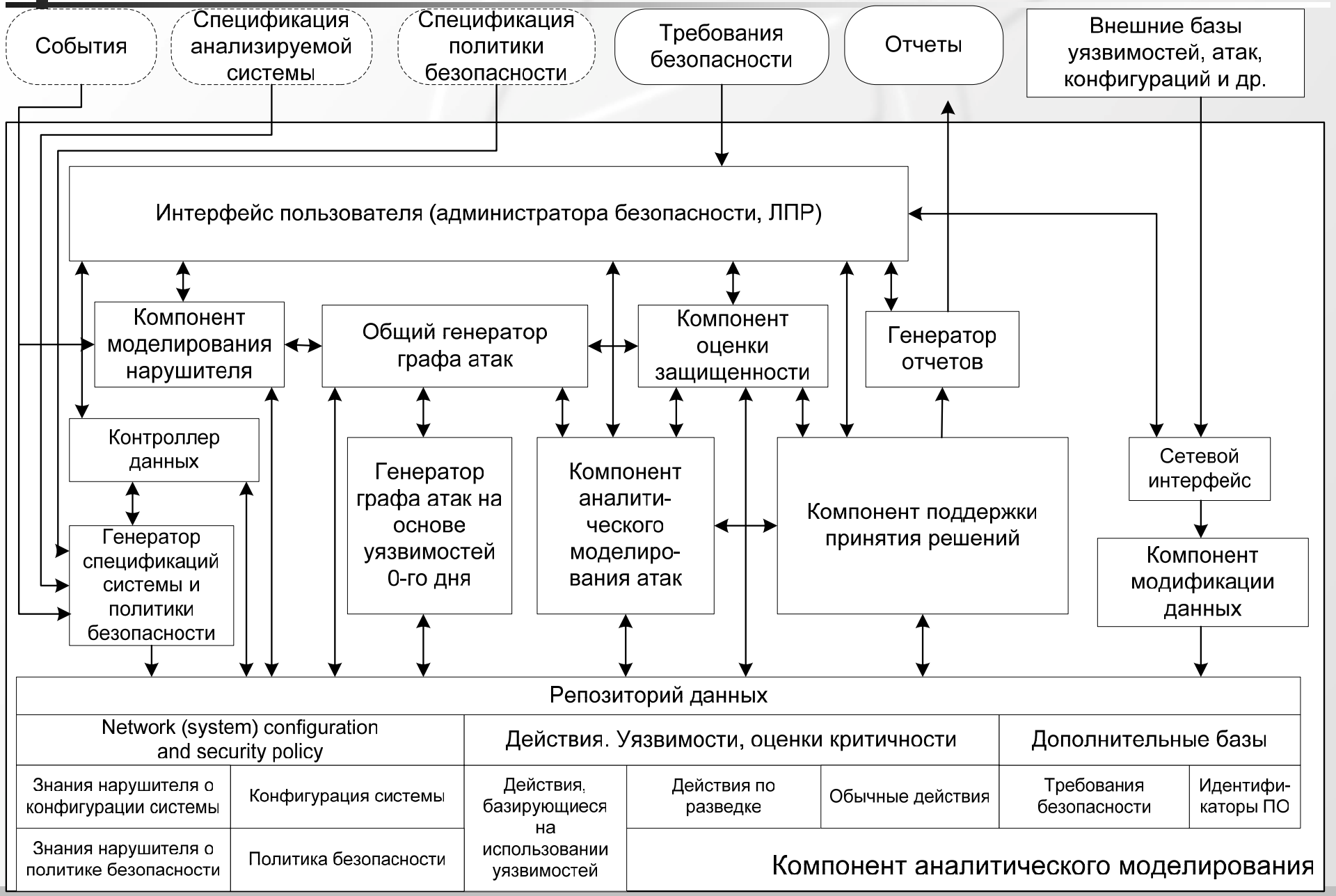
План доклада

- Введение
- Особенности моделирования механизмов кибербезопасности
- Подход к моделированию на уровне пакетов
- **Подход к аналитическому моделированию**
- Заключение

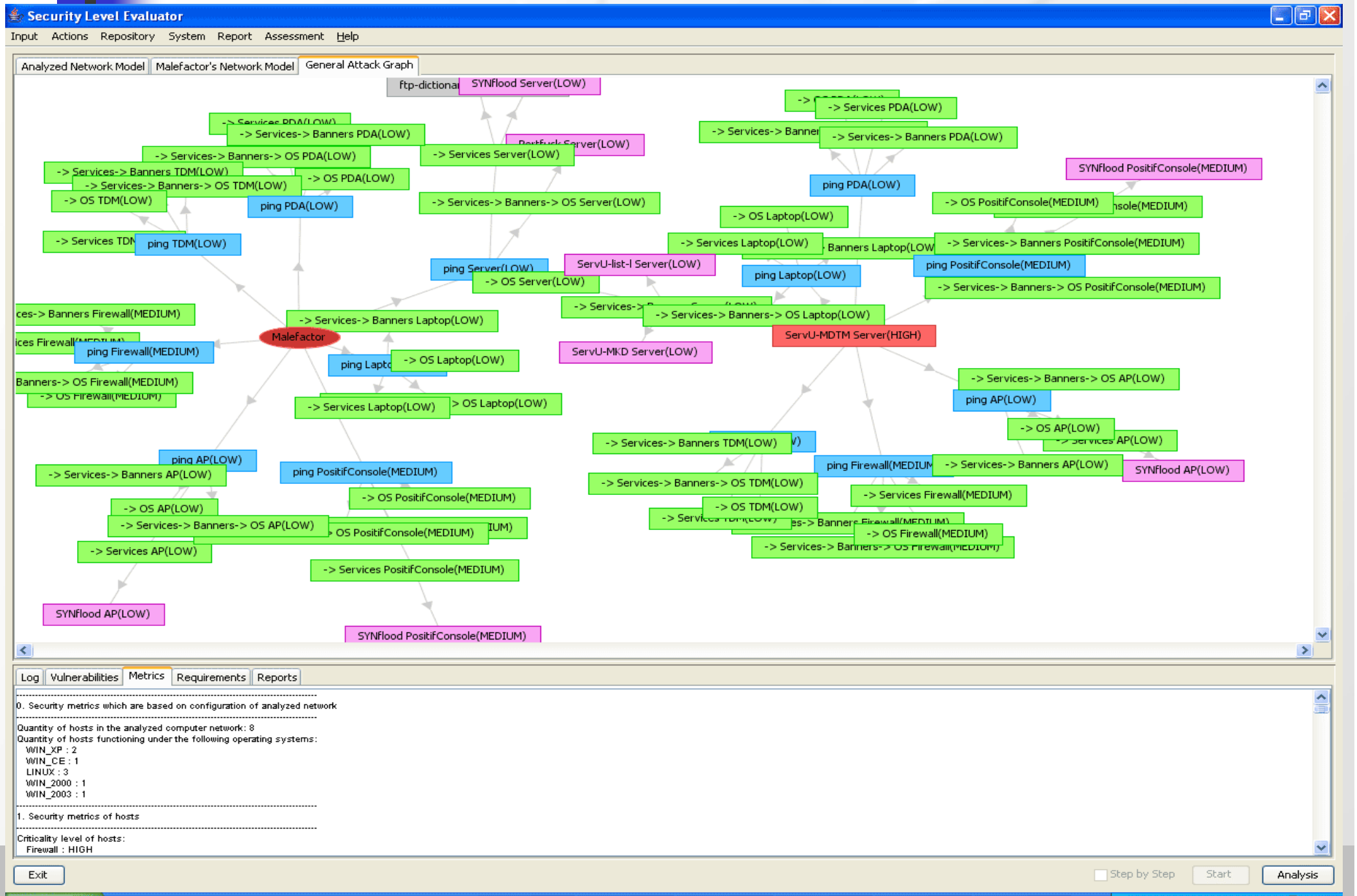
Базовые работы по моделированию атак для анализа механизмов защиты

- Проверка на модели (C.Ramakrishnan и R.Sekar, R.Ritchey и P.Ammann, O.Sheyner, S.Jha и J.Wing – SMV, NuSMV, SPIN). Требуют определить гипотезу (состояние системы), нарушение которой проверяется методом model checking
- Экспертные системы (M.Danforth – Java Expert System Shell). Правила – выполнение атакующих действий, факты – состояния системы. Атаки в виде предусловия/постусловия
- Логический подход (X.Ou, W.Boyer, M.McQueen – Datalog language). Граф состоит из вершин вывода и вершин фактов. Модель сети – множество высказываний Datalog, атаки – правила Datalog
- Графовый подход. Например C.Philips и L.Swiler строят граф: вершины – состояния системы, дуги – переходы

Архитектура компонента аналитического моделирования



Интерфейс среды моделирования



План доклада

- Введение
- Особенности моделирования механизмов кибербезопасности
- Подход к моделированию на уровне пакетов
- Подход к аналитическому моделированию
- **Заключение**

Основные результаты работы

- Представлен подход к исследованию механизмов кибербезопасности на основе интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического анализа графов атак, методов эмуляции и виртуализации сетевых процессов
- Разработаны средства моделирования, реализующие данный подход. Проведено большое количество экспериментов, показавших возможность использования предложенного подхода для моделирования механизмов кибербезопасности, а также анализа защищенности проектируемых сетей.
- Предлагаемый подход к моделированию позволяет исследовать различные механизмы построения защищенных сетей, отвечать на вопросы “Что, если…”, определять наиболее эффективные механизмы защиты.

Направления дальнейших исследований

- Совершенствование предлагаемого подхода и среды моделирования
- Анализ эффективности кооперативных механизмов взаимодействия различных команд атаки и защиты
- Исследование механизмов адаптации и самообучения (текущие механизмы подвержены манипуляции со стороны противника)
- Расширение библиотеки атак и механизмов защиты для анализа сложных сценариев взаимодействия бот-сетей и систем защиты и исследования новых механизмов защиты
- Улучшение масштабируемости и точности моделирования.
  Ведется разработка и исследование параллельной версии средств моделирования, а также разработка подхода и стенда моделирования, основанных на многорезолюционных методах моделирования. Данный подход позволяет интегрировать макро- и микро- уровневые модели бот-сетей и механизмов защиты *(аналитические, основанные на пакетах, базирующиеся на эмуляции) и реальных сетей небольшого размера.*

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), программы фундаментальных исследований ОНИТ РАН (проект № 3.2) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза Massif.

РОССИЙСКАЯ АКАДЕМИЯ НАУК