Перспективы нормативной работы вокруг технических аспектов блокировок

Филипп Кулин (Эшер II)

v 0.1.1

Сплошной клубок проблем

- Сопутствующий ущерб
- Волатильность нормативов и практик
- Трудность диагностики
- Непредсказуемость
- Невозможность рассчитать риски
- Неприемлемое время обратной связи
- Безысходность

Группы риска

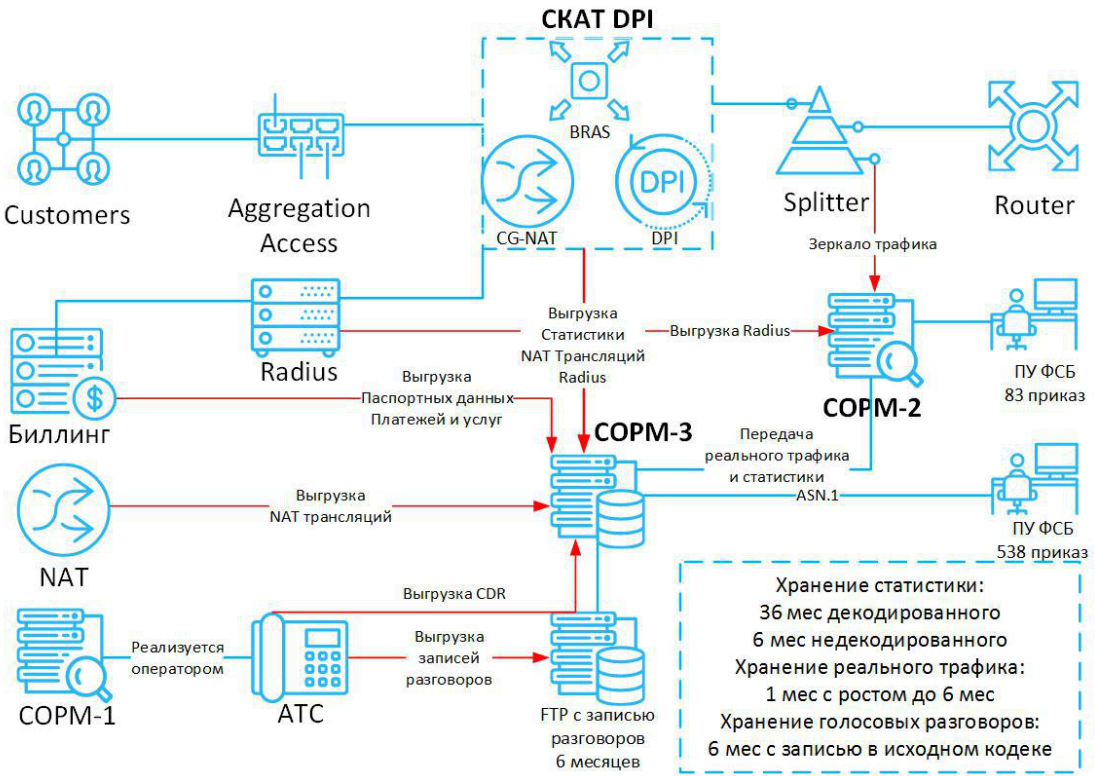
- Владельцы сайтов и сервисов
- Пользователи сервисов
- Хостеры и провайдеры

Проблемы фильтрации

Добросовестные участники интернета:

- Нет умысла
- Не нарушает законодательство

Будет весело, говорили они...



Начнем, пожалуй

Как это работает

- Решение ФОИВ или суда о запрете
- Внесение в реестр Роскомнадзором
- Решение Роскомнадзора о блокировке, внесение в «выгрузку»
- Получение провайдером «выгрузки»
- Осуществление провайдером ограничения
- Проверка провайдеров

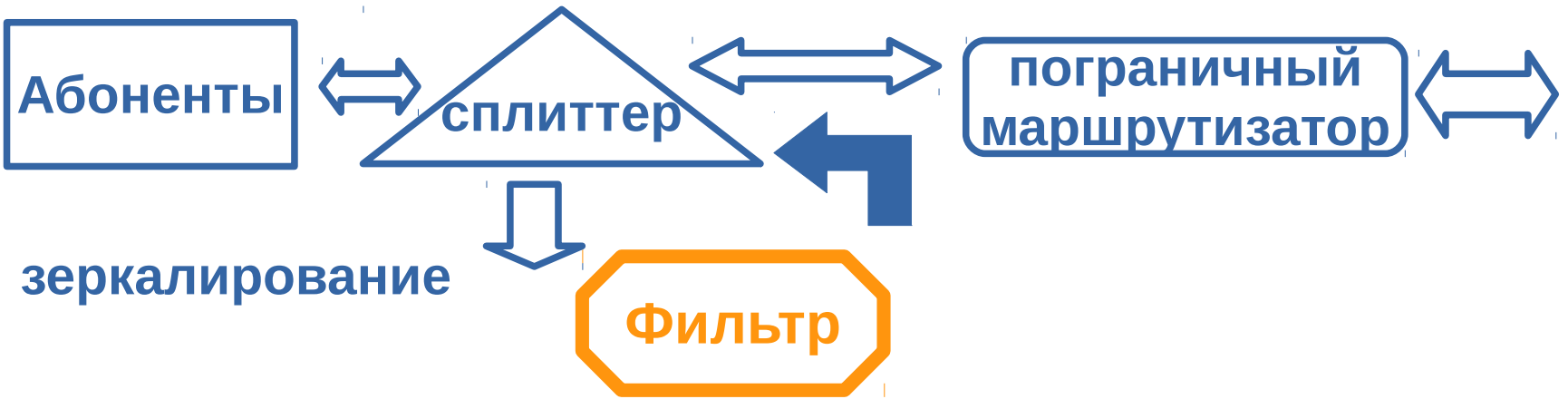
Как выглядит схема фильтрации

Чем фильтруют

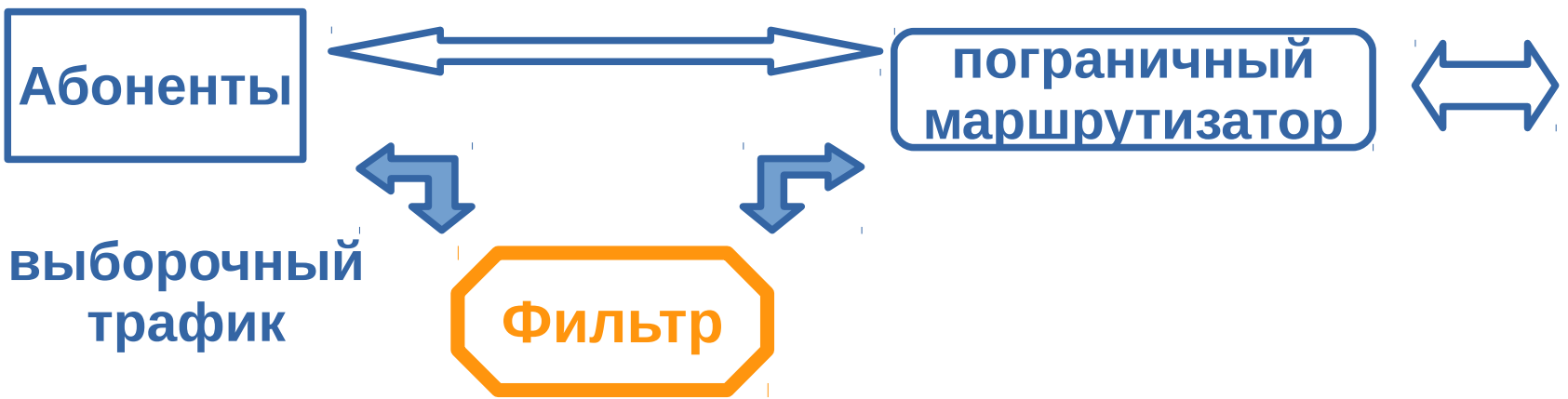
- Фильтрованный трафик вышестоящего провайдера
- Специальные комплексные коммерческие решения
- Свободно распространяемые решения с открытым исходным кодом
- Свой «колхоз»

Фильтр в разрыв

Работа на опережение



Выборочная маршрутизация



Распространённая практика

Выборочная маршрутизация
+ Наборы IP-адресов для фильтрации агрегируются в большую сторону
+ Комбинация с DNS-фильтром

Разберем поэтапно

Получение «выгрузки»

- Традиционная полная «выгрузка»
- *Так называемые «дельты»*

- *Нет регламента обслуживания сервиса «выгрузок»*
- *Нет регламента аварийной ситуации с каналами*
- *«Дельты» можно подключить только к ограниченному списку коммерческих решений*

Время применения «выгрузки»

- Сутки (и блокировка, и разблокировка)
  - например, ночные обновления коммутаторов
- Незамедлительно
  - в течение часа по устной договорённости

- *Правовая неопределенность «незамедлительно», срок — это юридический факт, событие*

Статистика «выгрузки»

записей:	175 077
тип «по URL»:	63 604 (36.3%)
тип «по домену»:	92 704 (53.0%)
тип «по маске»:	13 897 (7.9%)
тип «по IP-адресу»:	4 872 (2.8%)
уникальных URL:	84 901
IP-адресов «по IP»:	296 107
блоков IP-адресов:	39
охвачено IP «по IP»:	1 027 330

размер в архиве:	11 MB
размер «выгрузки»:	70 MB
в день:	~ 150

Токсичность «выгрузки»

- Избыточность
- Актуальность IP-адресов

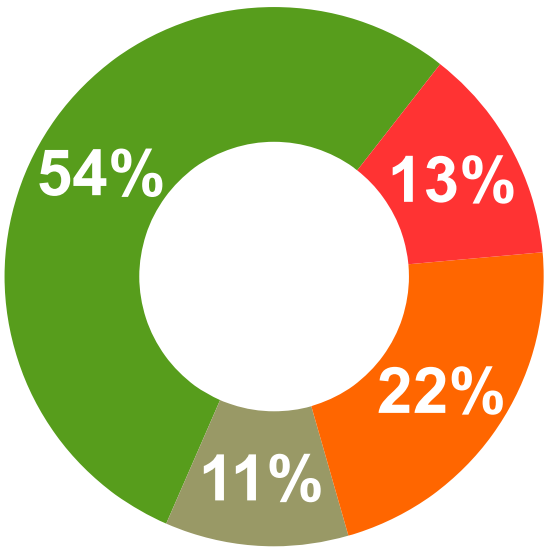
Отличная история! (приказ РКН №21 от 11.02.2019)

- URL с фрагментами (#) и сессиями (~900)
- Неправильные URL и домены (5)

Актуальность «выгрузки»

IP-адреса в «выгрузке»
и в реальности:

- Совпадают
- Частично
- Различаются
- Отсутствуют



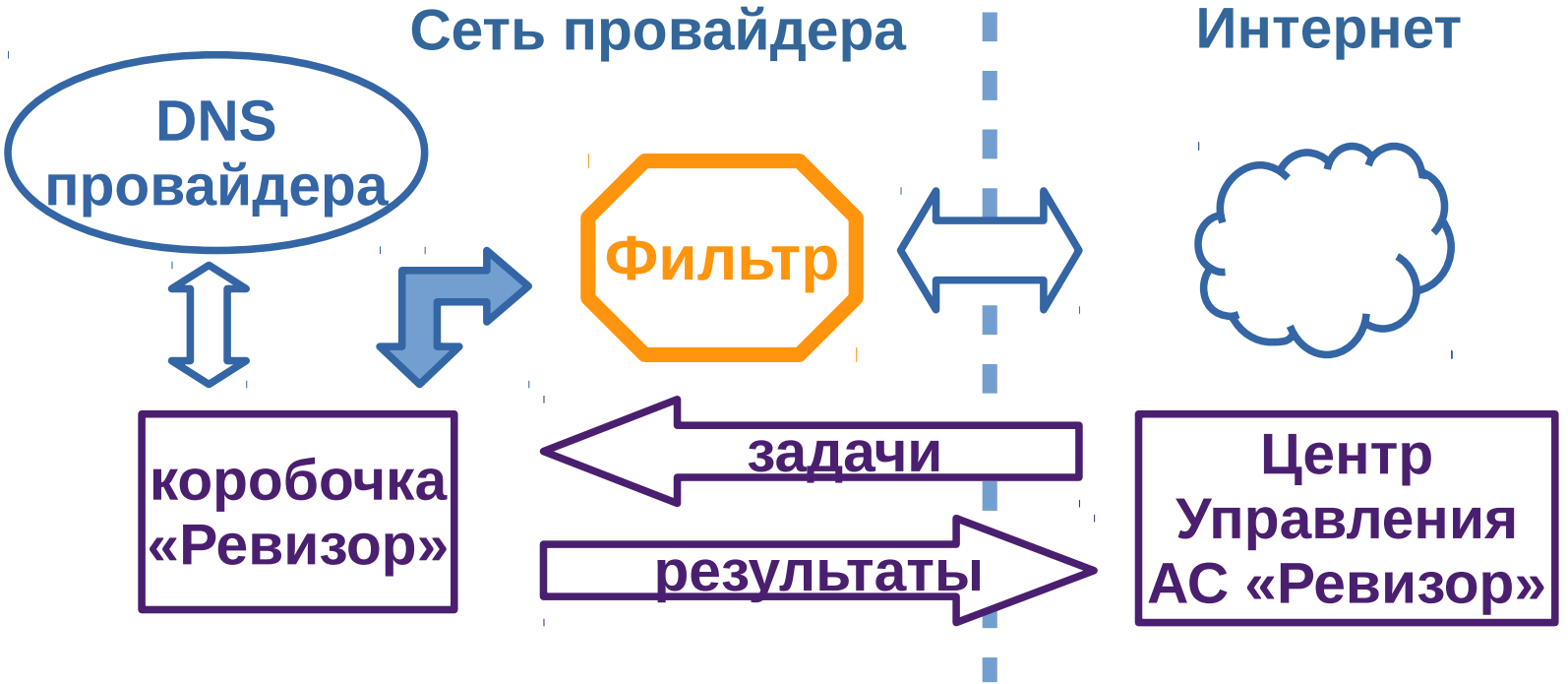
А каким нормативом вы руководствуетесь, принимая меры по ограничению доступа?

Проверка блокировок

Вся история реализации блокировок в России – это история проверок

До реестра запрещенных сайтов существовал список экстремистских материалов Минюста и прокурорские проверки блокировок по этому списку

Схема АС «Ревизор»



Проблемы проверки

- СПЕКТР-2017, доклад Вэклича А.А. (ФГУП ГРЧЦ)
- Это фильтр провайдера или ресурса?
- Показатель блокировки для HTTPS, домена, IP-адреса
- Показатель блокировки для других протоколов
- Как проверить домен по маске?

Методика работы АС «Ревизор»

Что делать без методики

- Экзистенциальный опыт
- Эмпирический путь
- Чатик в Телеграм

Метрология АС «Ревизор»

Метрология АС «Ревизор»

- *№ 102-ФЗ от 26 июня 2008 статья 1 часть 3 пункт 17*
- *№ 102-ФЗ от 26 июня 2008 статья 5 часть 5*
- *№ 126-ФЗ от 07 июля 2003 статья 12 пункт 2*

Тут мы пропустим проблемы фильтрации DNS, всякие VPN, QUIC и ESNI

Резолвинг домена

- В нормативе нет, но «вы же понимаете»
- Возможность выборочной фильтрации (не на всю полосу)

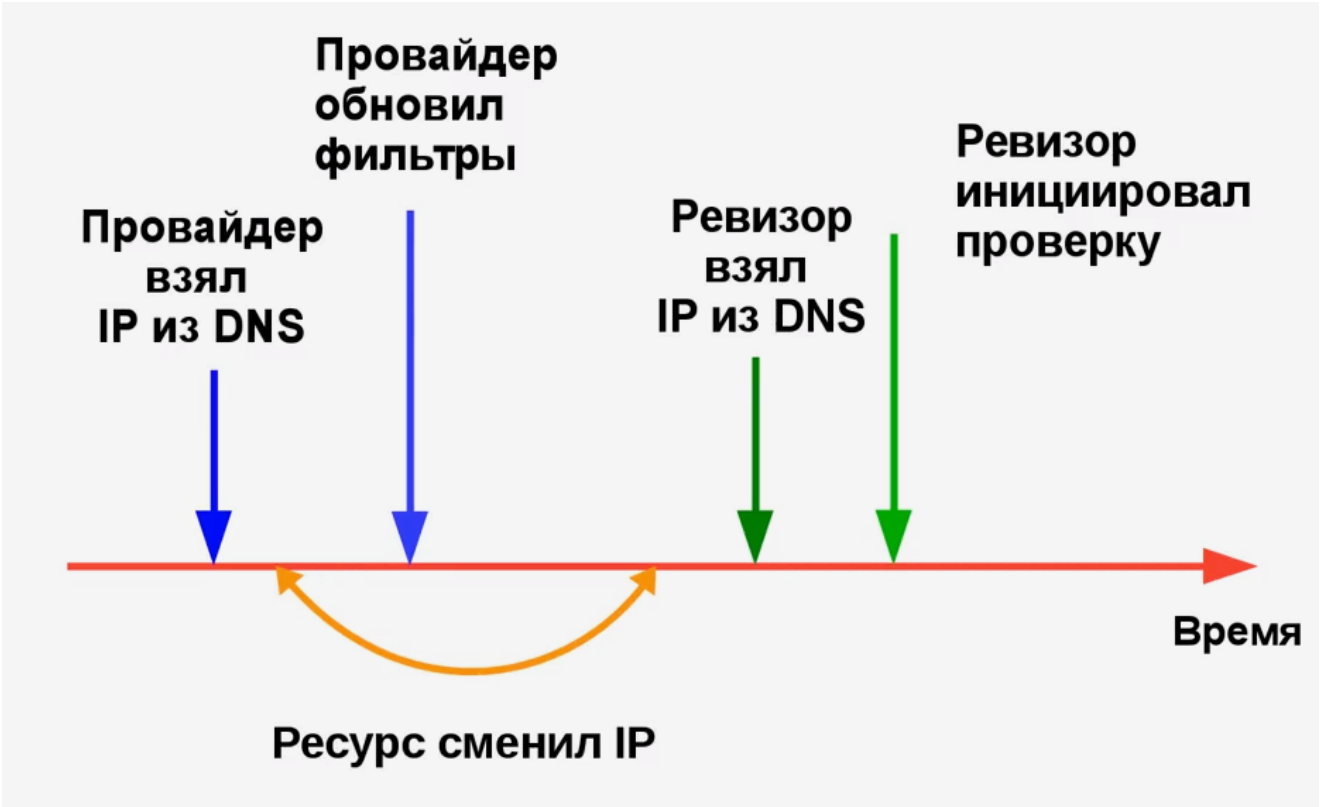
ВАЖНО

Законодательство РФ ничего не говорит об **эффективности** блокировок, только процедуры

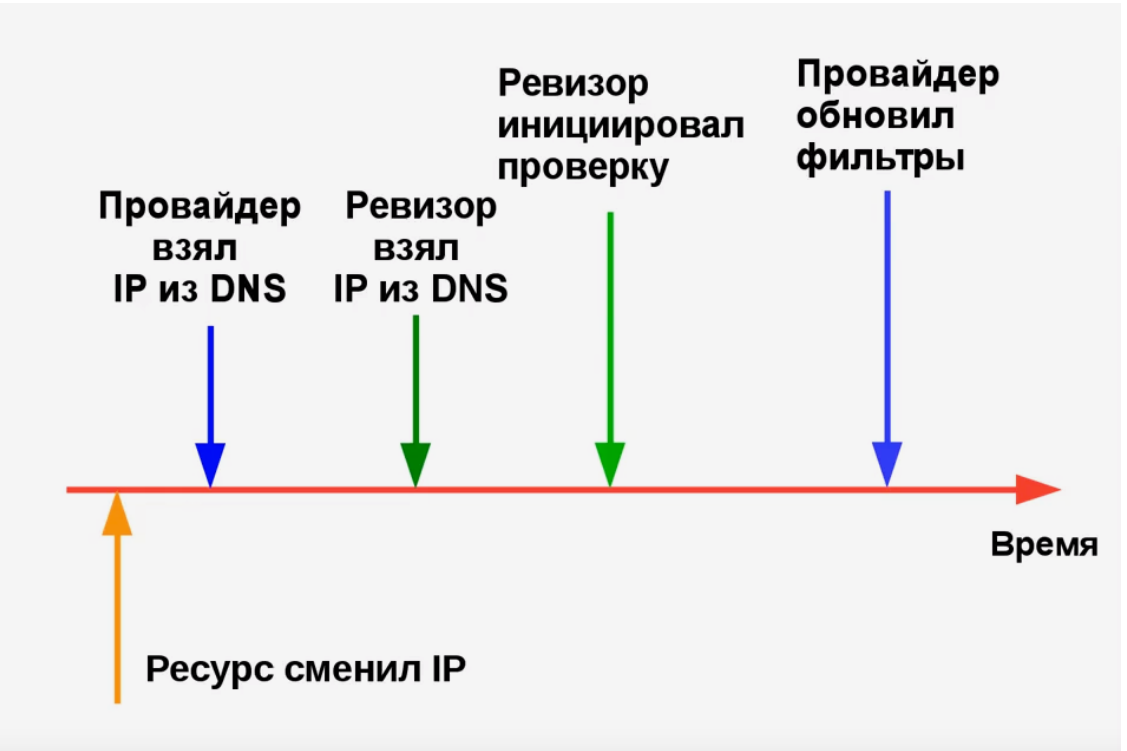
Этот непростой резолвинг

- Балансинг
- Геотаргетинг
- Миграция сервисов, в том числе и умышленная

Проблема фаз при проверке



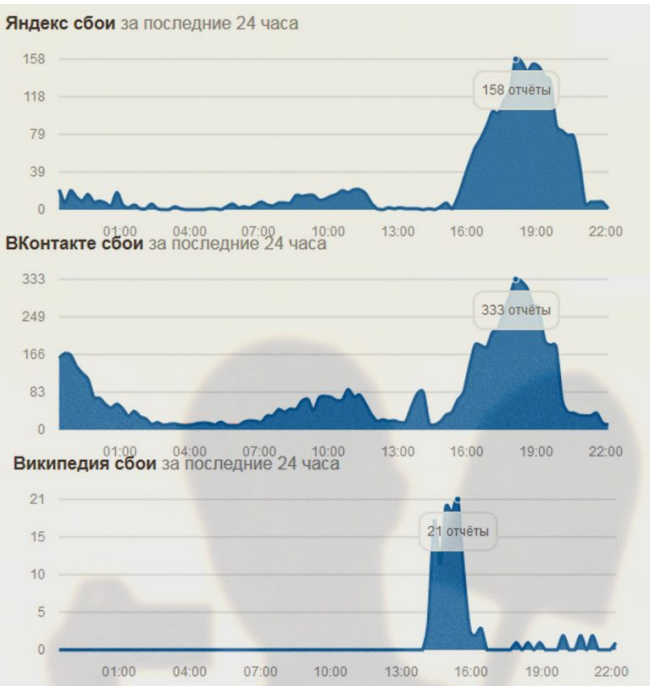
Проблема фаз при проверке

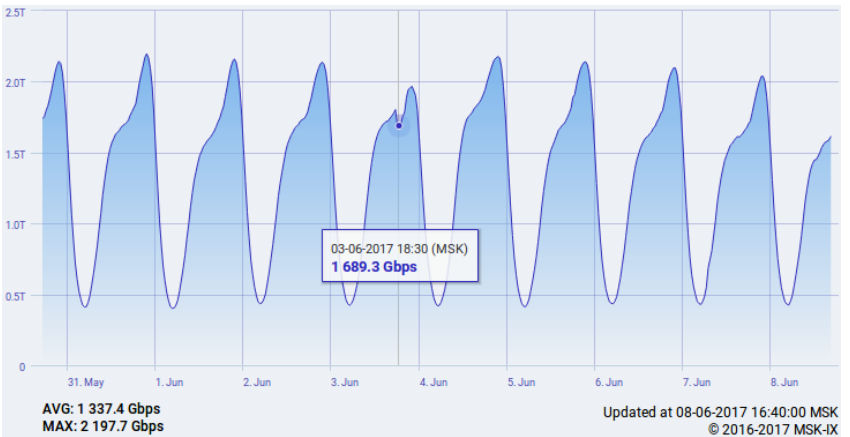


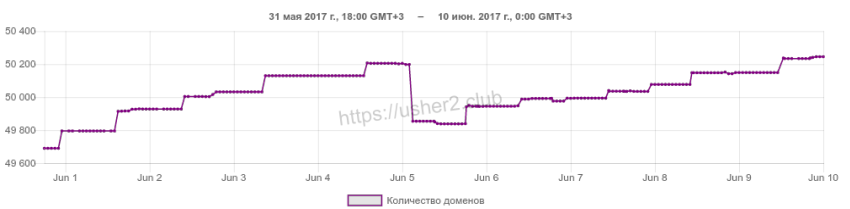
«Протухшие» домены

- У домена закончился срок регистрации, но он остаётся в выгрузке
- Новый владелец домена получает контроль над частью «выгрузки»
- Сейчас «протухших» доменов в «выгрузке» около 2100, но мы не знаем, сколько уже купленных

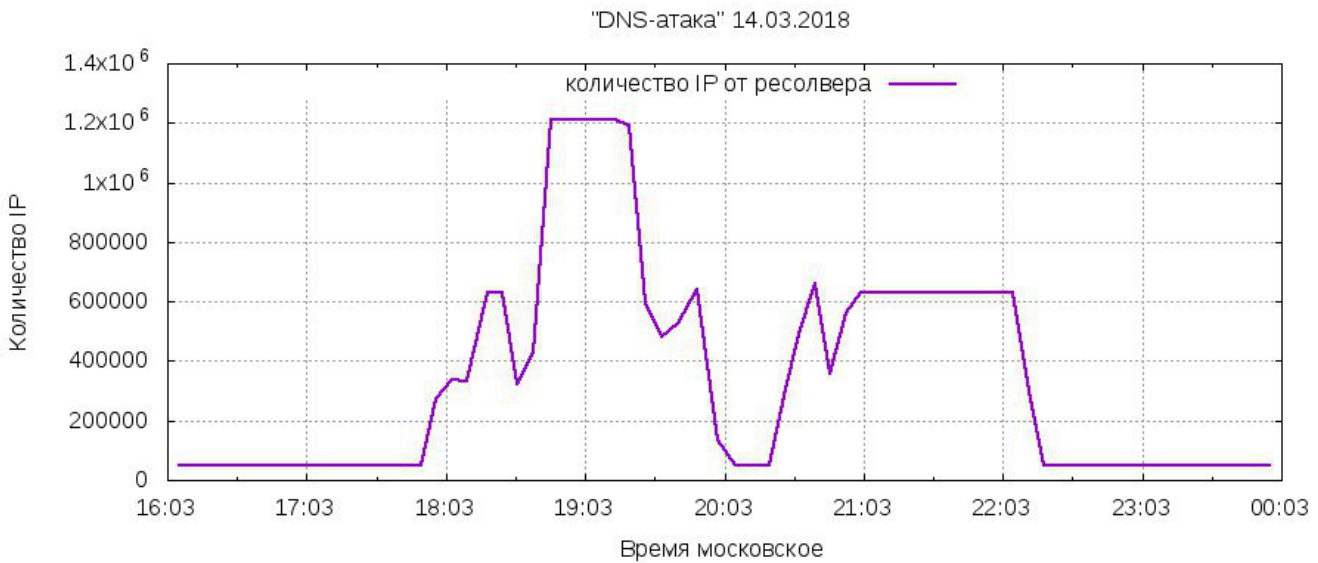
«DNS-атака» летом 2017



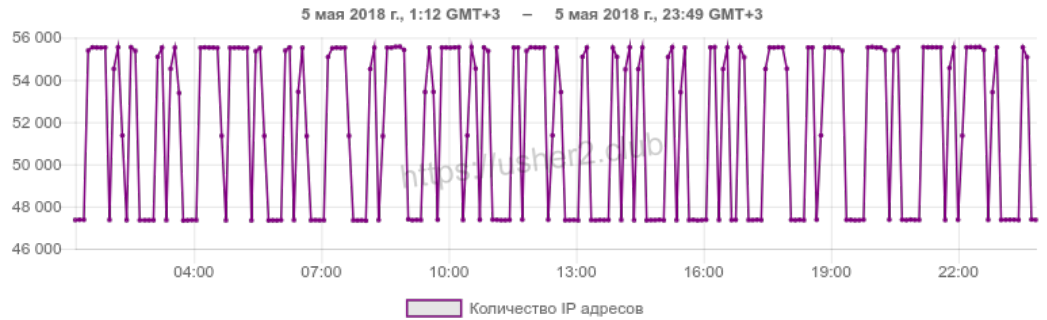


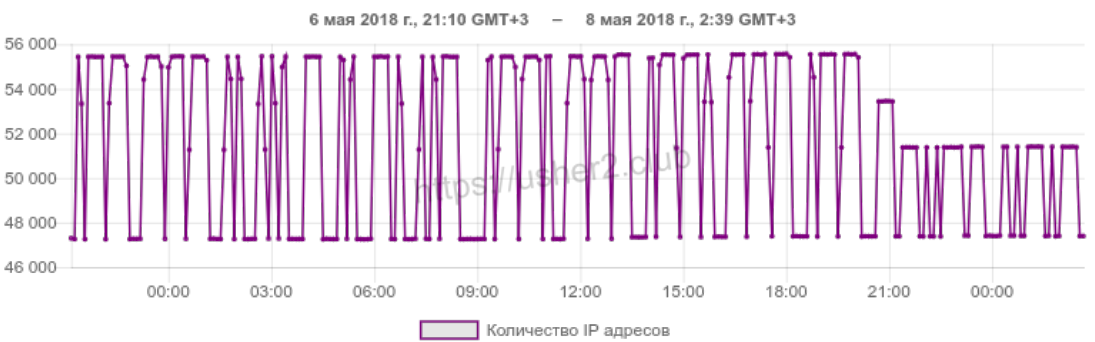


Авария ТТК 14 марта 2018



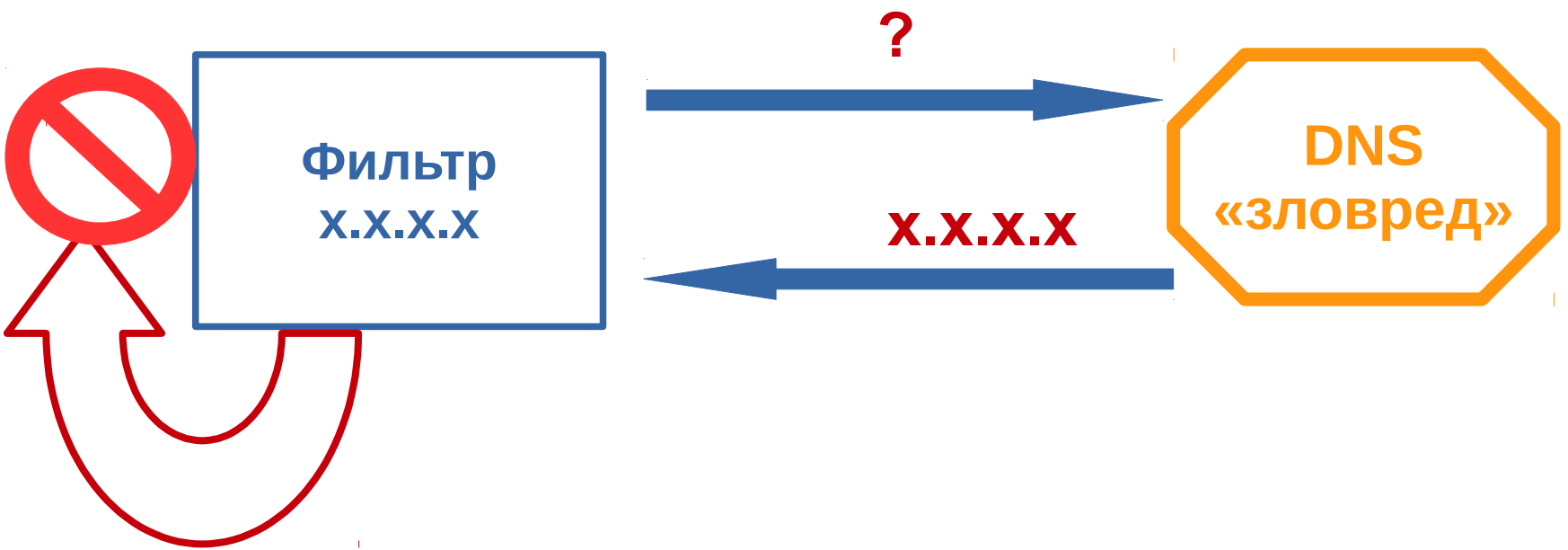
Послание на графике в мае 2018



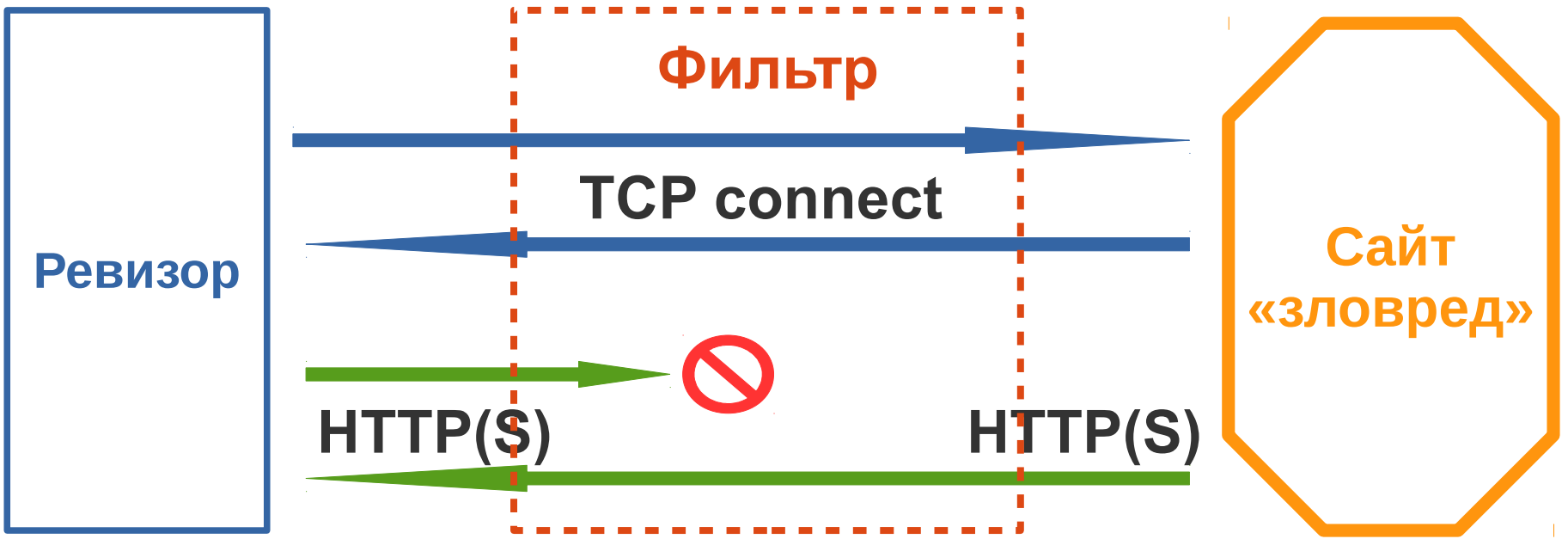


Новые вектора «DNS-атак»

Ответ адресом вопрошающего



HTTP(S) ответ без запроса



Регламент техобслуживания

- Не работает сервис «выгрузок»
- Авария на каналах связи
- Поломка фильтров
- Профилактика фильтров

Это абсолютно разумные понятные требования

Что делать-то?

Кто за что отвечает

Надо чётко понимать, что кто делает

- Министерство цифрового развития
- Центральный Аппарат Роскомнадзора
- Территориальные Управления Роскомнадзора
- ГРЧЦ

Разъяснения с помощью писаний

- И Минцифра, и Роскомнадзор имеют раздел обращения через сайт
- Желательно звонить на следующий день
- №59-ФЗ от 02 мая 2006 г. «Об обращении граждан»
- №79-ФЗ от 27 июля 2004 г. «О госслужбе»
- Контролирует — Генеральная Прокуратура

  у них, кстати, самая хорошая система регистрации обращений

Регуляторика

- Есть хорошие каналы в Telegram:
  - новости Правительства @govdigest
  - новости Минцифры и Роскомнадзора @ru_comnews
  - регулирование Телекома @ru_comreg
  - другие тематические паблики
- Официальный портал проектов нормативов: regulation.gov.ru

Не надо стесняться участвовать в обсуждения нормативов

Судебные разбирательства

- Система работает не по формальным правилам
- Пытайтесь ловить на нарушении процедур
- Дожимайте. Пытайтесь. Настойчивость может стать залогом успеха

Перспективы

- Все попытки последних лет что-то сделать — крайне жалкие, или так выглядели
- Закон «об изоляции Рунета» формально перечёркивает этот диспут
- Закон «об изоляции Рунета» метит в лидеры «долгостроя» и срыва всех сроков
- Закон «об изоляции Рунета» требует много нормативной работы, в которую можно и нужно вмешаться

Только бизнес

И он такой мне: «Я всего-лишь ростовщик — бизнесмен, так сказать. Я дело делаю — деньги зарабатываю. Сражаться — это не ко мне!»

Вопросы

Если возникли вопросы, предложения или требуется помощь, да и в любом случае — пишите мне:

phil@diphost.ru

Общественное достояние

Это бесплатный документ, переданный в общественное достояние.

Любой человек может свободно копировать, изменять, публиковать, цитировать, использовать, продавать или распространять этот документ на любых носителях целиком или по частям для любых коммерческих или некоммерческих целей во всех смыслах.