УНИВЕРСИТЕТ ИТМО

Автоматизация оценки защищенности компьютерных сетей

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

РусКрипто’2022

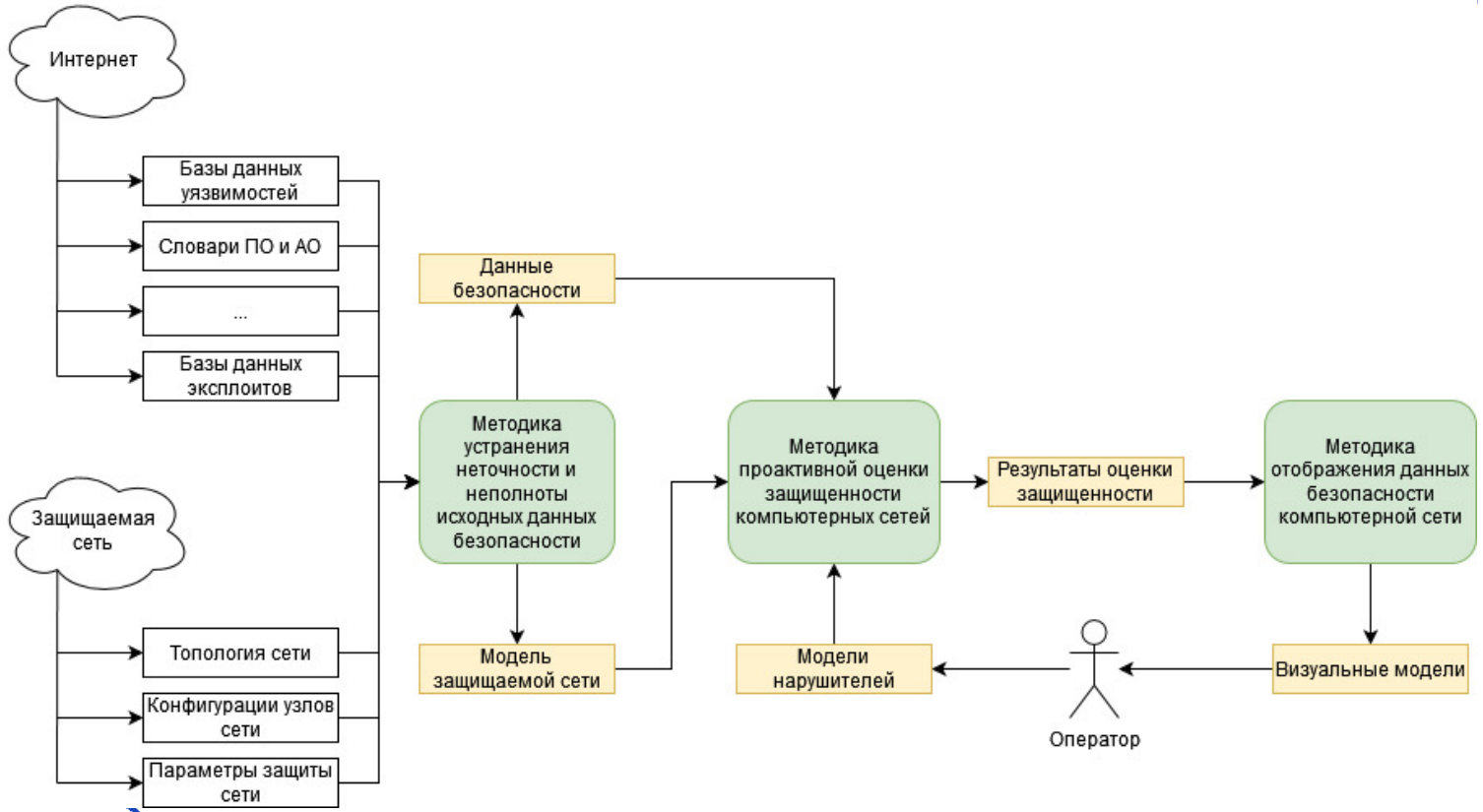
Назначение и основные функции комплекса

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

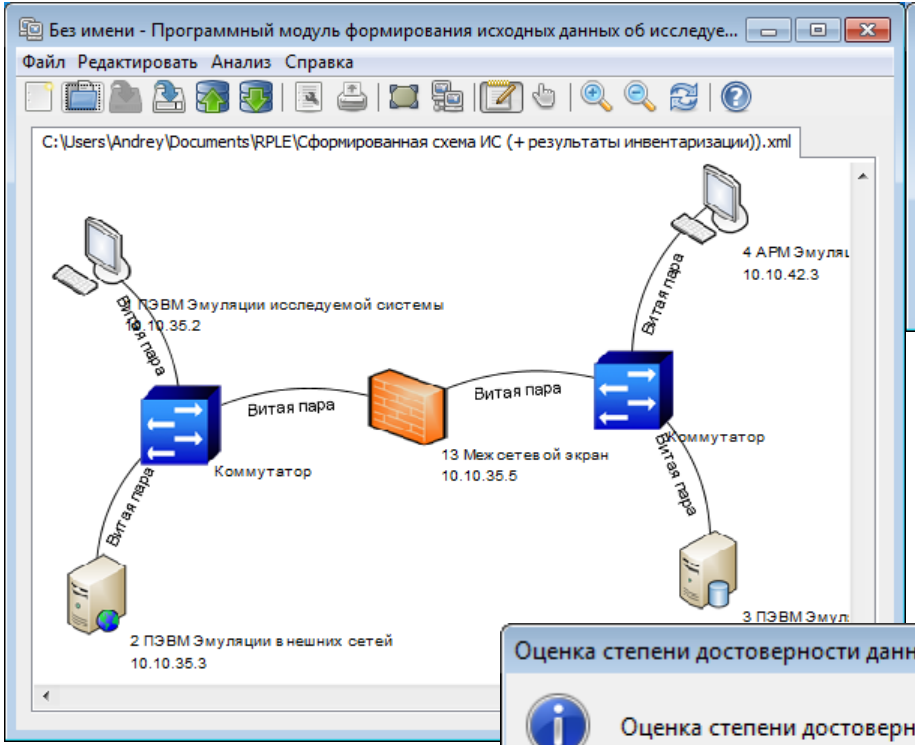


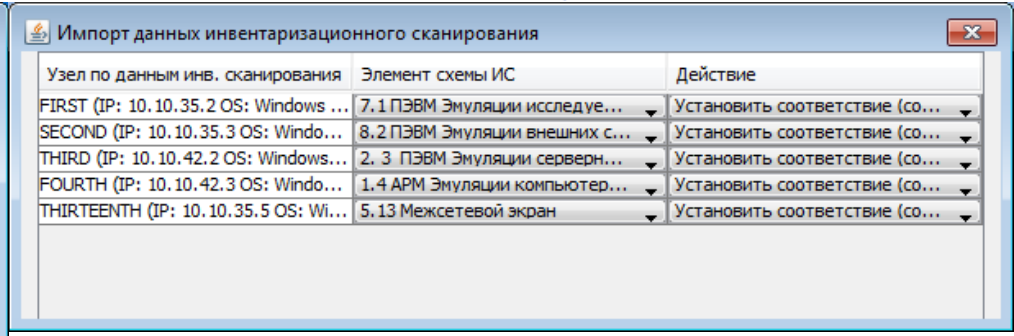
Входные данные (1/4)

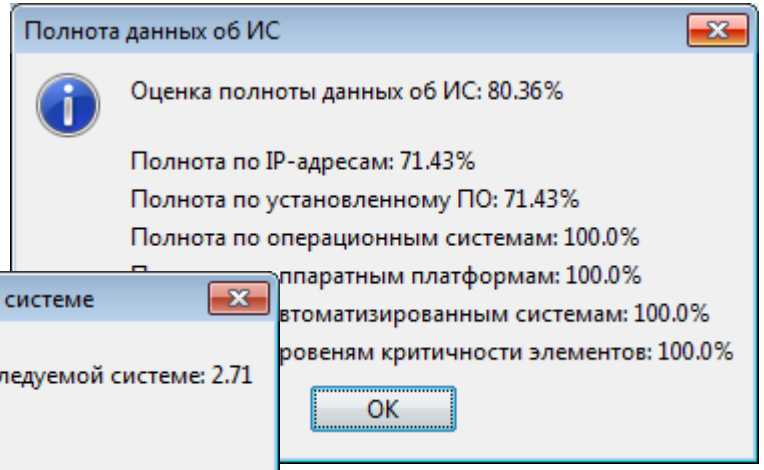
- Внутренние входные данные
  - Отчеты сканеров безопасности (Nmap, Nessus, MaxPatrol)
  - Сбор данных с сетевого оборудования
  - Сбор данных от агентов
  - Сбор данных от систем безопасности
  - Знания оператора
  - Параметры моделей нарушителя (задаются оператором)
- Проблемы
  - Противоречивость
  - Неполнота
  - Сложность внедрения агентов и проведения сбора данных

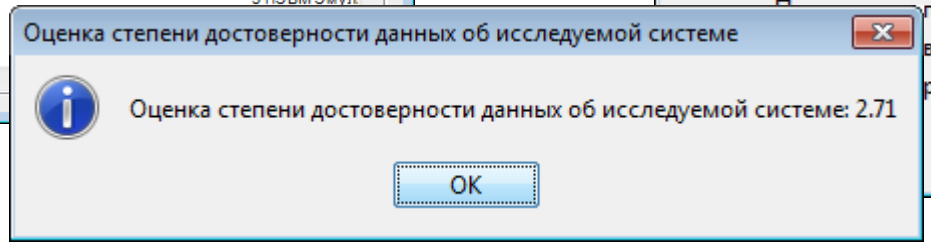
Входные данные (2/4)

УНИВЕРСИТЕТ ИТМО





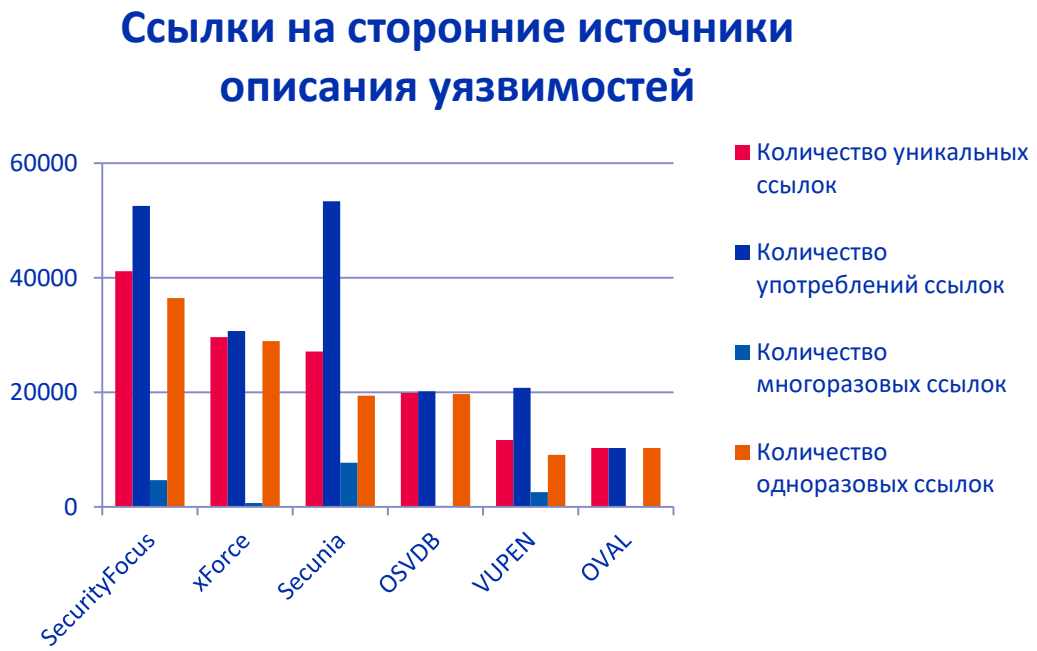




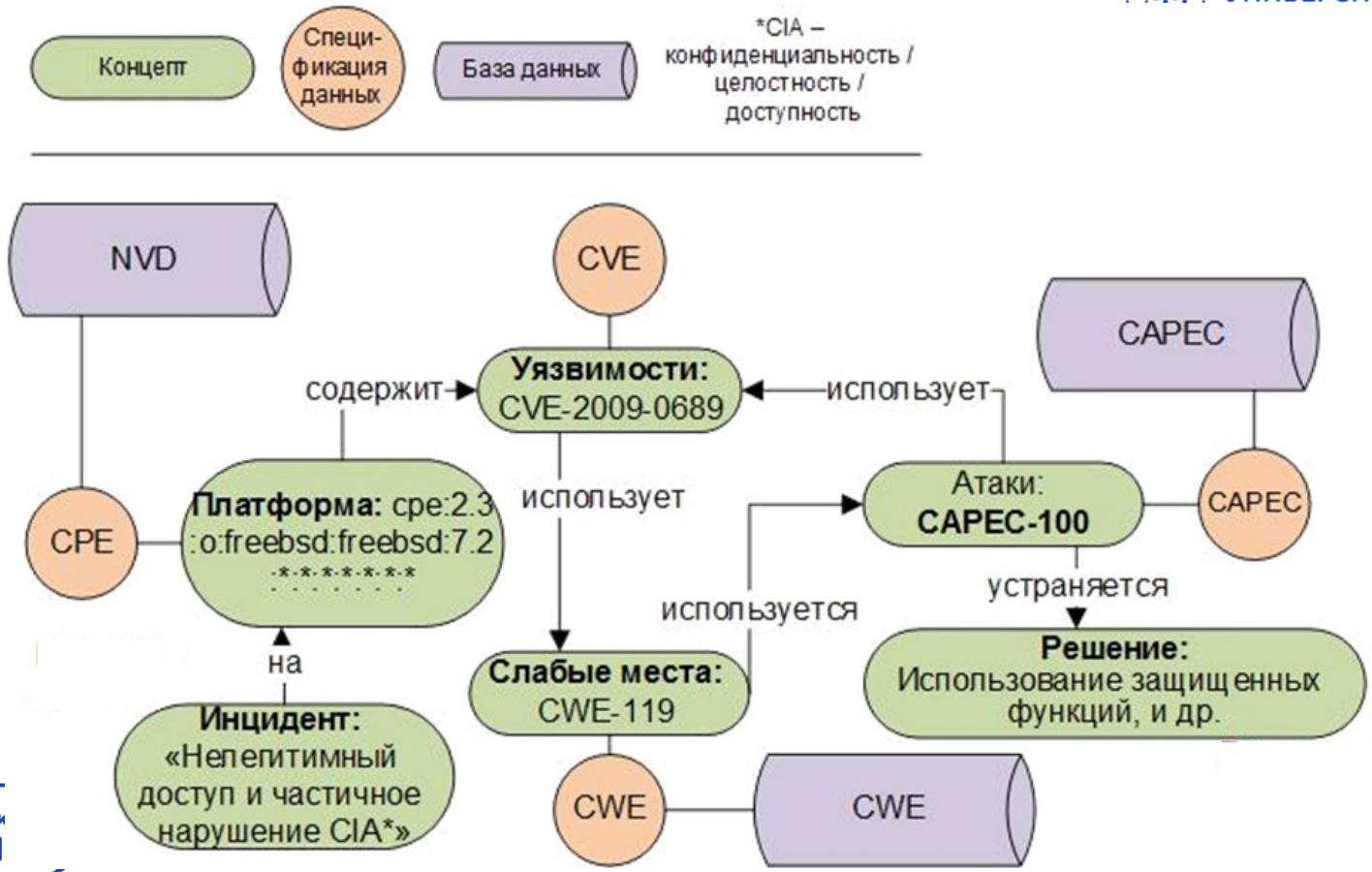
ITMO more than a UNIVERSITY

Входные данные (3/4)

- Внешние входные данные
  - Базы данных уязвимостей
  - Словари ПО и АО
  - Базы данных эксплоитов
  - Базы данных атак
- Проблемы
  - Противоречивость
  - Неполнота
  - Ограниченность доступа
  - Обновления

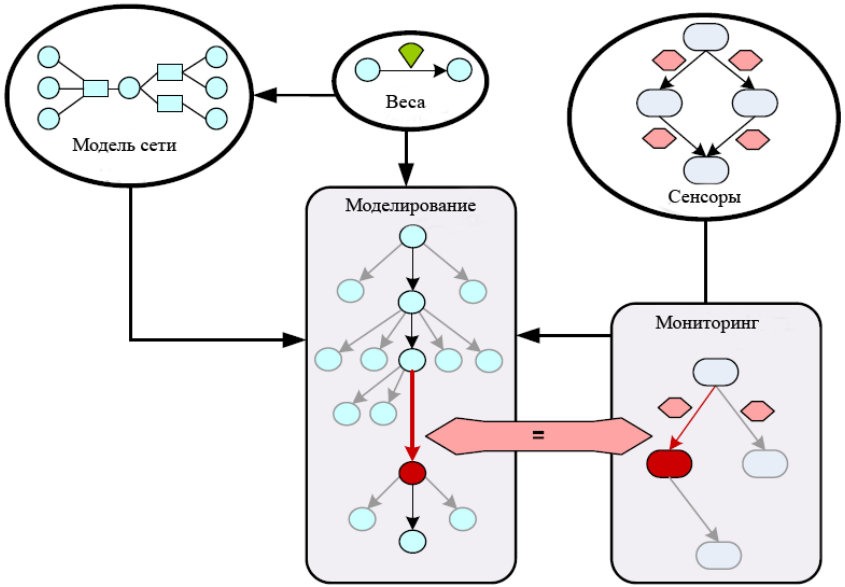


Входные данные (4/4)



Оценка защищенности (1/2)

- Входные данные
  - Данные об оцениваемой компьютерной сети
  - Данные о возможных нарушителях
  - Данные безопасности
- Проблемы
  - Изменчивость
  - Объем данных
  - Разнородность данных



Оценка защищенности (2/2)

Знания оператора

Модель сети

Спецификация

Расчет базовых метрик

Не real-time режим

Уязвимости

Деревья атак

Результаты моделирования

Базовые метрики

События в реальном времени

Обновленные деревья атак

Деревья атак

Расчет метрик защищенности

Режим anytime

Сценарии

Режим real-time

События в реальном времени

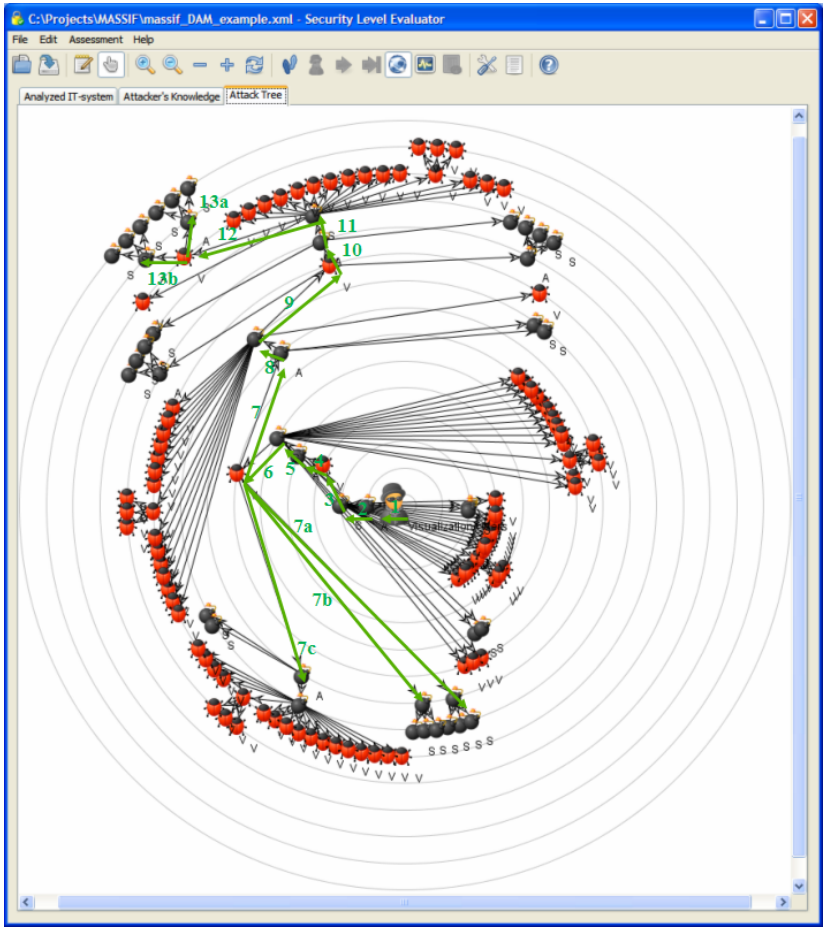
Определение сценариев атак

Рекомендации

Представление результатов (1/2)

УНИВЕРСИТЕТ ИТМО

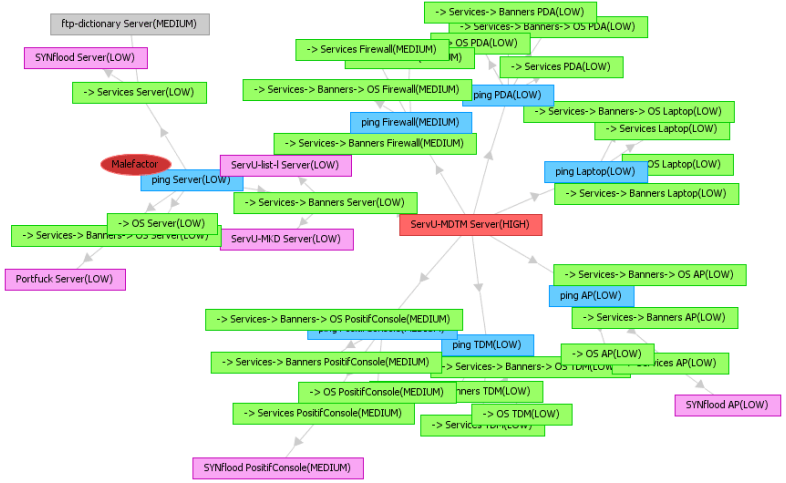
- Входные данные
  - Оценки защищенности
  - Модель компьютерной сети
  - Модели атак
- Проблемы
  - Объем данных
  - Важность данных
  - Слабость когнитивного аппарата оператора

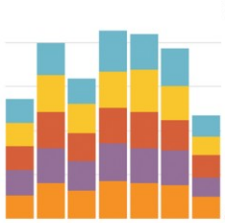


ITMOre than a UNIVERSITY

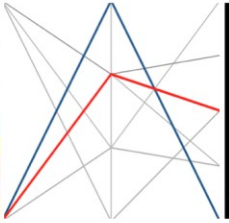
Представление результатов (2/2)

УНИВЕРСИТЕТ ИТМО

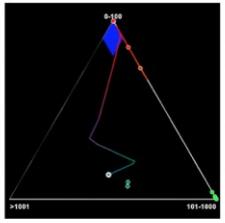




А. График

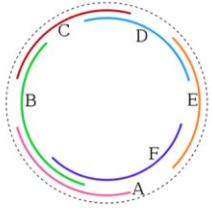


Б. Параллельные координаты



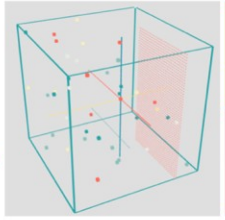
В. Трилинейные координаты

Г. Розы ветров

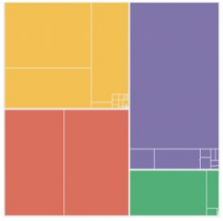


Д. Интервальные графы

Е. Графы

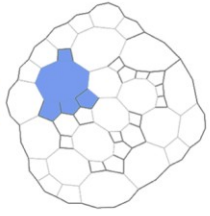


Ж. Матрицы

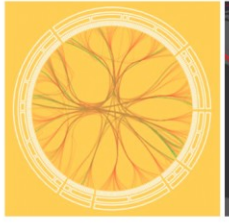


З. Карты деревьев

И. Глифы



К. Диаграммы Вороного



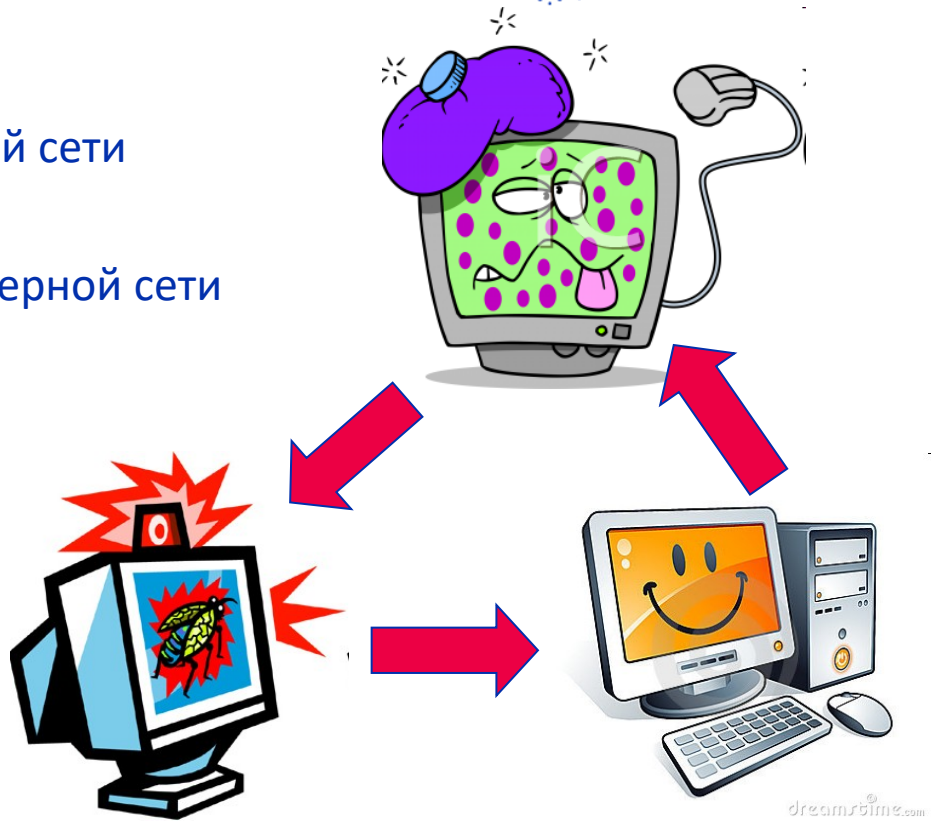
Л. Диаграммы Чорда

М. Гео-карты

ITMOre than a UNIVERSITY

Заключение

- Основные шаги
  - Исходные данные о защищаемой сети
  - Исходные данные 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

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

ITMO more than a UNIVERSITY