конференция
РусКрипто'2013
http://www.ruscrypto.ru/conference/

Обеспечение устойчивости функционирования распределенных многоагентных систем в сети Интернет в условиях целенаправленного разрушающего воздействия

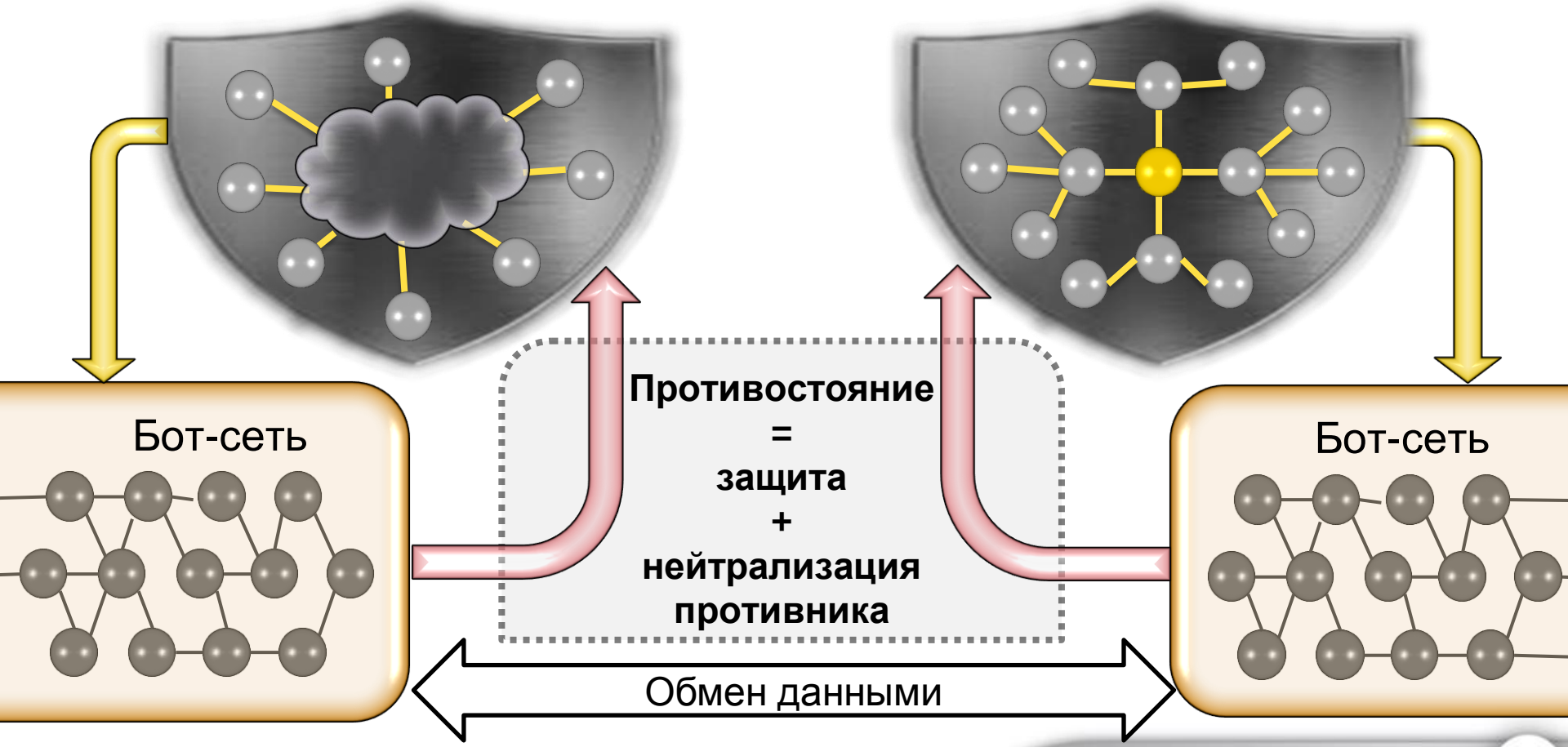
Степанова Т. В.

Противостояние бот-сетей и систем защиты

НЕОБИТ

Системы защиты:

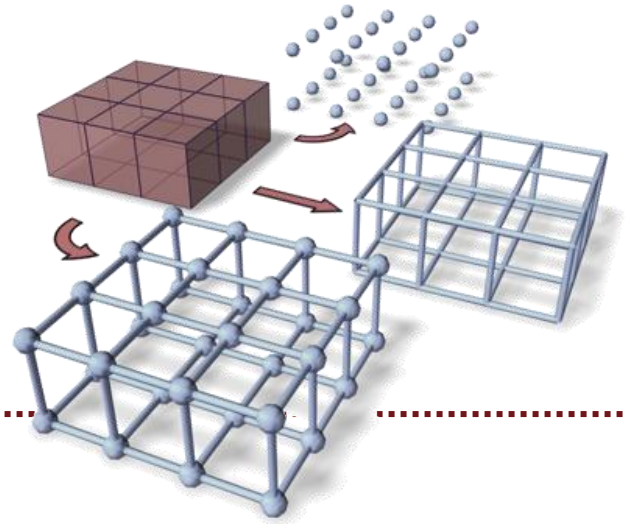
Kaspersky Security Network, ESET Live Grid, Panda Cloud Antivirus, …



Модель противостояния распределенных систем

Описание всех систем-участников

Система моделирования



Базовая сеть	$Net_B = (V_B, E_B)$
Сеть агентов	$\mathrm{G} = (V, E)$
Множество состояний агентов	$Q^A = \{q_{ij}^A\}$
Множество функций перехода	$\Delta = \{\delta_i\}$
Множество стратегий поведения	$Strat = \{strat_i\}$
Функция выбора функции перехода	γ
Функция выбора стратегии	ξ

Множество индикаторов $Ind = \{ind_i\}$

Множество входных параметров

НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ

✓ **Характеристики агента**

- управляющий статус
- состояние
- защищенность
- принадлежность к группе
- индивидуальные действия
- коммуникативные действия
- уязвимости
- эксплойты

✓ **Характеристики базовой сети**

- отображение на граф агентов
- функциональные типы узлов и соединений

✓ **Характеристики соединения**

- протокол
- уязвимости
- защищенность

✓ **Управляющие элементы**

- стратегии
- функции выбора стратегии
- функции перехода
- функции выбора функции перехода

Множество индикаторов модели

Системы защиты

Kaspersky Security Network
ESET Live GRID
Panda Cloud Antivirus ...

Nugache, Zindos,
SpamThru,
PhatBot, Storm ...

Бот-сети

Противостояние = защита + нейтрализация противника

- Управляемость
- Отказоустойчивость
- Константность функционирования
- Стойкость

- Мощность воздействия
- Имитомощность
- Эффективная мощность воздействия

Масштабируемость

Управляемость

Доля агентов, связанных с УЦ путем длины $\leq t$, задаваемая через вероятность наличия пути длины $\leq t$ от произвольно взятого узла до УЦ, и зависящая от значений параметров P конкретной системы

$$CT_P(t) = \begin{cases} \dfrac{\sum_{i=1}^{N} path\_num\_t_i}{\sum_{i=1}^{N} path\_num_i}, \text{если } \sum_{i=1}^{N} path\_num_i > 0, \\ 0, \text{если } \sum_{i=1}^{N} path\_num_i = 0, \end{cases}$$

В общем случае вычисляется с использованием методов построения альтернативных графов (с применением эвристик)

Отказоустойчивость

Отказоустойчивость R_{max} – определяет степень критического деструктивного воздействия на систему, при котором доля агентов, связанных с УЦ путем длины $\leq t$, где t фиксировано, $CR_P(R)$, стремится к нулю

$$\lim_{R \to R_{max}} CR_P(R) = 0,\ 0 \leq R \leq R_{max}$$

Аналог критической вероятности p_c в теории перколяций

Классический случайный граф	Регулярный случайный граф	Звезда
$p_c \sim \frac{\ln n}{n}, n > 0$	$p_c = \frac{1}{d-1}, d \geq 3$	1) $p_c = \frac{1}{n}, n > 0$ 2) $p_c = 1$

Константность функционирования и стойкость

Константность функционирования определяется уровнем необходимого изменения объема затрачиваемых в единицу времени ресурсов *V(R)* при изменении величины деструктивного воздействия *R*

$$Op_P = \frac{\partial V}{\partial R}$$

Стойкость – вероятность того, что агент входит в состав системы противника и имеет возможность управления рассматриваемой системой

$$T = \frac{\sum_i Sec(Type[e_i])}{|Type|} \cdot \frac{1}{SpyRate} \cdot MASVuln(Actuality[Vuln], VulnRate[Vuln])$$

Мощность воздействия

Мощность воздействия – оценивает мощность и применимость множества «эксплойтов» рассматриваемой системы

$$F = f(Expl, \Omega_{expl}, CP)$$

Эксплойтность: $Expl = \sum_i Actuality[exploit_i]$

Распределение эксплойтов по узлам графа агентов

Вычислительная мощность агентов

Имитомощность

Имитомощность – вероятность внедрения в сеть противника агента, находящегося под управлением рассматриваемой системы.

Факторы, способствующие увеличению имитомощности

- Наличие замаскированных агентов рассматриваемой системы в сети противника
- Низкая защищенность узлов и связей враждебной сети
- Наличие уязвимостей в атакуемой системе и наличие соответствующих эксплойтов у атакующей системы

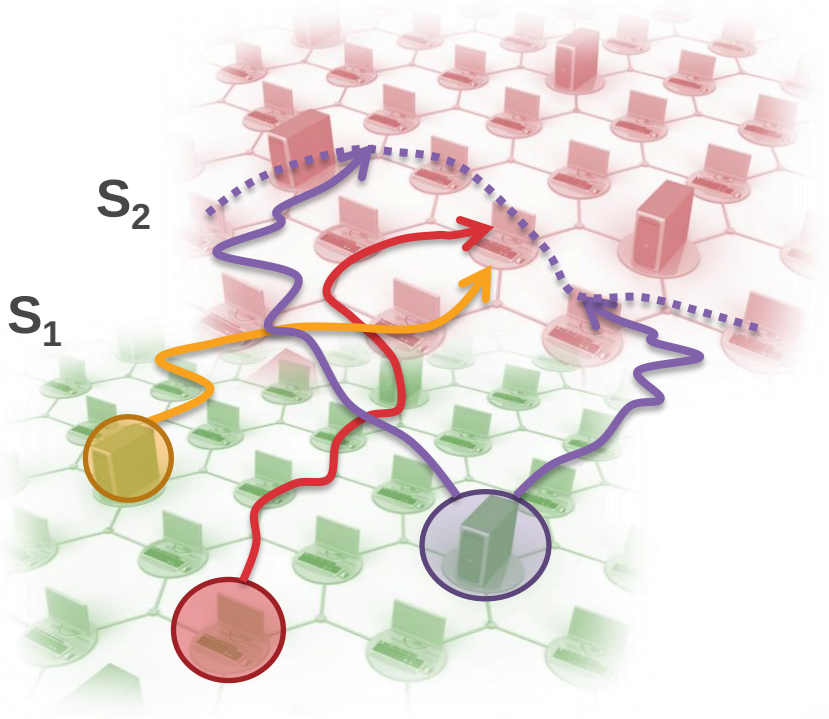
Эффективная мощность воздействия

Эффективная мощность воздействия – мощность воздействия рассматриваемой системы в противостоянии с одним из предполагаемых противников.

$$D = f(Strat_{at}) \cdot \sum_{j \in Type[V^*_{vuln}]} \frac{Sign[v_i] \cdot |V^{*j}_{vuln}|}{|V^*|}$$

$Sign[v_i]$ – значимость агента

V^*_{vuln} – множество враждебных агентов, находящихся в потенциальной зоне распространения эксплойтов рассматриваемой системы



Вычисление индикаторов модели

Формальное описание системы

Аналитическая оценка

Реальная система / Имитационная модель

Статистические испытания

Применение модели

Оптимизация показателей распределенных систем защиты и обеспечение устойчивости их функционирования

Оценка эффективности противостояния распределенных систем защиты определенным классам угроз

Оценка рисков, связанных с воздействием определенного класса угроз на рассматриваемую систему

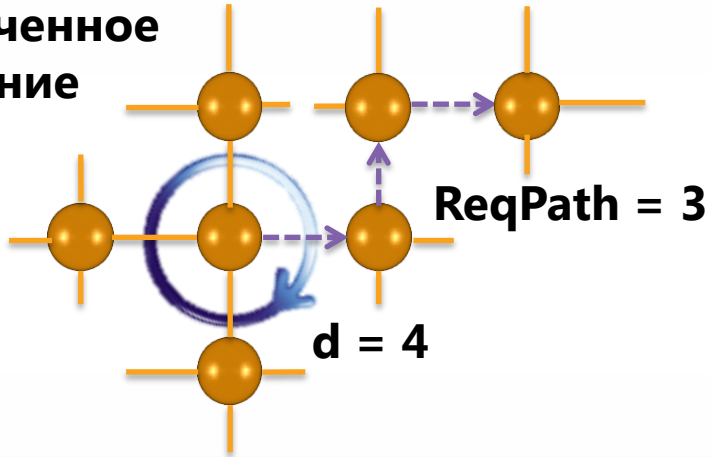
Пример: решение задачи оптимизации

НЕОБИТ — Новые безопасные информационные технологии

Задача оптимизации

$$\begin{cases} CT_P(t) \to max \\ R_{max} \to max \\ Op_P(R) \to min \end{cases} \Rightarrow \begin{cases} CT_P(t) \to max \\ R_{max} \to max \\ Op_P(R) < Op_{accept} \end{cases}$$

Полученное решение



Фиксированные параметры

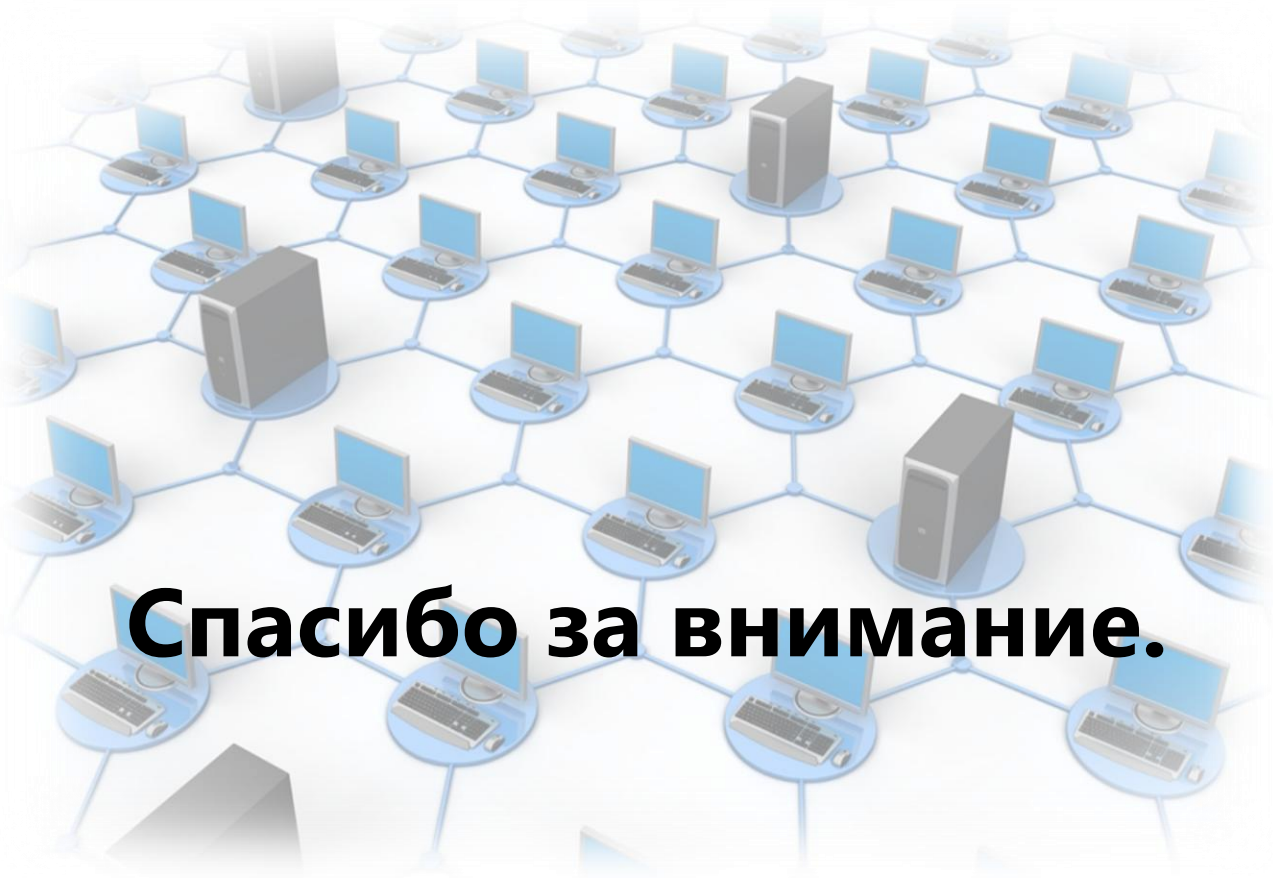
n = 1000
CC = 10
$T_q\_num = 15$
T_q = 60 с
T_{check} = 90 с
t = 35 мс

Выводы

Предложенная модель оперирует обобщенными понятиями и в силу этого может применяться при рассмотрении взаимодействия распределенных систем различного типа

Значения индикаторов могут быть отображены в вероятности победы каждого из участников на основании статистических данных

Модель применима для решения таких задач как оптимизация параметров рассматриваемых систем, оценка эффективности противостояния распределенных систем защиты определенным классам угроз, оценка рисков



Спасибо за внимание.