Ежегодная международная научно-практическая конференция
«РусКрипто'2019»

Автономность российского сегмента сети интернет, как система технических требований

А.М. Сухов[1], Е.С. Сагатов[1], В.А. Карпунин[2], О.В. Царькова[2]

[1] Самарский университет
[2] Код безопасности

САМАРСКИЙ УНИВЕРСИТЕТ

КОД БЕЗОПАСНОСТИ

Докладчик: Сухов Андрей Михайлович,
профессор кафедры суперкомпьютеров и общей информатики Самарского университета
amskh@ya.ru

Предпосылки для автономной работы российского сегмента сети Интернет

2014 год – санкции, под ударом:

- Банки и финансы
- Инфраструктура
- Ключевые отрасли экономики
- Высокие технологии

Режим санкций будет усиливаться. Вполне вероятны перебои в работе российского сегмента глобальной сети!

Критические Интернет-технологии

- DNS (Domain Name System «система доменных имён»)
- Маршрутизация
- Сетевые атаки
- Системы мониторинга

Уязвимости DNS

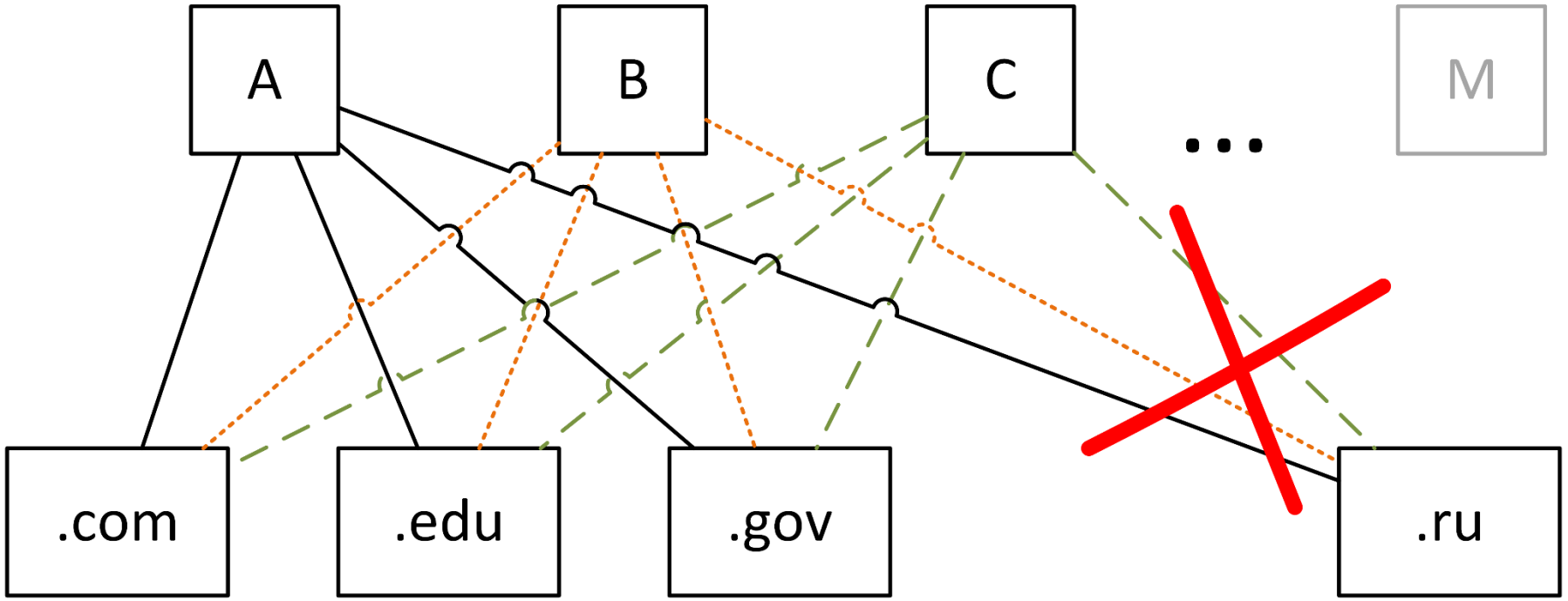
- В России нет собственных корневых серверов. Все корневые сервера расположены в странах НАТО.
- В России лишь копии корневых серверов.
- Национальные домены могут быть легко отключены от общей системы.
- Отключение делегирования обратной зоны.

Кто управляет корневыми серверами

Имя хоста	Управляющая организация
a.root-servers.net	VeriSign, Inc.
b.root-servers.net	University of Southern California (ISI)
c.root-servers.net	Cogent Communications
d.root-servers.net	University of Maryland
e.root-servers.net	NASA (Ames Research Center)
f.root-servers.net	Internet Systems Consortium, Inc.
g.root-servers.net	US Department of Defense (NIC)
h.root-servers.net	US Army (Research Lab)
i.root-servers.net	Netnod
j.root-servers.net	VeriSign, Inc.
k.root-servers.net	RIPE NCC
l.root-servers.net	ICANN
m.root-servers.net	WIDE Project

Иерархия DNS

Корневые сервера (a.root-servers.net, b.root-servers.net...)



Домены первого уровня

Альтернативные корневые DNS

- Chaos Computer Club DNS — (анонимность)
  - Совместима с основной иерархией ICANN, но расположена в Германии и США. Против цензуры.
- OpenNIC — (анонимность + домены)
  - .bit; .bbs; .chan; .dyn; .free; .fur; .geek; .gopher; .glue; .indy; .neo; .null; .oss; .oz; .parody; .pirate
- Open Root Server Confederation — (в зависимости от ICANN)
- Open Root Server Network — (за независимость от ICANN)
  - Совместима с основной иерархией ICANN, но расположена в Европе.
  - Создана, чтобы обеспечить независимость Интернета от ICANN.
  - Была запущена снова с июня 2013 (публикация файлов Сноудена).
  - ORSN не ориентирована на получение прибыли и не расширена с помощью дополнительных доменов верхнего уровня.

Россия может установить собственные корневые серверы и заменить существующие или добавить новые.

* Альтернативные корневые серверы DNS / Википедия. – URL: https://ru.wikipedia.org/w/index.php?title=Альтернативные_корневые_серверы_DNS

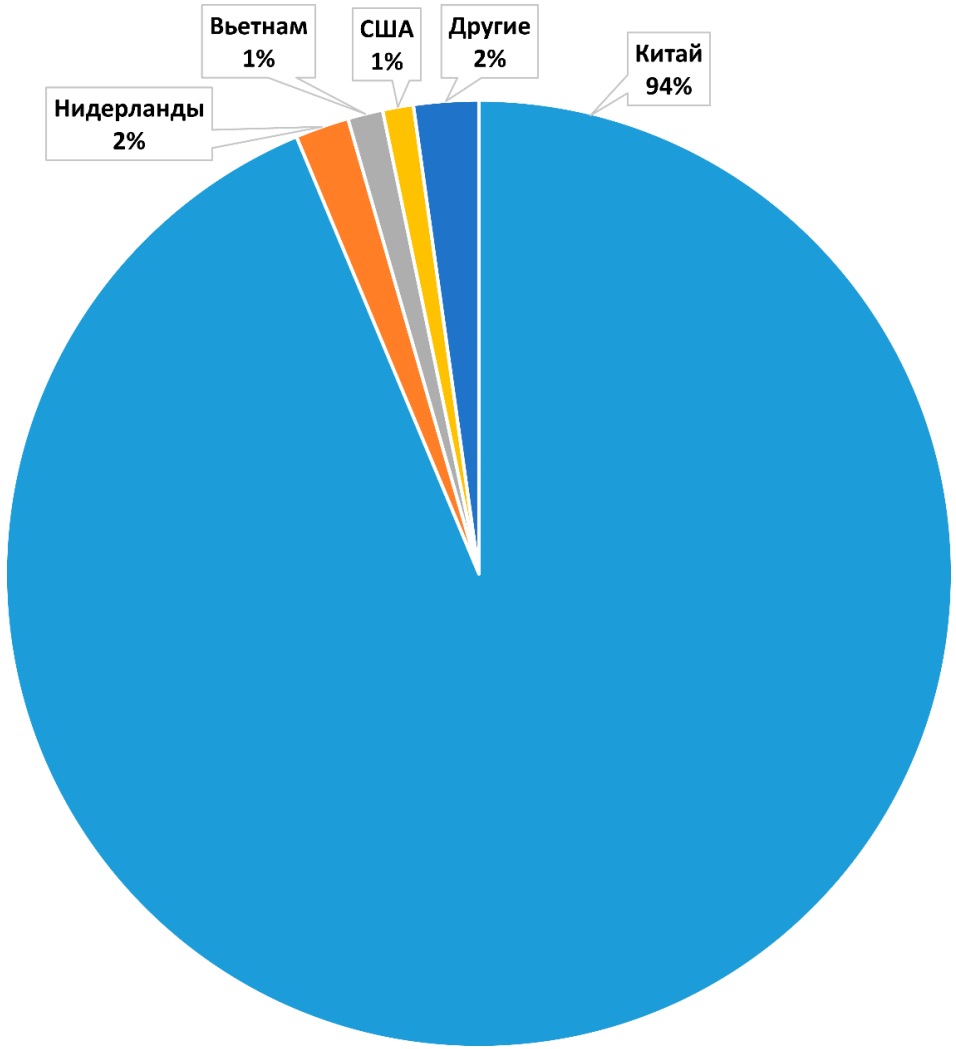
Реализация альтернативных DNS

- Новая версия ПО bind9
- Есть европейский опыт функционирования альтернативных DNS (работа возобновлена после откровений Сноудена)
- Замена на всех российских DNS серверах софта на новую версию с российскими корневыми серверами

Независимый сбор базы DNS

- В настоящее время в России доступен только кэш с нескольких реплик корневых серверов
- Необходим альтернативный способ сбора информации о доменах.
- Китай собирает данные о доменных именах с помощью роботов.
- 90% несанкционированных запросов к DNS – запросы из Китая (по данным с наших серверов ловушек).

Данные с наших серверов-ловушек



Нарушение маршрутизации

- AS – автономная система – минимальная независимая единица для маршрутизации.
- Междоменная маршрутизация – глобальная маршрутизация в сети Интернет по протоколу BGP (Border Gateway Protocol, протокол граничного шлюза)
- LIR - Local Internet registry, Локальный интернет-регистратор.
- 1’930 LIR в России из 17’394 LIR в Европе.
- 5’119 AS в России из 36’376 в Европе.
- Число внешних каналов из России – несколько сотен (наша оценка)

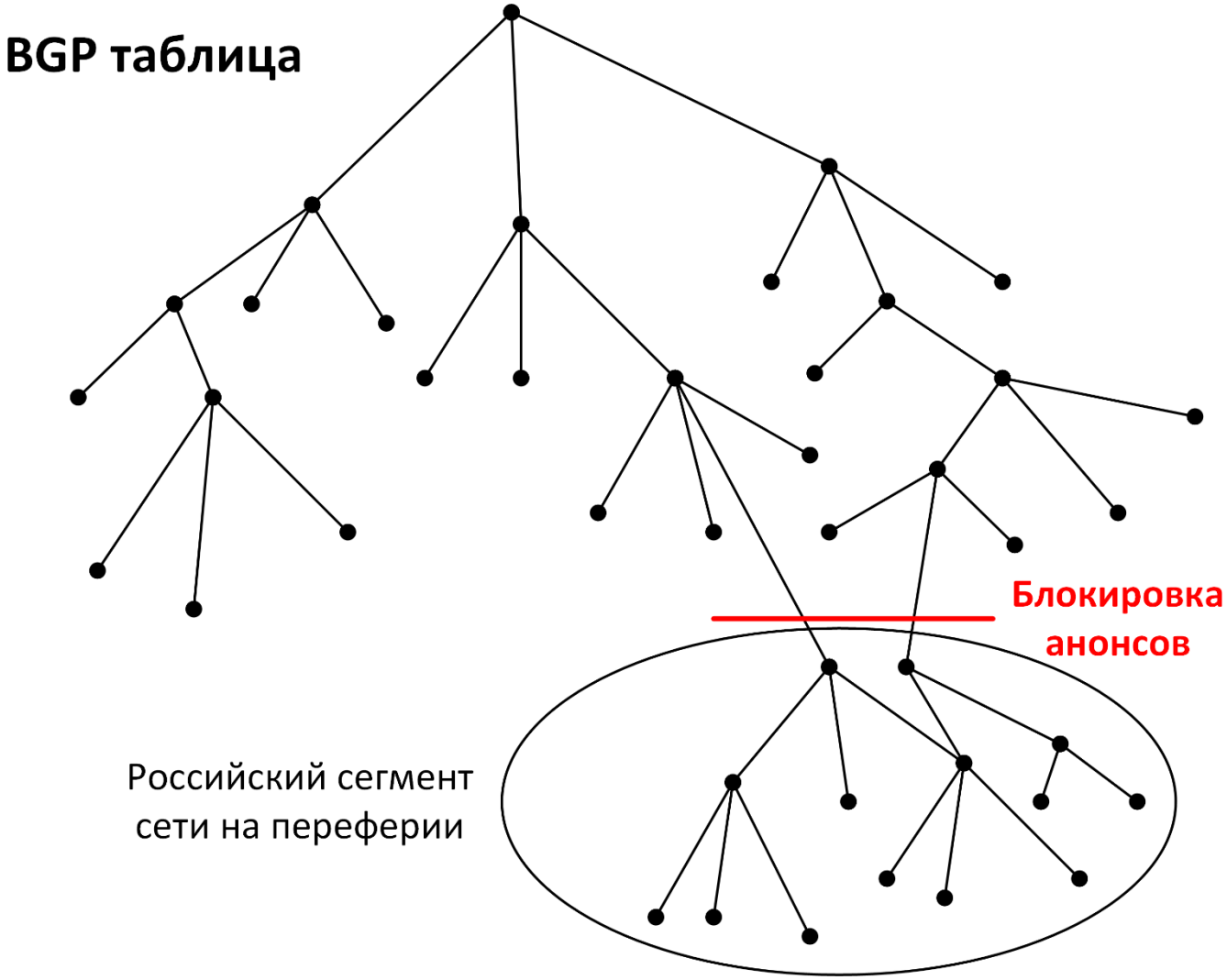
Недостатки маршрутизации в Рунете

- Более 20% внутрироссийского трафика обслуживается за границей.
- Невозможность управления трафиком и ограничения ряда типов трафика (Telegram)
- Для нарушения маршрутизации достаточно заблокировать BGP анонс от российских AS

Достоинства

- Невозможность отключить большую часть внешних каналов
- Невозможность проведения результативной DDoS атаки на переполнение всех каналов

Блокировка анонсов BGP таблиц



Каким пойти путём?

- Сокращение внешних каналов
- Введение ряда пунктов контроля за трафиком, через которые проходит весь трафик.
- Недостатки:
- Резкое уменьшение устойчивости сети (мало каналов – легче отключить или атаковать)
- Мало серверов – легче вывести из строя.
- Монополизм приведёт к резкому росту стоимости услуг для конечных потребителей.

Возможные решения

- Для замыкания трафика внутри России – технология локальных точек обмена трафиком (IX), свободный обмен, пиринг.
- В идеале все автономные системы должны быть подключены к единой распределённой точке обмена трафиком.
- Число IX в России – 39,
- Общее число подключений 1683 на конец 2017 года,
- Охват 39,2% из всех российских автономных систем подключены к точкам IX
- 2 AS, даже подключенные к одной IX, часто не имеют пиринга. В результате доля каналов с внешним (зарубежным) трафиком среди AS, подключенных к MSK-IX около 20% в 2018 году.

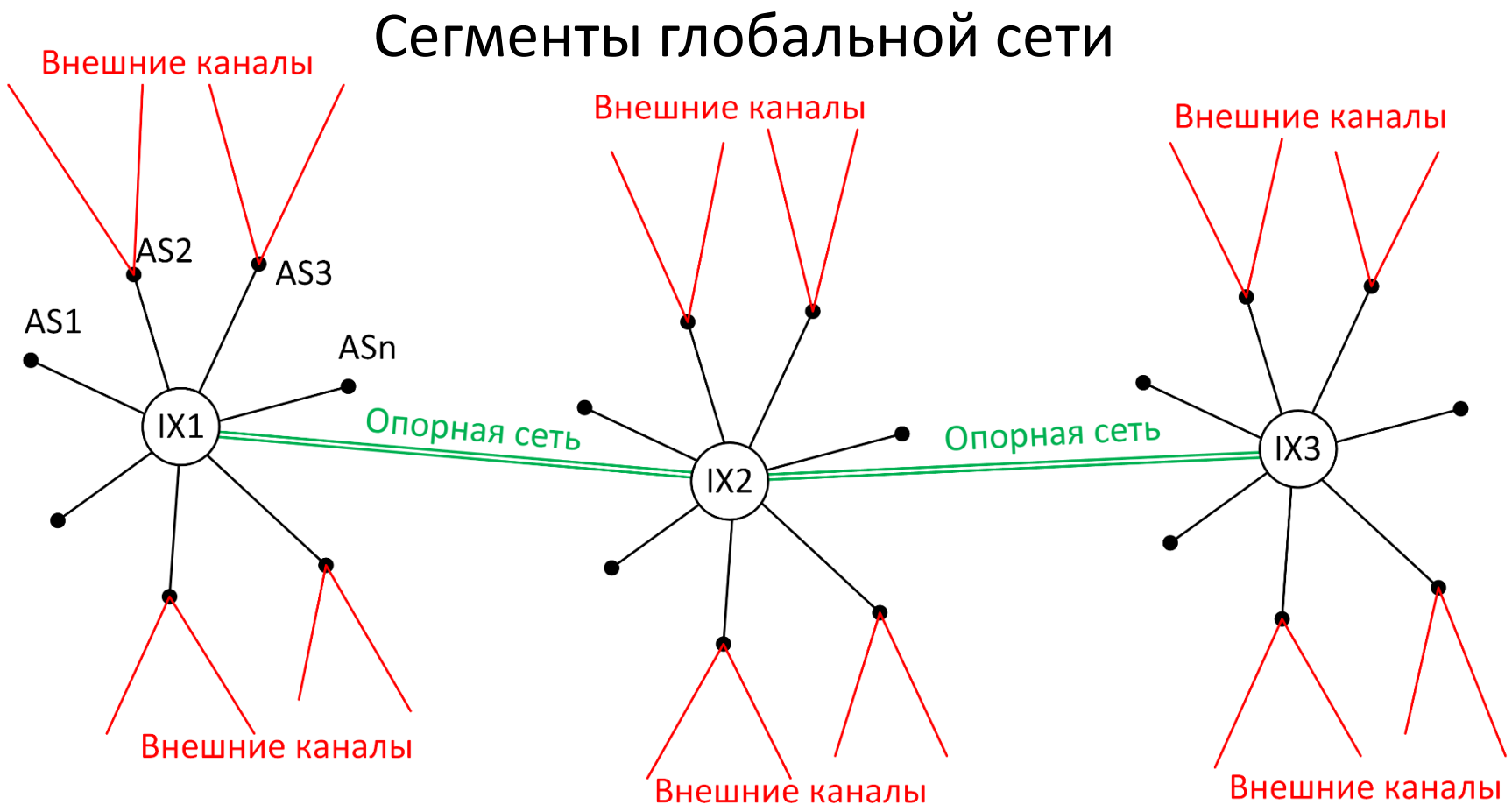
Почему IX не выполняют своей роли?

- Очень дорогое подключение
- Плата за ежемесячную аренду порта
- Плата за трафик через IX
- Плата за внешний канал дешевле

Решение по маршрутизации

- Все российские IX должны быть подключены к единой распределённой точке IX
- Между всеми российскими IX должен быть пиринг
- Региональные IX должны быть соединены единой опорной сетью
- Цена подключения к IX должна быть очень невысокой (в разы дешевле, чем внешний трафик по BGP)

Создание опорной сети между IX



Управление трафиком

- Для эффективности управления необходимо сильно упростить схему управления и отвязать её от топологии маршрутизации
- Технология, когда управление отдельно от маршрутизации существует – это технология SDN (software-defined networking, программно-определяемая сеть, программно-конфигурируемая сеть)
- Требования к этой сети должны разрабатываться отдельно и коррелировать с топологией IX.
- Необходимы исследования в области SDN безопасности.

Мониторинг качества сетевых соединений

- RIPE Atlas – измерительное устройство от европейского центра управления Интернет.
- 450 активных узлов в России.

Они знают о Рунете всё:

- Доступность DNS
- Какие узлы подключены к IX
- Внутренние маршруты, на которых трафик уходит за границу
- и т.д.

Российской системы мониторинга нет!

САМАРСКИЙ УНИВЕРСИТЕТ

КОД БЕЗОПАСНОСТИ

Спасибо за внимание!

Контакты: Сухов Андрей Михайлович

amskh@ya.ru

Работа выполняется в рамках государственного задания Министерства образования и науки РФ (проект 2.974.2017/4.6) и при поддержке гранта РФФИ № 16-07-00218а.