УНИВЕРСИТЕТ ИТМО

Перспективные направления применения аналитического моделирования атак для оценки защищенности компьютерных сетей

Доцент Университета ИТМО
к.т.н., доц. Андрей Чечулин

РусКрипто’2022

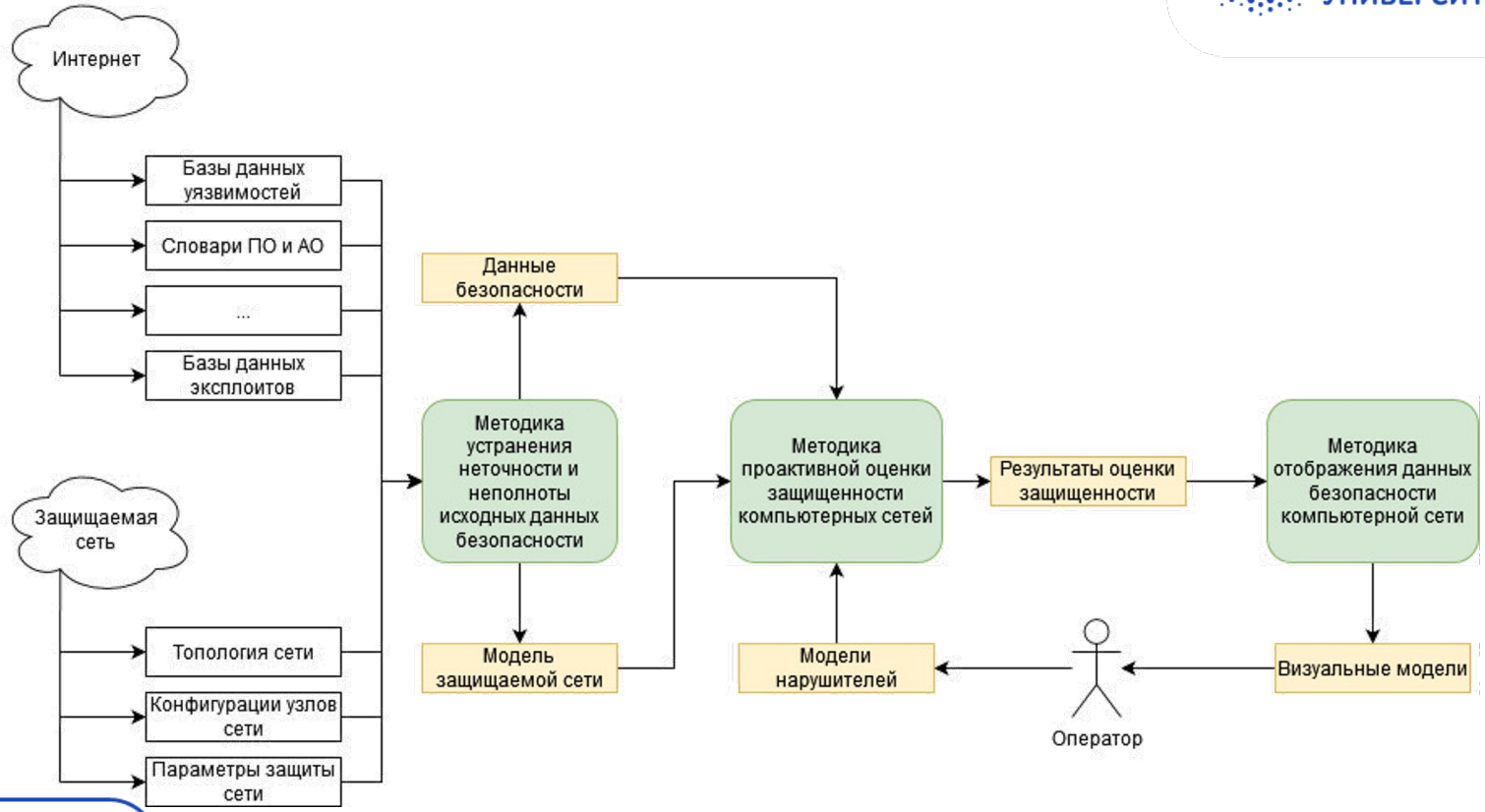
Назначение и основные функции комплекса

УНИВЕРСИТЕТ ИТМО

- импорт результатов автоматизированного сбора информации о компьютерной сети из внешних источников
- формирование в автоматизированном режиме программной модели исследуемой компьютерной сети, отражающей ее структуру и состав
- графическое отображение данной модели в виде схемы компьютерной сети
- формирование непротиворечивых данных безопасности
- определение уровня защищенности исследуемых систем
- анализ степени доверия к результатам оценки защищенности
- визуальное представление результатов для поддержки принятия решений

ITMO more than a UNIVERSITY

Общая архитектура комплекса

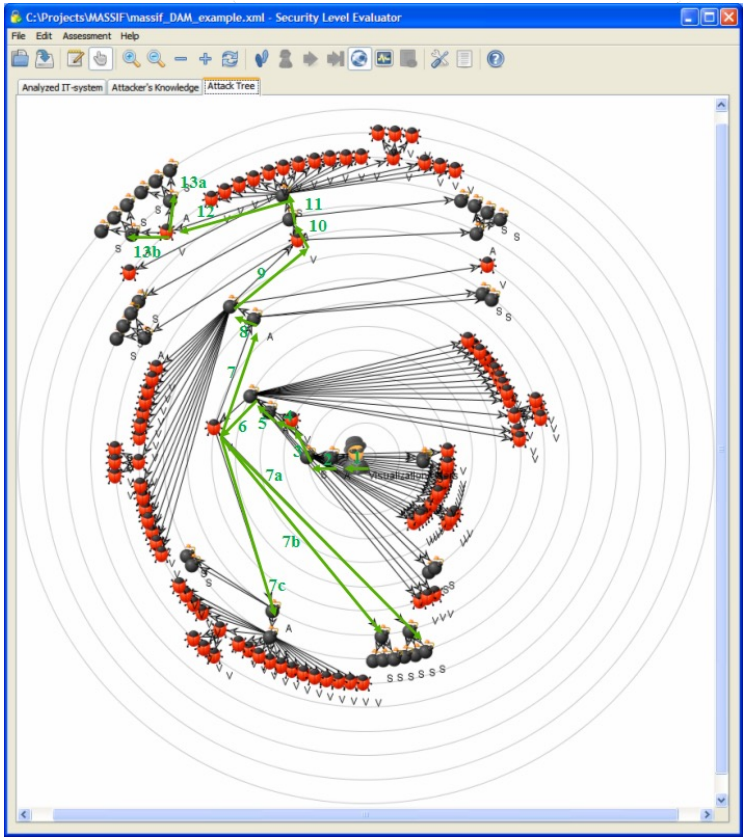


Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Оценка защищенности компьютерной сети

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о ценности информации на хостах
- Выходные данные
  - Оценка защищенности компьютерной сети
  - Слабые места компьютерной сети
  - Оценка возможного ущерба



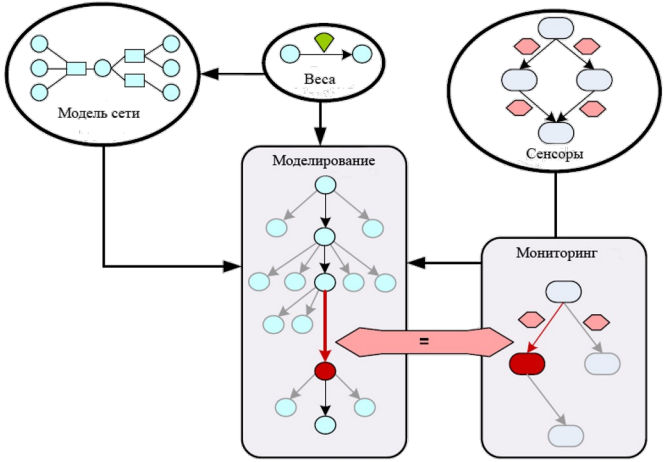
ITMOre than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Обнаружение вредоносного ПО

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о событиях безопасности
- Выходные данные
  - Оценка скорости распространения
  - Обнаружение уязвимых элементов
  - Прогноз возможного ущерба



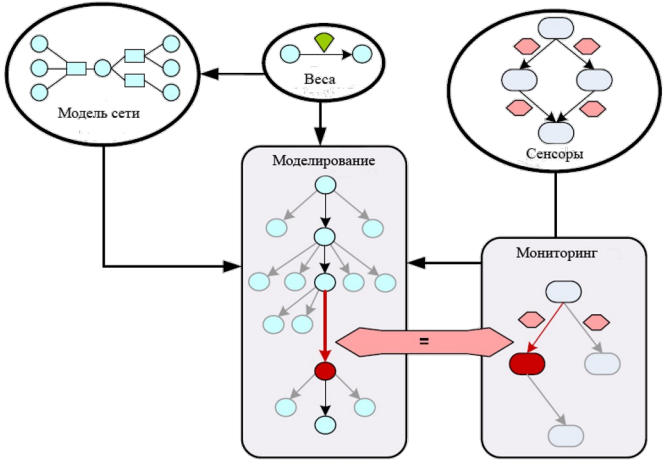
ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Обнаружение цепочек атак (APT)

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о событиях безопасности
- Выходные данные
  - Пропущенные события безопасности
  - Прогноз развития атаки
  - Прогноз возможного ущерба



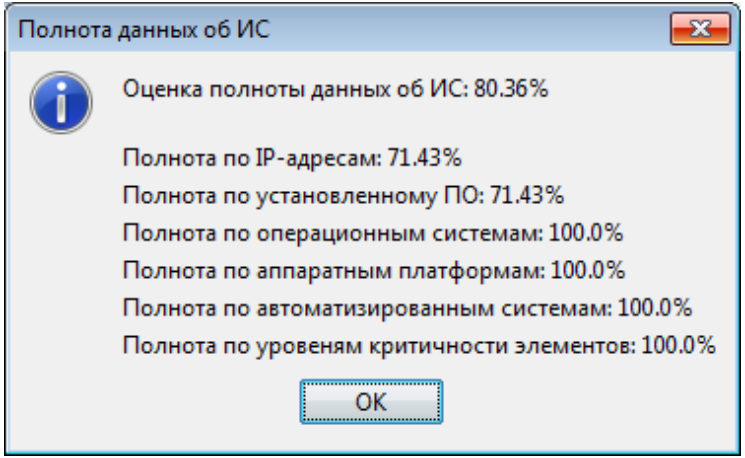
ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Анализ уязвимостей нулевого дня

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о статистике уязвимостей
- Выходные данные
  - Прогноз возможного ущерба при появлении различных уязвимостей нулевого дня



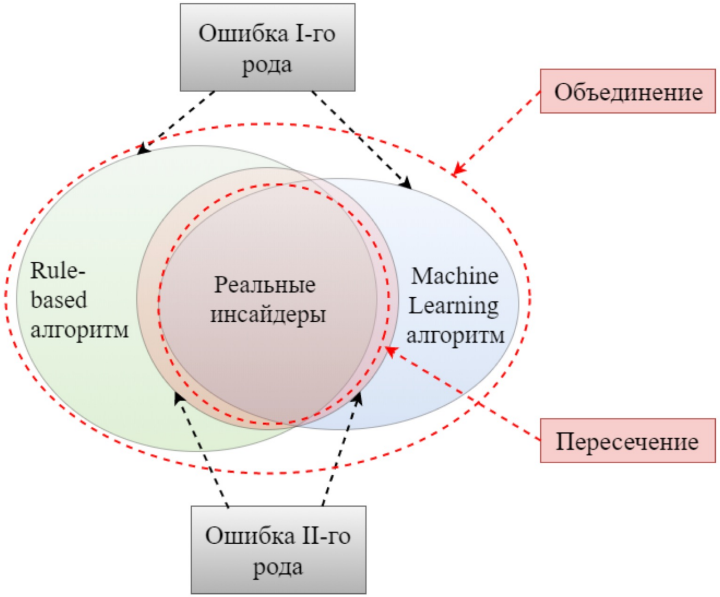
ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Анализ угроз от инсайдеров

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о правах пользователей
- Выходные данные
  - Оценка защищенности компьютерной сети от конкретных пользователей
  - Прогноз возможного ущерба



ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Анализ угроз от социоинженерных атак

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о правах пользователей
  - Характеристики пользователей
- Выходные данные
  - Оценка защищенности с учетом социоинженерных атак

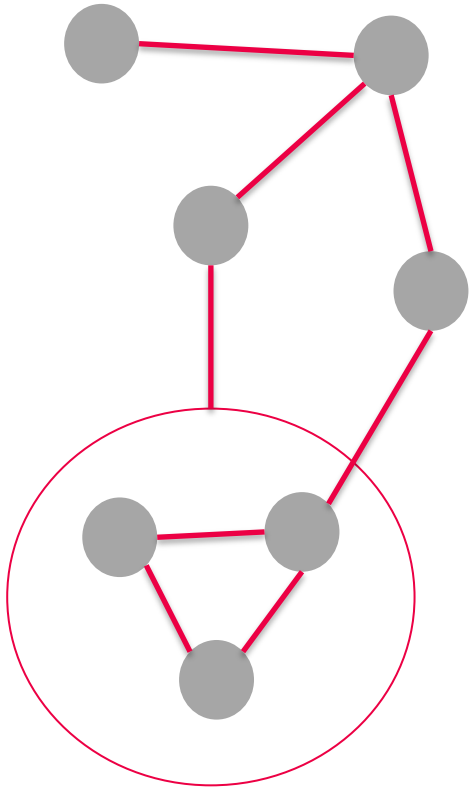
ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

Анализ виртуальных инфраструктур

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Данные о вложенности виртуальных систем
- Выходные данные
  - Оценка защищенности с учетом атак побега из виртуальной среды и возможности прямого обращения к оборудованию



ITMO more than a UNIVERSITY

Области применения моделирования

УНИВЕРСИТЕТ ИТМО

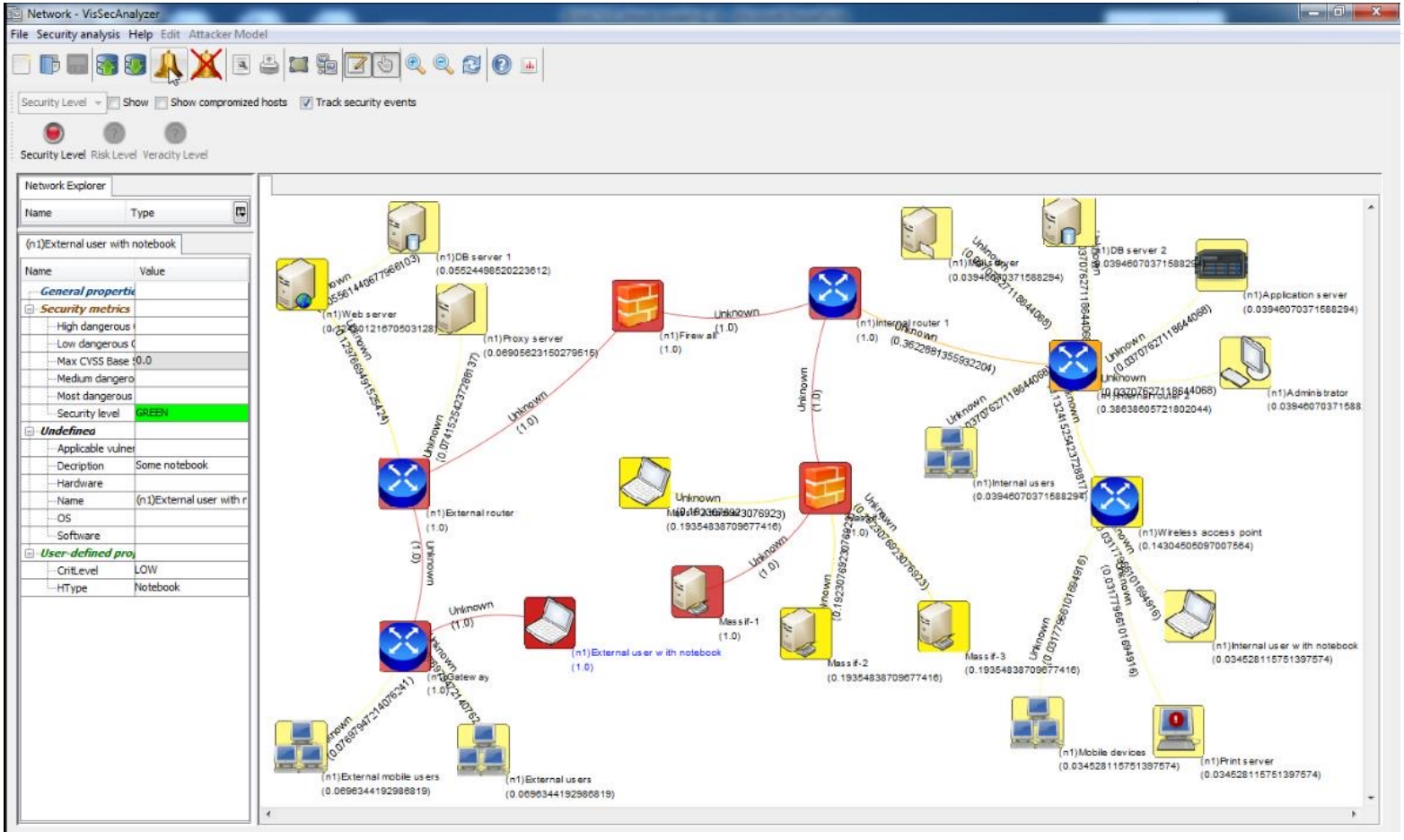
Оценка эффективности контрмер

- Входные данные:
  - Данные о топологии компьютерной сети, отдельных хостах и системе безопасности
  - Данные об известных уязвимостях из открытых и внутренних баз данных
  - Списки возможных контрмер
- Выходные данные
  - Оценка защищенности после контрмер
  - Оценка контрмер по соотношению цена/эффект для безопасности

ITMO more than a UNIVERSITY

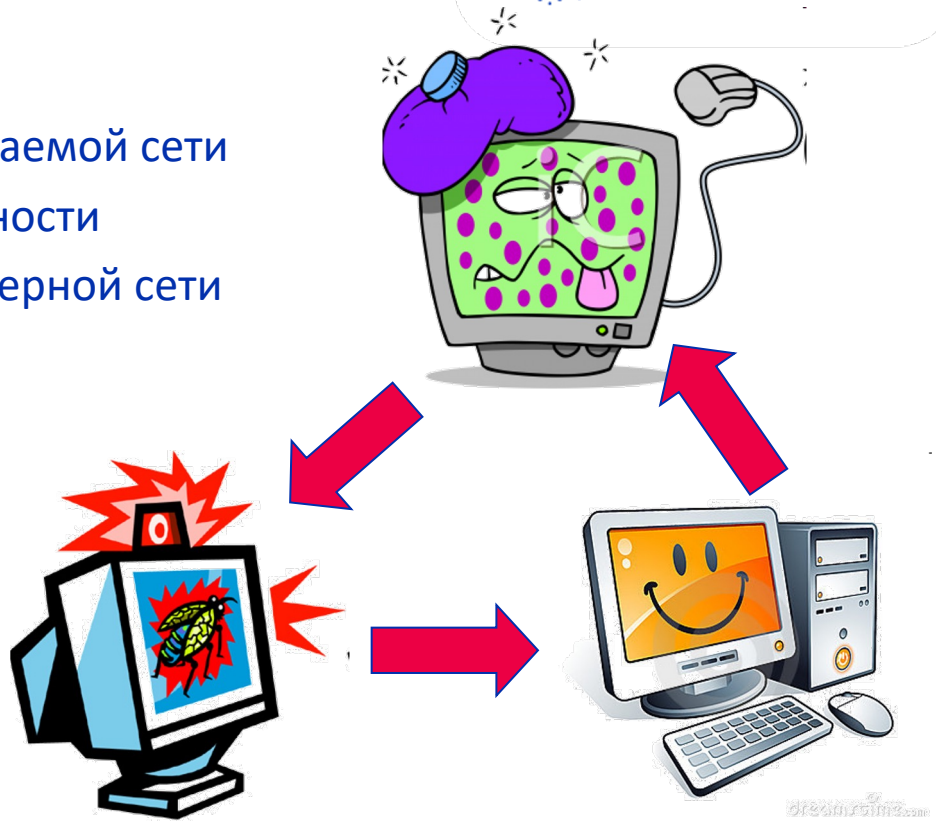
Пример интерфейса системы

УНИВЕРСИТЕТ ИТМО



Заключение

- Основные шаги
  - Сбор исходных данных о защищаемой сети
  - Сбор исходных данных безопасности
  - Оценка защищенности компьютерной сети
  - Представление результатов
- Проблемы
  - Неполнота
  - Противоречивость
  - Изменчивость
  - Объем
  - Разнородность



Спасибо за внимание!

доц., к.т.н. Чечулин Андрей Алексеевич
achechulin@itmo.ru

ITMO more than a UNIVERSITY