

# Критерий Поппера и исследования в области сетевой безопасности

---



Денис Гамаюнов

лаборатория вычислительных комплексов ВМК  
МГУ имени М. В. Ломоносова



# Критерий Поппера

---

- 1935 год, Карл Поппер
  - Критерий научности эмпирической теории - определяет научность, исходя из принципа фальсифицируемости:
    - «Научная теория не может быть принципиально непроверяемой, всегда должна существовать методологическая возможность экспериментального опровержения этой теории»
-



# Исследования в области сетевой безопасности

---

## □ Публикуют:

- Гипотезы, идеи
- Алгоритмы\*
- Методики испытаний
- Результаты экспериментов

## □ Не публикуют\*:

- Реализации алгоритмов
- Тестовые данные

---

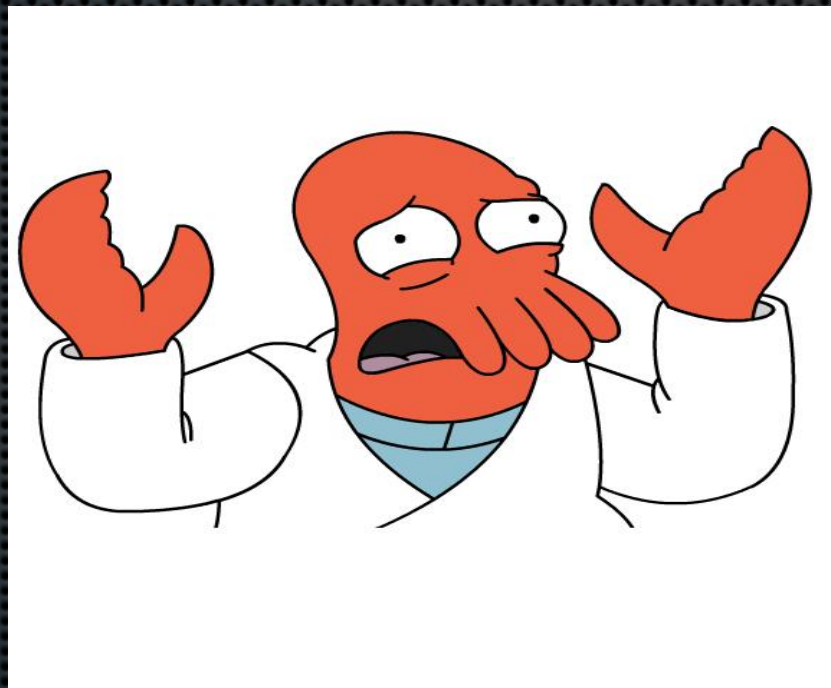
\* в любом правиле есть исключения



# Готовность к сотрудничеству между научными группами

---

Thanks for writing.  
We won't be releasing the implementation.  
Sorry that I can't be more helpful





# Открытые коллекции данных

---

- ❑ KDD Cup'99 — запись трафика атак, предобработанные векторы признаков для алгоритмов машинного обучения
- ❑ VX Heavens — коллекция вирусов  
**БЛИЗКА К ПОЛНОМУ УСТАРЕВАНИЮ**



# Закрытые коллекции данных

---

- **Anubis** — кластеризация malware, формирование коллекции через открытый сервис анализа исполнимых файлов
  - **CWSandbox** — аналогично Anubis
  - **Wepawet** — коллекция вредоносного JavaScript и заражённых веб-сайтов, формирование коллекции через открытый сервис проверки сайтов, а также с помощью краулера
-



# Цитируемость коллекций данных\*

Название коллекции	Число упоминаний в научных статьях	Год публикации	Нормированное по годам число упоминаний
KDD Cup 99 dataset	2,850	1999	237
Vx heavens	9,530	1999	794
Anubis	115	2007	28
CWSandbox	243	2006	48
Wepawet	25	2008	8

\* По данным Google Scholar



# Выводы

---

- Публикация тестовых данных обязательна для научной работы
  - Сообществу нужны открытые данные
  - Проблема поддержания актуальности открытых коллекций данных разрешима — возможно децентрализованное решение
-



# Спасибо за внимание

---

- Контактная информация:
    - Денис Гамаюнов: [gamajun@lvk.cs.msu.su](mailto:gamajun@lvk.cs.msu.su)
    - Тел. +7 (495) 939 46 71
    - Москва, 119899 Ленинские горы вл. 1/52, факультет ВМК МГУ имени М. В. Ломоносова, к. 764
-