Черная дыра критической инфраструктуры

Еще в 2016-ом году, в ноябре, Минкомсвязи выдали в публичное обсуждение законопроект "Об обеспечении устойчивости российского сегмента сети "Интернет"". С тех пор законопроект так и не стал законом, что довольно редкий случай, надо отметить. Обычно законы регулирования интернета, направленные на "контроль через запрещение", принимаются законотворцами с радостью. И иногда переходящей в овации.



Но не в этом случае.

Законопроекту на ресурсе "обсуждения" (кавычки - потому что никогда никаких обсуждений на этом ресурсе не было) regulation.gov.ru было выдано резко отрицательное заключение. Причем, заключение было дано аж через целый год. Дата окончания публичных консультаций 3 ноября 2017 г.

Подробности и точные формулировки проекта доступны вот здесь: http://regulation.gov.ru/projects#npa=71277. А собственно объявление о работе от Минкомсвязи - вот здесь: http://minsvyaz.ru/ru/events/36040/

По сути, МКС хотели создать некую государственную (гипотетическую) информационную систему, которая управляла бы "критической инфраструктурой сети "Интернет"". Те, кто на самом деле понимает, как функционирует интернет, были, конечно, поражены отточенными формулировками про "особенности регулирования ключевых элементов" и описанием "обязанностей операторов связи в части технических требований к организации линий передачи данных". Было задумано, что законопроект затронет вопрос организации точек обмена трафиком и пропуска трафика на территории России, и определит порядок его организации.

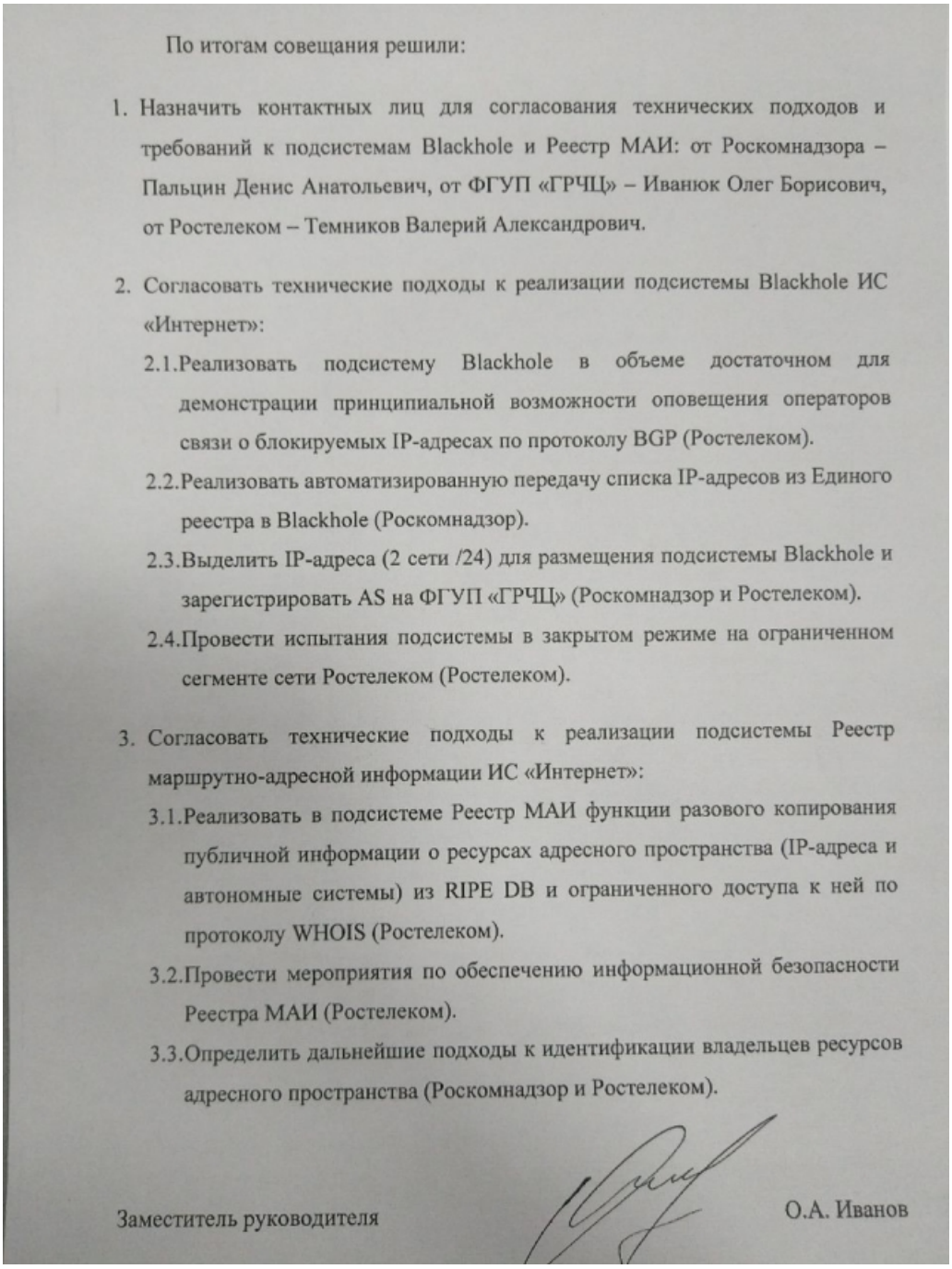
Выдержка из заключения Минэкономразвития, где имеется целых шесть пунктов возражения, но выделим только один самый первый пункт:

1.1. В проекте акта содержатся требования к операторам связи по подключению используемых ими сетей связи к точкам обмена трафиком на территории Российской Федерации, которые включены в реестр в составе Государственной информационной системы обеспечения целостности, устойчивости функционирования и безопасности информационно-коммуникационной сети Интернет в Российской Федерации (далее – ГИС "Интернет"). Указанное требование полностью реформирует действующую децентрализованную модель пропуска трафика в сторону жестко централизованной, что может привести к невозможности выбора коротких оптимальных способов маршрутизации трафика и дополнительной существенной финансовой нагрузке на участников рынка из-за необходимости пропуска трафика по удлиненному маршруту.

Кроме того, одинаковая топология сетей передачи данных у многих операторов связи и аналогичные присоединения для обмена трафиком в точках обмена трафиком, зафиксированных в ГИС "Интернет", всех операторов связи содержат риск неустойчивости функционирования сетей связи именно из-за узлов единой централизации, которые представляются более предпочтительной целью для хакерских атак и других способов воздействия, и ставят под вопрос обеспечение общей кибербезопасности.

В общем, законопроект был отклонен.

Но на днях мне в руки попал кусок вот такого документа:



По итогам совещания решили:

1. Назначить контактных лиц для согласования технических подходов и требований к подсистемам Blackhole и Реестр МАИ: от Роскомнадзора – Пальцин Денис Анатольевич, от ФГУП «ГРЧЦ» – Иванюк Олег Борисович, от Ростелеком – Темников Валерий Александрович.

2. Согласовать технические подходы к реализации подсистемы Blackhole ИС «Интернет»:
   2.1. Реализовать подсистему Blackhole в объеме достаточном для демонстрации принципиальной возможности оповещения операторов связи о блокируемых IP-адресах по протоколу BGP (Ростелеком).
   2.2. Реализовать автоматизированную передачу списка IP-адресов из Единого реестра в Blackhole (Роскомнадзор).
   2.3. Выделить IP-адреса (2 сети /24) для размещения подсистемы Blackhole и зарегистрировать AS на ФГУП «ГРЧЦ» (Роскомнадзор и Ростелеком).
   2.4. Провести испытания подсистемы в закрытом режиме на ограниченном сегменте сети Ростелеком (Ростелеком).

3. Согласовать технические подходы к реализации подсистемы Реестр маршрутно-адресной информации ИС «Интернет»:
   3.1. Реализовать в подсистеме Реестр МАИ функции разового копирования публичной информации о ресурсах адресного пространства (IP-адреса и автономные системы) из RIPE DB и ограниченного доступа к ней по протоколу WHOIS (Ростелеком).
   3.2. Провести мероприятия по обеспечению информационной безопасности Реестра МАИ (Ростелеком).
   3.3. Определить дальнейшие подходы к идентификации владельцев ресурсов адресного пространства (Роскомнадзор и Ростелеком).

Заместитель руководителя О.А. Иванов

Документ подписан заместителем руководителя Роскомнадзора Олегом Ивановым. За достоверность и реальность документа поручиться я лично не могу - он был получен из "анонимных источников в телеграме". Но выглядит очень похоже на настоящий протокол. Всё, что о документе известно, то это то, что он датирован 25 января 2018 года и номер у него "5-пр".

Прошу отметить факт, что это внутренний протокол совещания Роскомнадзора. А РКН != Минкомсвязи, по заверению некоторых сотрудников Минкомсвязи. Хотя, на официальном сайте МКС Роскомнадзор, наряду с Россвязью и Роспечатью указан в разделе "подведомственные органы". Очень трудно там разобраться, особенно когда министр почти не заметен на фоне таких эпичных личностей, как Жаров.

Что из этого "протокола" можно понять. Попробую изложить последовательно:

1. Несмотря на то, что Законопроект был отклонен, Роскомнадзор продолжает "копать". Отметим факт, что Ростелеком не обязан выполнять указаний РКН, если требования не подкреплены законодательной базой. Насколько мне известно, никаких "реестров маршрутно-адресной информации (МАИ) ИС "Интернет" не существует. Но Ростелеком в процессе участвует.
2. Роскомнадзор, подчиненный ему ФГУП "ГРЦЧ" и совместно с формально не подчиненным им Ростелеком договариваются о "технических подходах" по реализации "реестра МАИ". И уже даже согласуют какие-то конкретные технические параметры и адресацию.
3. В системе МАИ существует подсистема с кодовым названием Blackhole. Из текста становится

понятным, что "подсистема" предназначена для организации блокировок IP-адресов по протоколу BGP.

Короткий вывод из этого: РКН готовит очередной способ блокировок "неугодного контента". И планирует провести "испытания" на буквально живых людях "в закрытом режиме на ограниченном сегменте сети Ростелекома". На сколько добровольно в этом "испытании" участвует Ростелеком - из документа не очень ясно. Но участвует.

А поскольку нарушение связности на уровне базовых протоколов маршрутизации может повлечь нарушение функционирования Интернет вообще, то можно предположить, что в ближайшее время на сетях Ростелекома будут технические проблемы.

Давайте попробуем разобраться, что и как можно заблокировать.

Очевидно, речь идет о технологии, описанной в RFC 7999 под названием BLACKHOLE Community. RFC был написан еще в 2016-ом инженерами из DE-CIX из Франкфурта, Германия. У них уже довольно давно даже такая услуга есть, которая так и называется Blackholing.

Суть сводится к достаточно простой штуке - BGP-маршрутизации "вредного трафика" в "drop".

Необходимость системы оповещения всех автономных систем (peers) говорит о том, что на какой-то конкретный IP-адрес маршрутизировать трафик не нужно. Собственно, "вредным трафиком" при разработке механизма, или точнее сказать метода, считается трафик при DDoS-атаках.

И действительно, если какой-то интернет-хост при DDoS атаке просто отключить от интернета, то это собственно то, чего добивался злодей при организации атаки. То есть недоступность некоторого узла.

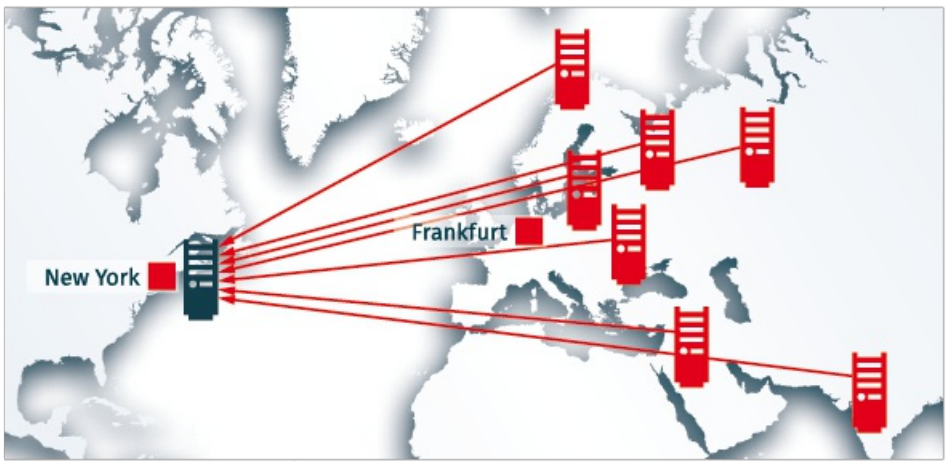
При этом, если атака действительно "распределенная" (слово Distributed в аббревиатуре как бы намекает), то выявить источник вредоносного трафика фактически невозможно. Но можно выявить, или заранее определить довольно безопасные маршруты. Что, собственно, RFC-7999 и описывает.

Но для того, чтобы раздать всем автономным системам адрес хоста, по которым нужно дропать пакеты, необходима какая-то информационная система, передающая нужную информацию. То есть, IP-адрес системы, находящийся под атакой. И передавать эту информацию нужно достаточно оперативно и в такой последовательности: выявили атаку -> определили главные источники вредных пакетов -> передали AS целевой хост для передачи трафика в "черную дыру". Атака прекратилась - тут же все автономные системы оповещаются о том, что сбрасывать пакеты не нужно.

Достаточно просто написать один абзац "видения системы", но вот реализовать такую систему гораздо сложнее. Потому что для реализации такой схемы нам будет нужно, во-первых, соответствующее оборудование с поддержкой этого механизма, а. во-вторых, добрая воля участников обмена трафиком, которые бы ВНЕЗАПНО согласились бы, чтоб их маршрутами управлял кто-то другой.

Пункт "во-вторых" мы оставим на сладкое, а вот по первому - решение есть. Называется BGP Communities.

Для неинженерного читателя попробую объяснить на картинках, которые невозбранно взяты с сайта DE-CIX:



На картинке выше - обычное состояние автономных систем, которые входят в "сообщество" (Communities) по обмену трафиком со включенной опцией BGP Communities. Эти АС обозначены красненьким и находятся в "старом свете". Тут выясняется, что началась распределенная атака на

ресурс в Нью-Йорке (синенький).



Некая система обнаружения DDoS (возможно, просто админы, у которых поднялся алярм в системе мониторинга) просигналила представителям франкфуртской IX о том, что некий конкретный IP-адрес необходимо вывести из-под атаки специальным сообщением Blackhole announcement. И теперь все АСки начали объявлять атакуемый хост недоступным. Достаточно просто. Причем, например, атакуемый сервер в Нью-Йорке остается доступным для местных и не выключается. Да, потери владельца информационной системы от простоя будут, но не тотальные. Тем более что одновременно можно поднять резервные адреса этого хоста или еще что-то, что сведет потери от атаки к минимальному ущербу.

Для инженерно подкованного читателя я специально нагуглил хорошую статью, где все четко-конкретно описано на русском языке. Вот цитата, взятая на бложике:

BGP Communities является опциональным транзитивным (optional transitive) атрибутом маршрутов BGP, т.е. маршрутизатор, не поддерживающий данный атрибут, просто передаст его другому маршрутизатору без изменений. Атрибут BGP Communities может передаваться как внутри одной AS, так и между разными AS. С помощью BGP Communities "помечаются" (можно ещё сказать тегируются) маршруты BGP, с которыми в дальнейшем возможно выполнить те или иные действия на основании данного Community (например поменять Local Preference). Таким образом, данный атрибут "приклеивается" к определённому маршруту/префиксу, передаваемому в update'ах через BGP. Атрибут BGP Communities в чём-то напоминает тегирование маршрутов (route tag) в классическом варианте. BGP Communities - это 32-ух битное значение от 0 до 4 294 967 200, записываемые, как правило, в формате AS_NUMBER:VALUE, где AS_NUMBER - номер AS, установившей данный community (значения "все нули" и "все единицы" зарезервированы), VALUE - произвольное числовое значение.

*Для представления BGP Communities в таком виде на оборудовании Cisco (*обратим внимание, что на оборудовании других вендоров этот механизм может быть реализован иначе - прим. WF*) необходимо добавить команду:*

```
ip bgp-community new-format
```

в режиме глобального конфигурирования.

Существуют так называемые well known communities, и имеют они не числовое значение:

- no-advertise - update с таким community не будет передан ни одному пиру;
- no-export - update с таким community не будет передан ни одному внешнему пиру, кроме внешних пиров внутри конфедерации. Является одним из наиболее распространённых community;
- local-as - update с таким community будет передан только внутри локальной AS или в AS - члене конфедерации;
- internet - update с таким community будет передан повсюду.

В статье есть примеры конфигураций маршрутизации и подробное описание механизма. Но на действующие атрибуты конфигов прошу обратить особое внимание - далее они будут важными.

Но мы вернемся к РКН и МАИ ИС "Интернет". Это обещанное сладкое.

Для того чтобы Blackhole announcement заработал в принципе - должно быть создано "сообщество", которое доверяет этим анонсам. Это и есть разрабатываемое РКН поделие "реестр маршрутно-адресной информации (МАИ) ИС "Интернет". Очевидно, что всех операторов, имеющих собственные автономные системы, будут в эту самую МАИ загонять.

Механизм загона - понятен и уже опробован на примере "АС Ревизор". То есть, для создания общероссийской системы "испортить интернеты" совсем не нужно никаких законодательных актов класса "закон". Достаточно подзаконных актов, которые цензурное ведомство может штамповать пачками. И никакие законы "Об обеспечении устойчивости российского сегмента сети "Интернет"" де-юре не нужны.

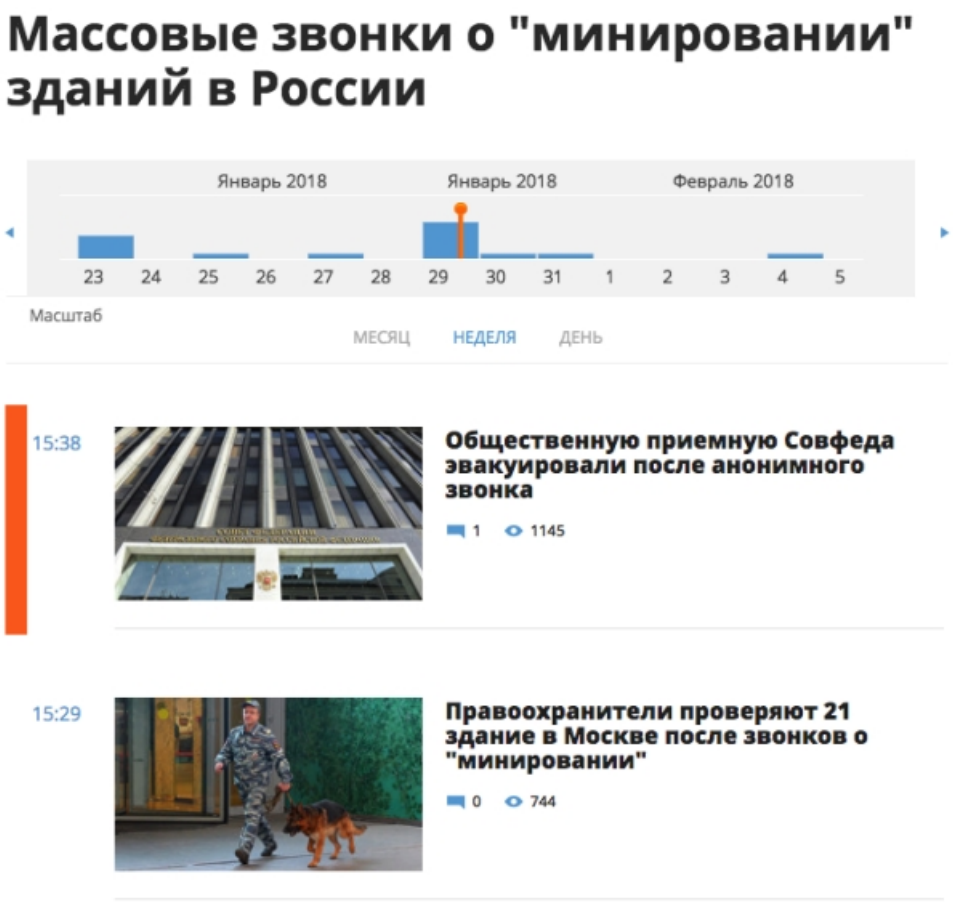
Это достаточно серьезная проблема для отрасли. Почему?

Объясняю:

1. Система блокировок, по сути, не работает. При этом российские интернет-провайдеры тратят значительные собственные средства и усилия для реализации фантазий регулятора.
Кто-то может возразить про то, что, например, LinkedIn или RuTracker был заблокирован и вот результат - они заблокированы. Но мы-то знаем, что блокировки обходятся в два клика, и что заблокированы все эти ресурсы довольно условно. В качестве примера: мой любимый мессенджер-рация Zello, заблокированный РКН еще в апреле 2017-го, но совершенно нормально функционирующий. Можете убедиться самостоятельно.



2. Система блокировок не столько помогает в борьбе с запрещенным контентом, сколько затрудняет оперативную работу с действительно плохими людьми. Об этой сентенции можно с удовольствием поспорить в комментариях, но я регулярно встречаю "рекламу" интернет-магазинов веществ на улицах. Или вот случаи с телефонным терроризмом, где спецслужбы показали себя абсолютно импотнентыми что-нибудь решить. Случаи "телефонного терроризма", к слову, очень хорошо мониторят РИА "Новости" - можете убедиться, что их не стало меньше.



3. Архитектурные слабости систем блокировок могут быть использованы против самой системы. Напомню, летом 2017-го была целая волна блокировок произвольных ресурсов по DNS-записям заблокированных доменов. Так, что РКН даже пришлось вводить "белые списки". Если вы думали, что проблема решена, то нет. Вот очередные истеричные документы РКН про теперь уже "избыточные блокировки":

РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ТЮМЕНСКОЙ ОБЛАСТИ, ХАНТЫ-МАНСИЙСКОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ И ЯМАЛО-НЕНЕЦКОМУ АВТОНОМНОМУ ОКРУГУ
(Управление Роскомнадзора по Тюменской области, Ханты-Мансийскому автономному округу – Югре и Ямало-Ненецкому автономному округу)

ул. Республики, д. 12, Тюмень, 625003
телефон: (3452) 56-86-50; факс: (3452) 56-86-51
E-mail: rsockanc72@rkn.gov.ru

29.01.2018 № 1969-03/72

На

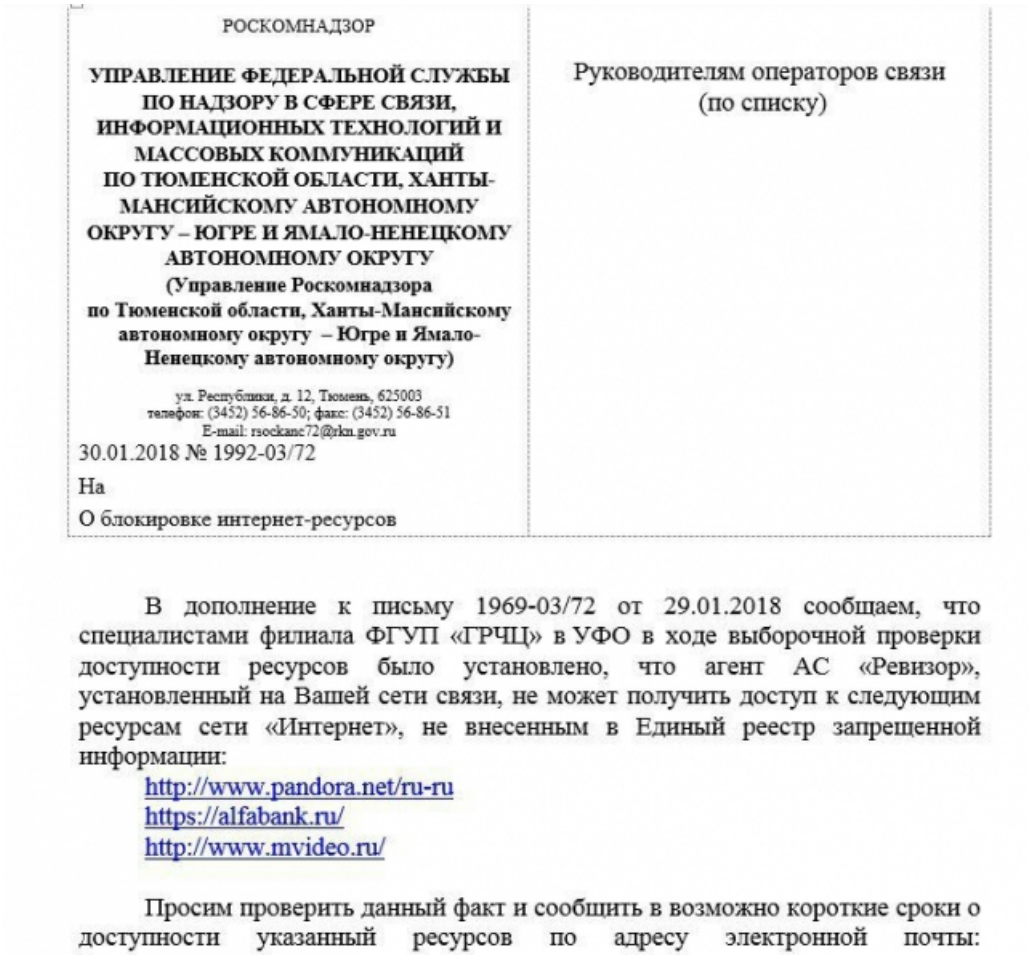
О направлении информации

Руководителям операторов связи
(по списку)

В ходе анализа информации о блокировании операторами связи доступа к запрещенным ресурсам специалистами ФГУП «ГРЧЦ» на территории различных субъектов Российской Федерации выявлены случаи избыточного ограничения доступа к ресурсам сети Интернет либо умышленное препятствие штатной работе агента АС «Ревизор».

В настоящее время филиалами ФГУП «ГРЧЦ» проводится внеплановый мониторинг операторов связи на предмет выявления избыточного ограничения доступа к ресурсам сети Интернет, не внесенным в Единый реестр запрещенной информации. В случае выявления подобных фактов материалы будут направлены в территориальные органы Роскомнадзора для принятия мер в установленном порядке.

Учитывая изложенное, просим осуществлять блокирование доступа к запрещенным ресурсам в соответствии с Единым реестром, а также обеспечивать корректную работу агента АС «Ревизор».



РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ТЮМЕНСКОЙ ОБЛАСТИ, ХАНТЫ-МАНСИЙСКОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ И ЯМАЛО-НЕНЕЦКОМУ АВТОНОМНОМУ ОКРУГУ

(Управление Роскомнадзора по Тюменской области, Ханты-Мансийскому автономному округу – Югре и Ямало-Ненецкому автономному округу)

ул. Республики, д. 12, Тюмень, 625003
телефон: (3452) 56-86-50; факс: (3452) 56-86-51
E-mail: rsockanc72@rkn.gov.ru

30.01.2018 № 1992-03/72

На

О блокировке интернет-ресурсов

Руководителям операторов связи
(по списку)

В дополнение к письму 1969-03/72 от 29.01.2018 сообщаем, что специалистами филиала ФГУП «ГРЧЦ» в УФО в ходе выборочной проверки доступности ресурсов было установлено, что агент АС «Ревизор», установленный на Вашей сети связи, не может получить доступ к следующим ресурсам сети «Интернет», не внесенным в Единый реестр запрещенной информации:

http://www.pandora.net/ru-ru
https://alfabank.ru/
http://www.mvideo.ru/

Просим проверить данный факт и сообщить в возможно короткие сроки о доступности указанный ресурсов по адресу электронной почты:

Но вернемся к "реестру маршрутно-адресной информации (МАИ) ИС "Интернет".

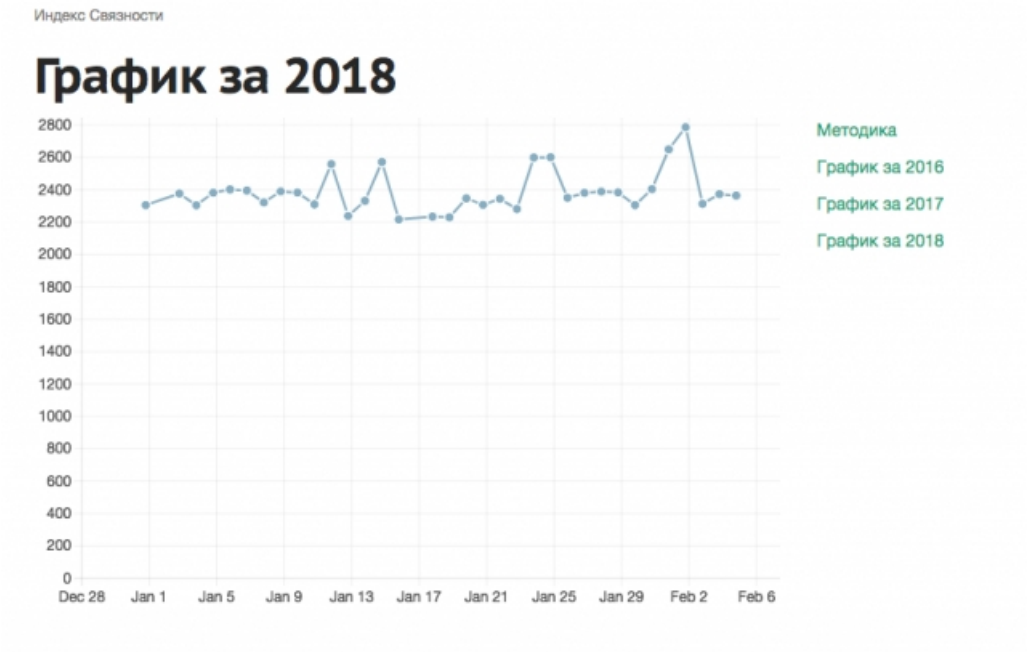
В самом начале приведена фоточка протокола совещания РКН, ГРЧЦ и Ростелекома, где имеется пункт 3.1. про "разовое копирование публичной информации из публичной базы данных RIPE DB". Особенно примечательна там приписка про "ограниченный доступ к ней по протоколу WHOIS". Зачем это нужно для "реестра МАИ" - я не понимаю. Но могу предположить, что таким образом горе-регуляторы хотят решить одну из, или обе сразу, задачи. Возможно, я ошибаюсь - это просто предположение:

1. Понять какие интернет-ресурсы хостятся в России, и как их половчее заблокировать.Тут могу только пожелать удачи, особенно в случае "разового копирования", да.
2. Понять какие автономные системы принадлежат именно российским провайдерам и хостерам.

По второму пункту - мы в "Обществе Защиты Интернета" уже выполнили эту работу. И ведем ее регулярно (РКН - обращайтесь! *ехидный смайл). И даже сделали небольшой мониторинговый инструмент, который считает так называемый "Индекс связности", который рассчитывается ежедневно.

Вычисляется "Индекс" следующим образом: это совокупное количество связей между российскими и нероссийскими автономными системами, рассчитанное автоматически на основании данных из атласа RIPE. (Если совсем упрощать, то можно в первом приближении сказать, что "автономная система" - это сеть одного провайдера или крупная корпоративная сеть).

Цель индекса - увидеть, когда число связей АС между российскими и иностранными операторами будет резко сокращаться. Это будет означать, что в России начали "отключать интернет" совсем. Ну, или что-то произошло экстраординарное. За третий год наблюдений, мы пока такового не зафиксировали, хотя некоторый тренд по сокращению связей все же заметен. Вот такой график у нас получается (есть еще за 16 и 17 годы - изучайте по ссылке):



Вывод из выше сказанного пока такой: интернет очень динамичная и изменяющаяся система, и "разовая выгрузка данных из RIPE DB" не поможет решить задачу выявления "всех российских АС".

Но что произойдет, когда всех (ха-ха!) российских владельцев АС загонят в "реестр маршрутно-адресной информации"?

Очевидно, что заставят принимать Blackhole-анонсы. И вот тут-то и начнутся реальные проблемы со связностью, которые, к слову, никак не решат проблемы неработающей системы блокировок.

Вот что будет:

1. Поскольку компетентность сотрудников РКН и ГРЧЦ множество раз ставилась под сомнение, то вполне возможно попадание в анонсы "черных дыр" адресное пространство популярных хостингов, CDN и даже целых подсетей операторов. Ну, например, "война РКН с Zello" может привести к недоступности целых подсетей. Единственное утешение - RFC-7999 рекомендует не блокировать подсети с маской меньше, чем /32, но то, что RFC не указ РКН, - публичный факт.
2. BGP-комьюнити - это довольно тонкая сфера для централизованного управления. Вообще, российские госорганы в целом, и тем более МКС многократно утверждали, что "институты гражданского общества - вредные". И с настойчивостью дятла пытаются то "перевести управление интернетом под ООН", то создать какой-то мифический "интернет для стран БРИКС". Что еще раз подтверждает, что компетентность регулятора находится где-то на уровне домохозяек. Очевидно, что доверие комьюнити к регулятору будет находиться где-то в той же категории. И не потому что "российские операторы не патриотичны". Но потому, что операторы зарабатывают деньги. А сломанные системы денег не приносят совсем.
3. Механизмы blackhole-комьюнити, описанные в приведенном выше списке атрибутов анонсов, позволяют потенциально вмешаться в систему работы "реестра МАИ" кому угодно, входящему в комьюнити. Еще раз - потенциально. И это может _потенциально_ стать одним из методов жесткой конкурентной борьбы. Можно будет просто произвольно "отключать вражеские АС" в одну команду с подменой значения атрибута с *no-export* на *internet.* Хотя, возможно, здесь я преувеличиваю.

Ну, и традиционная гифка. Реакция здорового человека, когда РКН предлагает что-то попробовать:

