



ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ



2013

CEE-SEC(R)

Разработка ПО

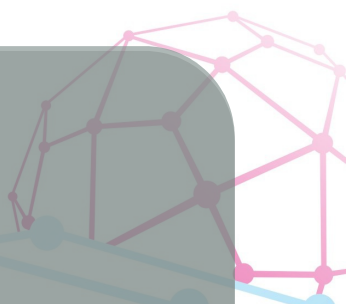
Моделирование WAN-сетей для исследования вредоносного ПО

Антоненко Виталий
ЦПИ КС, программист-
разработчик


24 октября 2013



Мотивация



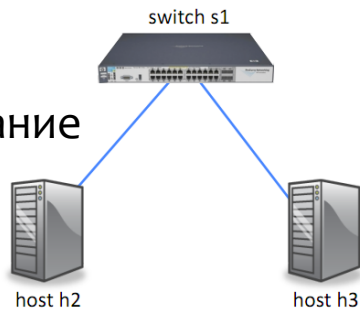
Создание среды разработки и отладки приложений для контроллера ПКС сети.



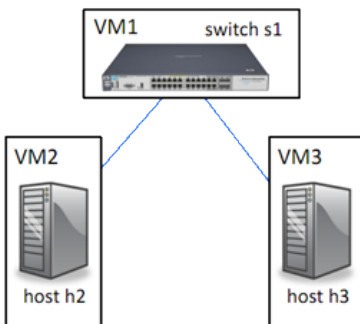
Разработка системы моделирования сетевой структуры и сетевой активности.

Моделирование компьютерной сети

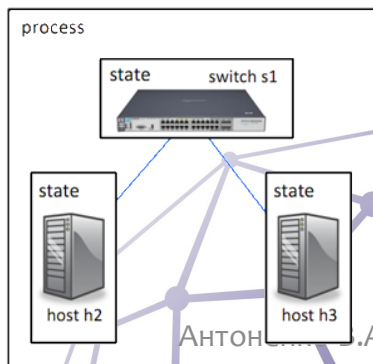
Физическое оборудование



Эмуляция



Моделирование



ЗА:

- высокая степень доверия

ПРОТИВ:

- плохая масштабируемость

ЗА:

- высокая степень доверия
- нет необходимости покупки оборудования

ПРОТИВ:

- высокие требования к ресурсам

ЗА:

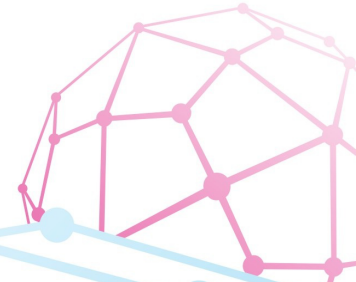
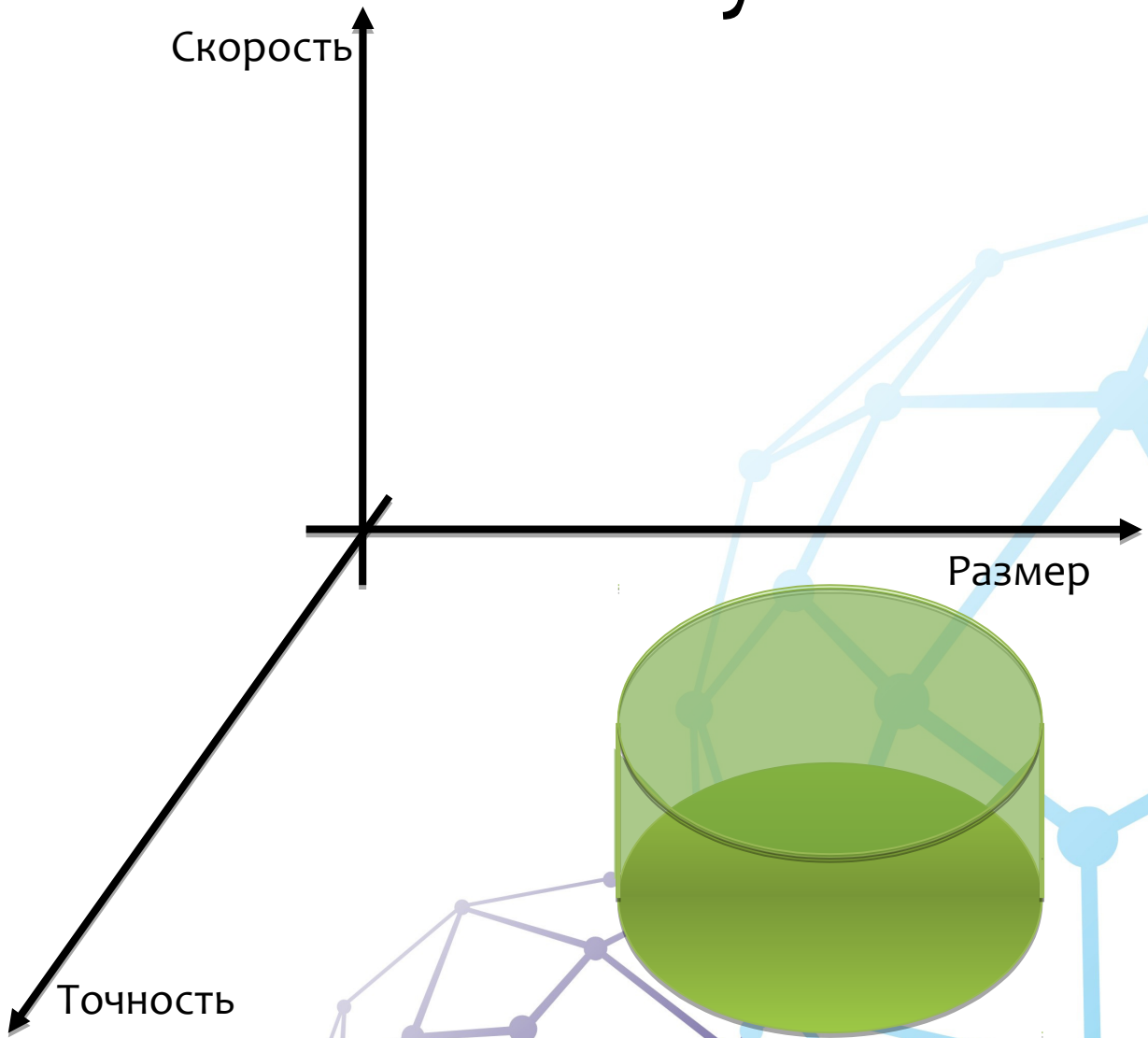
- пониженные требования к ресурсам

ПРОТИВ:

- необходимость доказывать корректность и адекватность модели

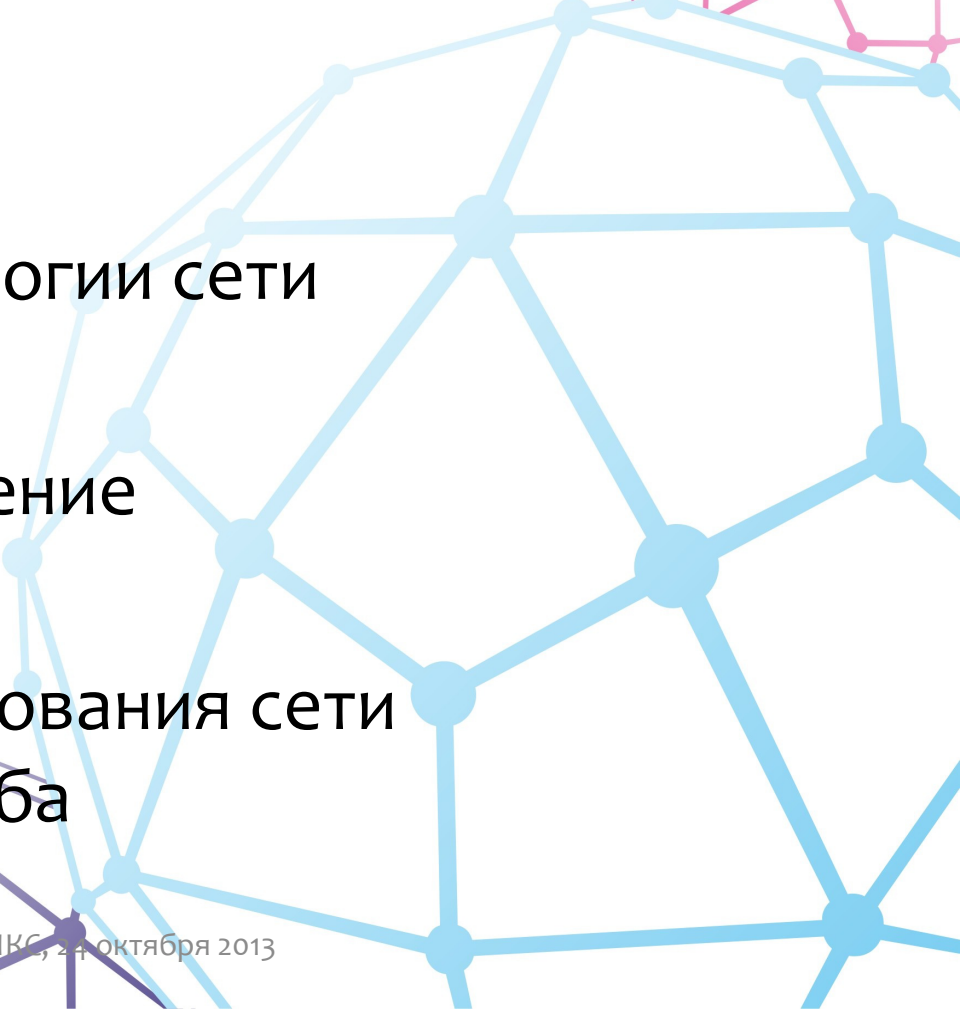


Что хотелось получить?

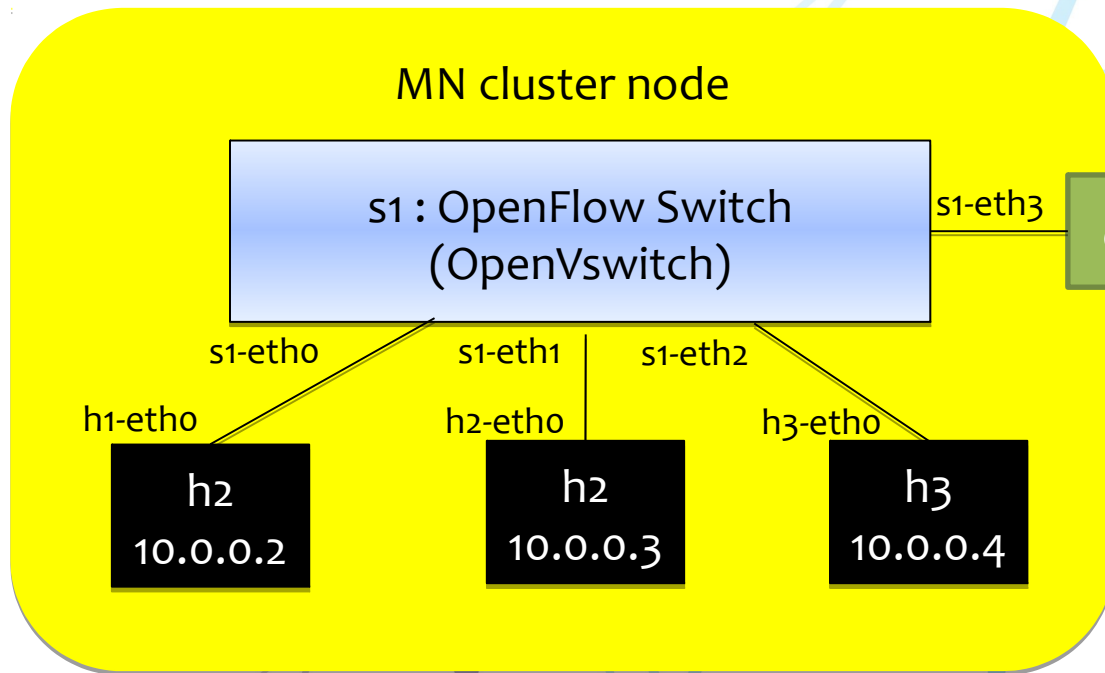




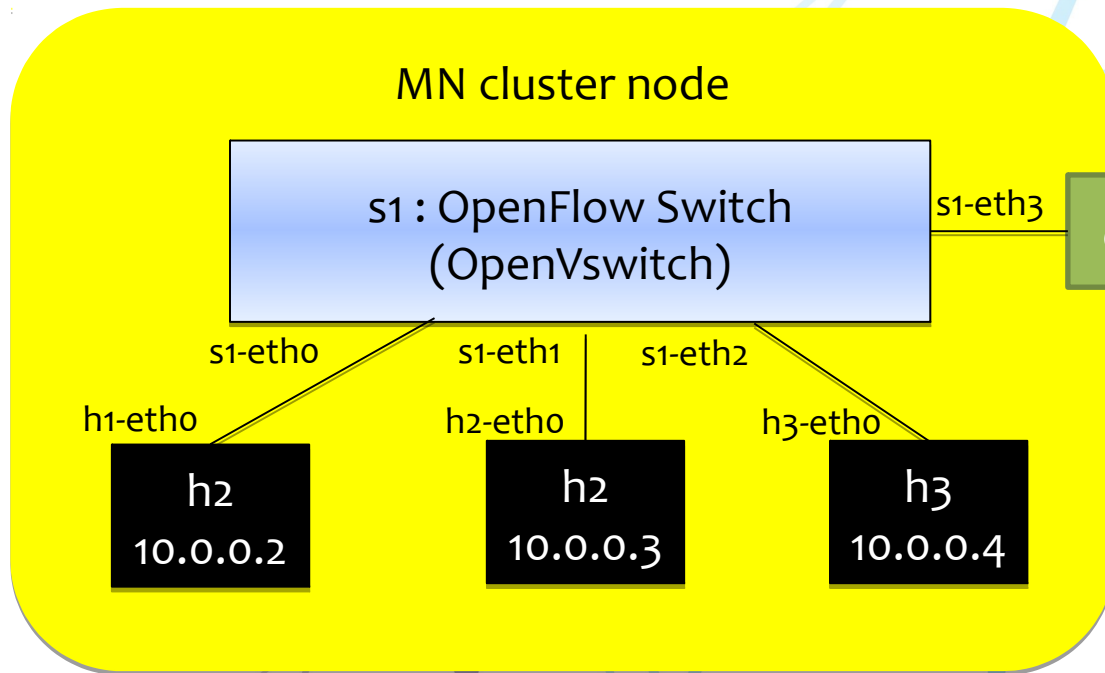
Решение – MNCE (Mini Network Cluster Edition)

- Виртуальная сеть на локальном ПК или кластере компьютеров
 - Гибкое создание топологии сети
 - Масштабируемое решение
 - Возможность моделирования сети регионального масштаба
- 

Архитектура MNCE



Архитектура MNCE



Архитектура MNCE

MN Supervisor Console

SSH

SSH

SSH

SSH

SSH

SSH

**Где моделирование
вредоносного ПО?**

MN cluster node

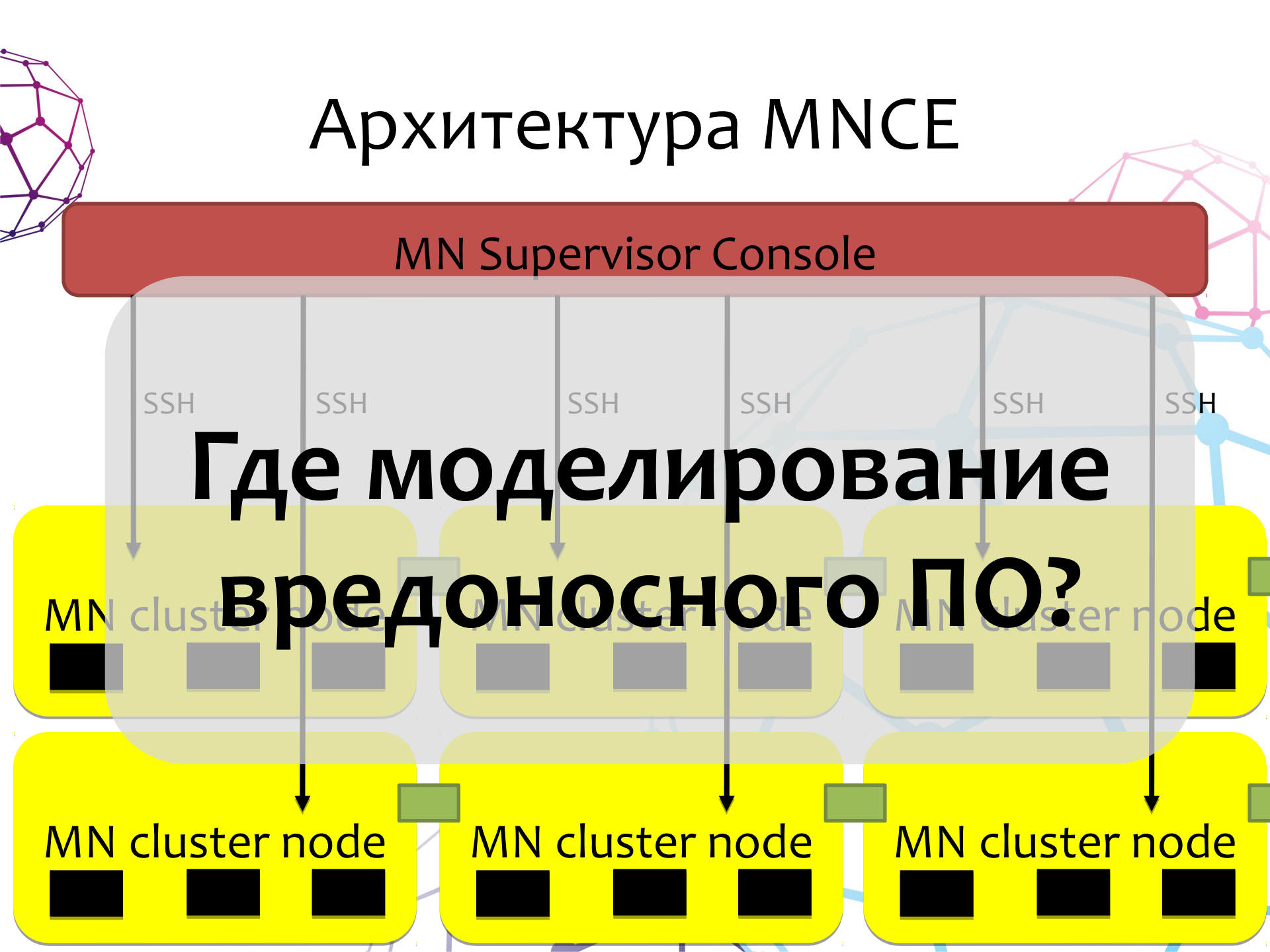
MN cluster node

MN cluster node

MN cluster node

MN cluster node

MN cluster node



Распространения сетевого червя



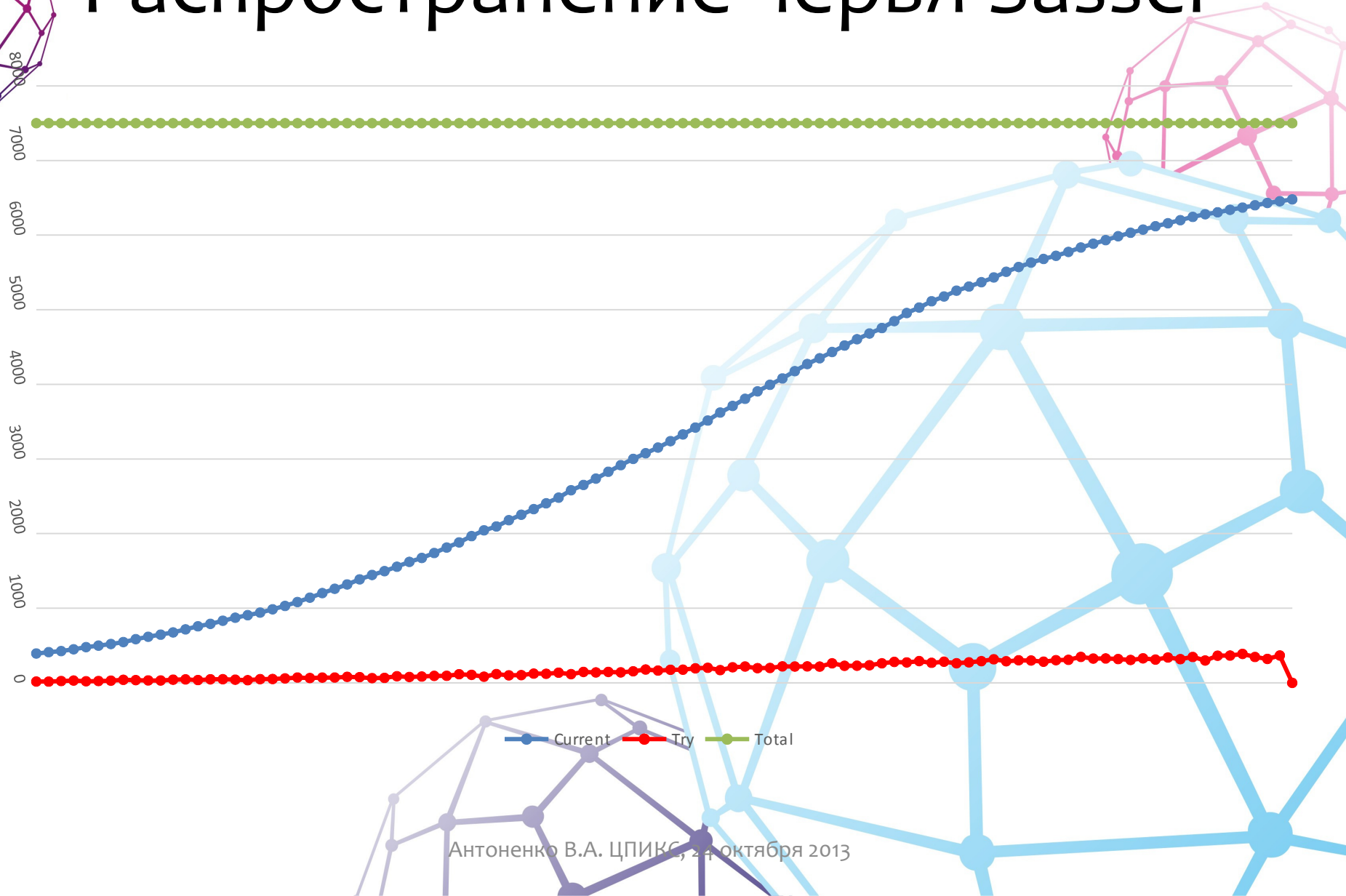
Графический интерфейс MNCE

The image displays the Mininet CE Graph Editor interface. The main window shows a network graph with nodes labeled h1 through h74 and s1 through s70. The nodes are color-coded: blue for 10.211.55.11, green for 10.211.55.12, and red for 10.211.55.13. The interface includes a menu bar with options like 'live', 'options', 'undo', 'reset', 'visualization', 'world map', and 'result'. A terminal window on the left shows the Mininet CE console output, including messages like 'Configuring loggers', 'Taking modelist from config file', 'Preparing graph', 'Opening SSH connections to all nodes in cluster', 'Splitting network graph into components', 'Sending scripts to nodes', 'Executing start up scripts on nodes', and 'Configuring host-processes eth interfaces'. The terminal output concludes with 'Setting up cluster for 18.6227149963 sec. Welcome to Mininet CE console!'.

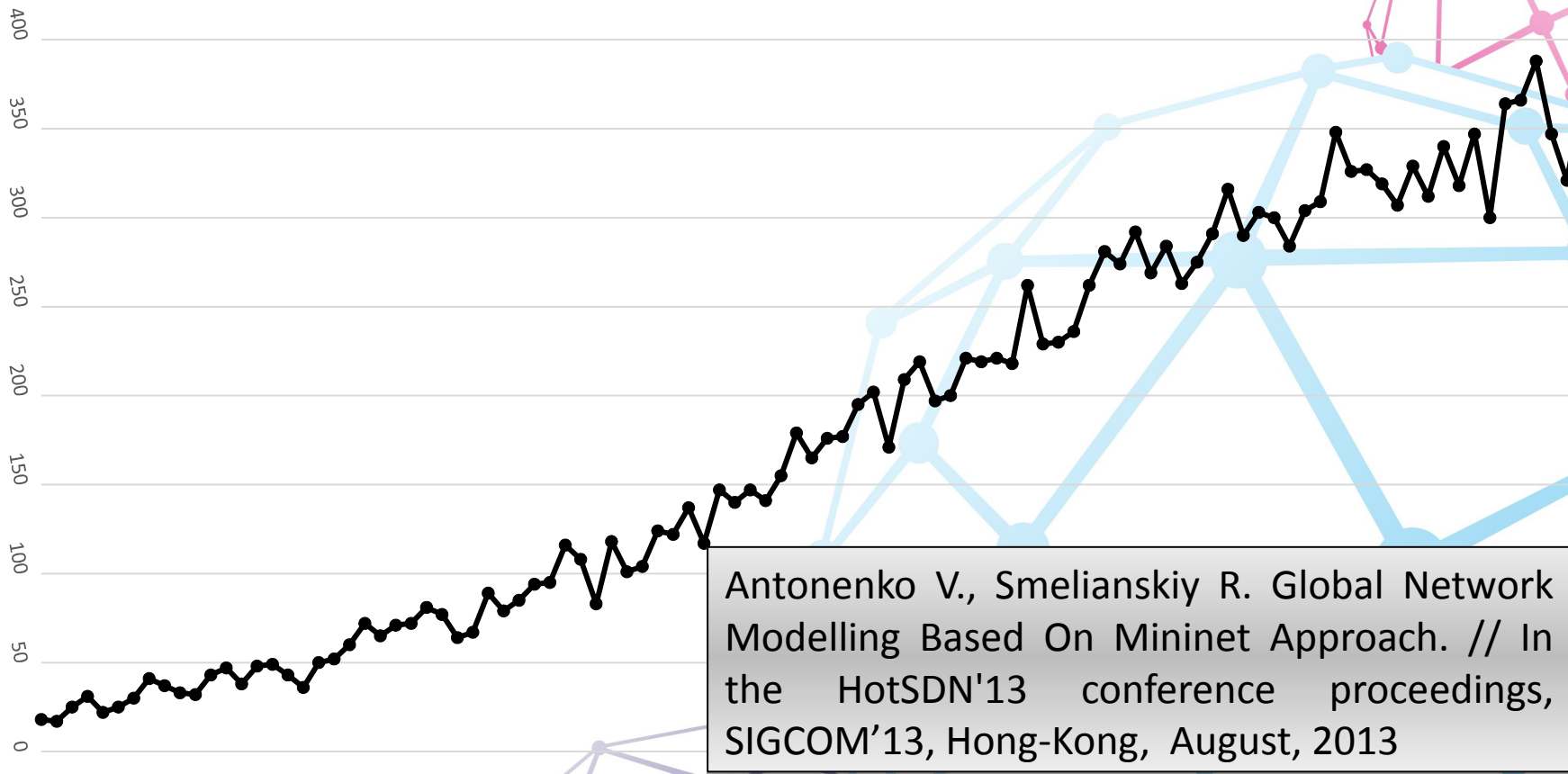
Open Source
anvi.al.github.io/MininetClusterEdition

Антоненко В.А. ЦПИКС, 21 октября 2013

Распространение червя Sasser



Распространение червя Sasser



Масштаб сети MNCE

MN Supervisor Console

SSH

SSH

SSH

SSH

SSH

SSH

MN cluster node

MN cluster node

MN cluster node

MN cluster node

MN cluster node

MN cluster node

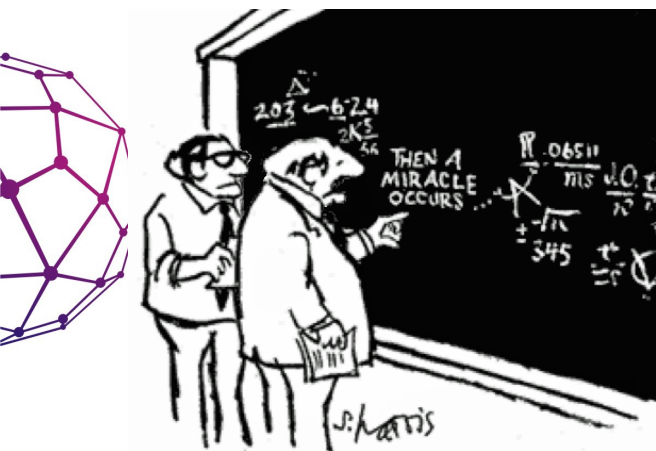
Количество процессов хостов на одном узле кластера: до **2000**

Количество процессов хостов на одном узле кластера при проведении экспериментов: от 250 до **1000**

Количество узлов кластера на одном сервере: **15**

Количество доступных серверов: **2**

ИТОГО: ~ 30 тыс. узлов в графе сети



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

SI?

Антоненко Виталий

vantonenko@arccn.ru



APPLIED
RESEARCH
CENTER FOR
COMPUTER
NETWORKS

www.arccn.ru



@arccnnews



anvial.github.io/MininetClusterEdition



Спасибо за внимание!

Антоненко Виталий
vantonenko@arccn.ru



APPLIED
RESEARCH
CENTER FOR
COMPUTER
NETWORKS

www.arccn.ru



@arccnnews



anvial.github.io/MininetClusterEdition

Антоненко В.А. ЦПИКС, 24 октября 2013