КООРДИНАЦИОННЫЙ ЦЕНТР
НАЦИОНАЛЬНОГО ДОМЕНА
СЕТИ ИНТЕРНЕТ

Сотрудничество в борьбе с интернет «зловредами»

ИНФОФОРУМ 2013

Андрей Колесников
Координационный центр национального домена сети Интернет

«Зловреды»

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

- **Доставка malware;**
- **Phishing;**
- **СПАМ;**
- **Управление ботнетами;**
- **Fast Flux;**
- **SEO spam**

Указанные категории привязаны к именам доменов

Участники НТС

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

Яндекс
Найдётся всё

KASPERSKY lab

@mail.ru

GROUP IB

Технический Центр Интернет

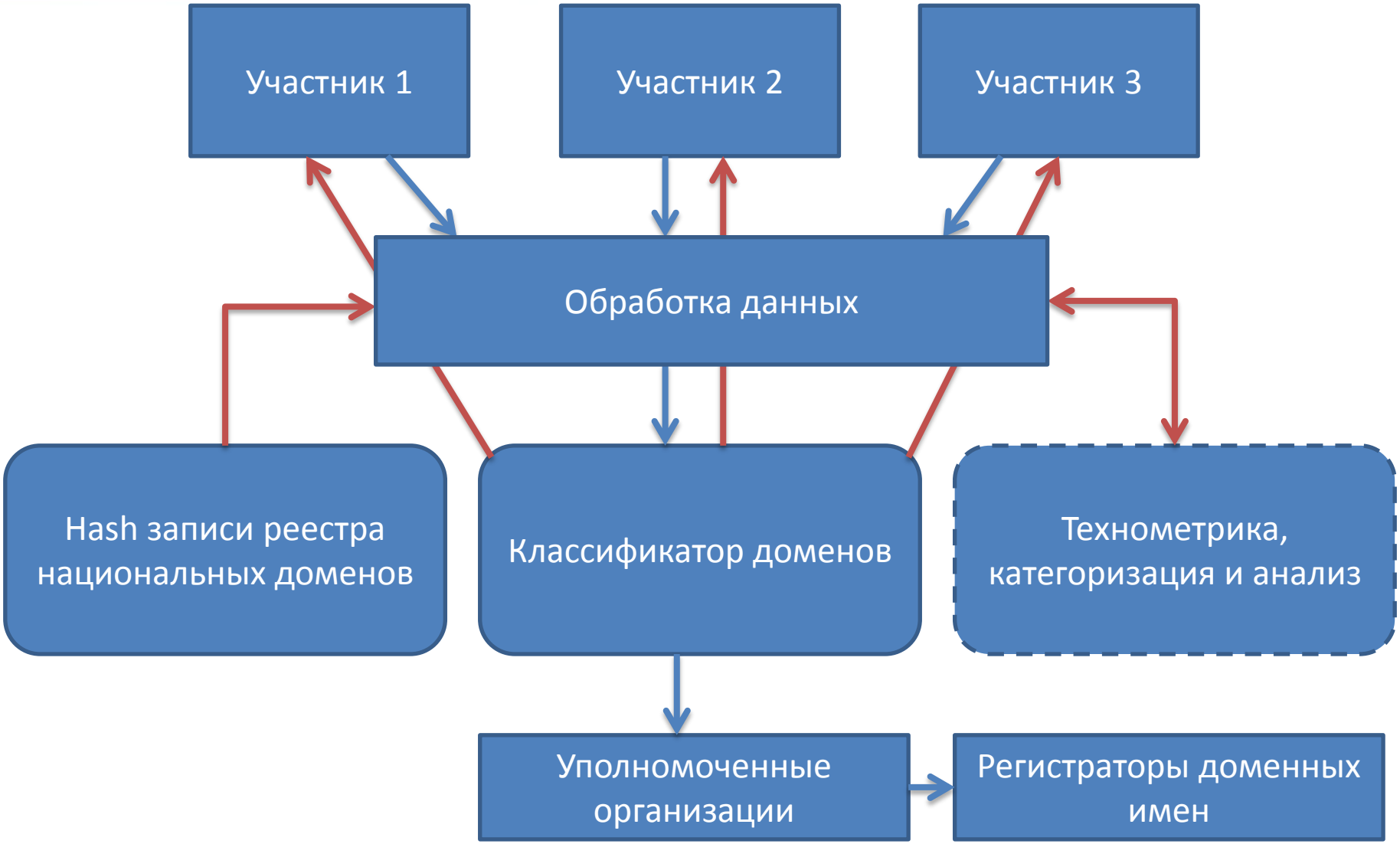
RU-CERT

Сотрудничество

научно-техническое, некоммерческое, добровольное

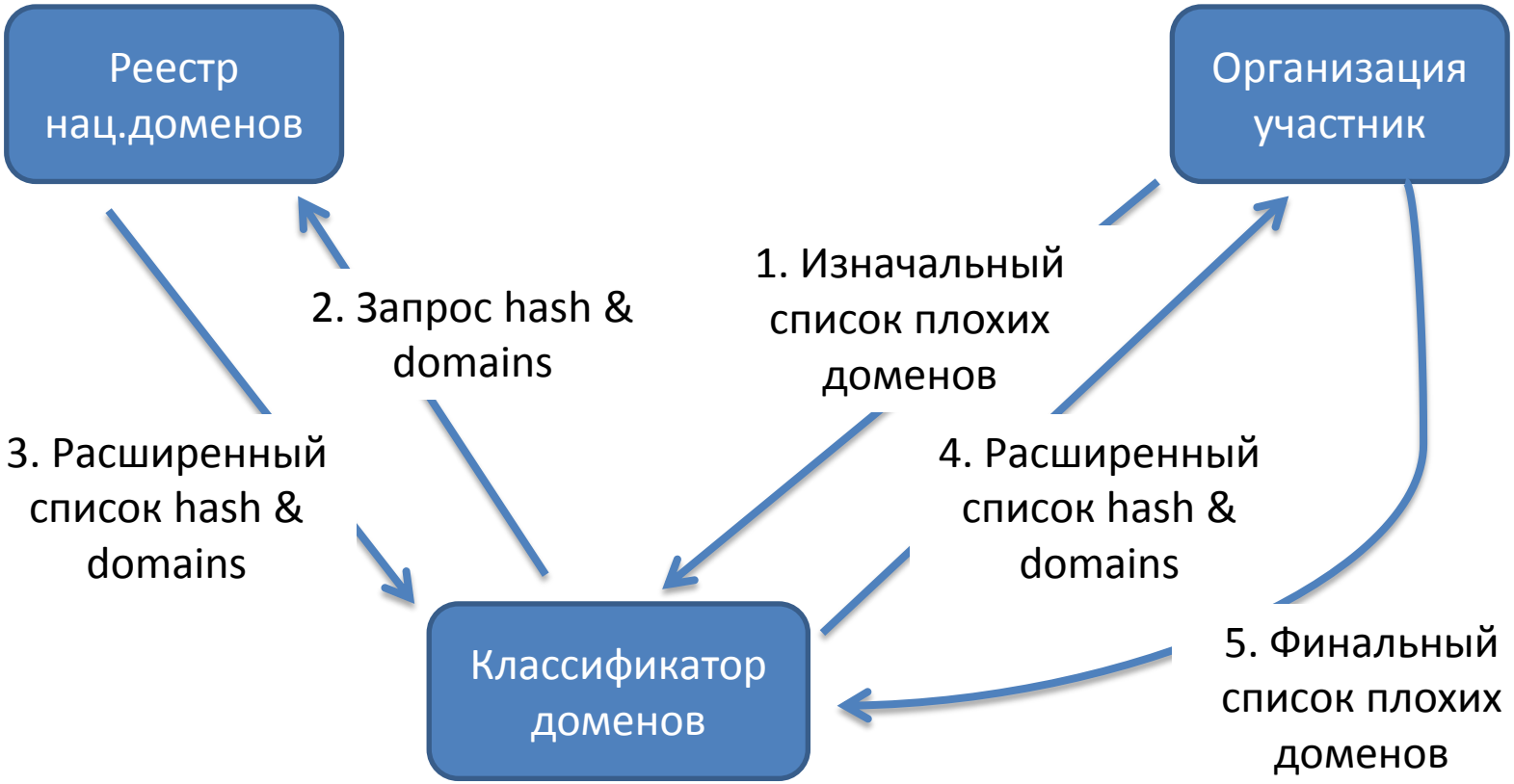
Взаимоотношения участников НТС

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ



Процесс обогащения данных

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ



Экспресс статистика (лето 2012)

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

- **Первые результаты, лето 2012 г.**
  - **Количество «плохих» доменов примерно 60.000 в зоне .RU**
  - **1000 доменов могут быть названы «точно плохими»**
  - **Примерно 6800 записей администраторов доменов из общего числа 1300000 связаны с «плохими» доменами**

Число проверенных доменов	**294810**
Лаборатория Касперского	289732
RU-CERT	7808
Из них «плохие»:	**243198**
Malware	126853
Phishing	8982
Spam	37105
Сразу две категории	2359
Уже удаленных	68931

Первые выводы и дальнейшие шаги

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

- «Плохие» домены часто регистрируют «пачкой»;
- «Плохие» домены замечены в деятельности SEO:
  - Вполне легальная работа «днем»;
  - Управление ботнетами, malware итд «ночью»
- Дальнейшие шаги:
  - Советом Координационного центра одобрен бюджет на развитие проекта;
  - Совершенствование регламентирующих документов регистрации российских доменных имен;
  - Совместный сайт статистики и аналитики «зловредов» доменных имен России;
  - Развитие сотрудничества между участниками проекта: технометрика, категоризация и анализ «вредоносных» паттернов по расширенному набору признаков

Заключение

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

- **Уникальный и не имеющий аналогов в мире опыт научно-технического сотрудничества;**
- **Не государственная инициатива на принципах саморегулирования;**
- **Высокий потенциал дальнейшего развития сотрудничества в интересах всех участников**

Проект не коммерческий и преследует цель:
Уменьшение количества «зловредов» в Рунете и мире

Спасибо

Андрей Колесников

andrei@cctld.ru