Быть лучше каждый день

О ГРАНИЦАХ, ДОВЕРИИ, БЕЗОПАСНОСТИ И КООПЕРАЦИИ

Ольга Макарова

28 апреля 2021 года

Вестфальская модель мира

- Вестфальский мир состоит из суверенных государств, в нем отсутствует общемировая высшая власть и принцип универсалистской иерархии в управлении;
- Вестфальский мир базируется на принципе суверенного равенства государств и невмешательстве в дела друг друга;
- в Вестфальском мире суверенное государство обладает неограниченной полнотой власти на своей территории над своими гражданами;
- Вестфальский мир регулируется международным правом, понимаемым как право договоров суверенных государств между собой;
- в Вестфальском мире только суверенные государства выступают субъектами международного права, и потому только они являются признанными участниками.

О нахождении внутри и вне Вестфальской модели мира

Внутри Вестфальской модели мира

Операторы связи обязаны строго соблюдать положения местного законодательства.

В большинстве юрисдикций операторы связи должны иметь лицензию.

Операторы мобильной связи должны иметь разрешение на использование частот в каждой юрисдикции.

Для ведения бизнеса в другой юрисдикции требуется регистрация другого юридического лица.

Каждое юридическое лицо в каждой юрисдикции развертывает телекоммуникационную инфраструктуру для обслуживания пользователей только на территории этой юрисдикции.

Поддержка клиентов для каждой юрисдикции предоставляется на родном языке этой юрисдикции.

Операторы связи всегда сильно зависят от местного законодательства. Нарушение закона - потеря лицензии.



Вне Вестфальской модели мира

Провайдеру OTT часто не нужно создавать юридическое лицо в юрисдикции и получать лицензию на услуги связи, чтобы предоставлять пользователям Интернета в этой юрисдикции доступ к своим услугам.

Пользователи получают доступ к OTT через телекоммуникационную инфраструктуру операторов связи в разных юрисдикциях.

OTT не нуждается в организации поддержки пользователей другой юрисдикции на их родном языке, этим занимаются операторы связи.

Число OTT провайдеров существенно превышает число операторов связи

Локальные требования сетевого нейтралитета и требования клиентов позволяют сохранить хрупкий баланс интересов OTT и телекомов.

1. **Вестфальская модель мира не предусматривает возможности отказа от национального регулирования и перехода к трансграничному регулированию.**

2. **Никто в мире не готов отказаться от Вестфальской модели мира, пандемия еще раз подтвердила это.**

3. **Развитие института законодательства не успевает за развитием технологий. Существует конфликт между необходимостью применять местные законы в каждой юрисдикции и трансграничным характером интернет-услуг.**

4. **Тем не менее, новые подходы к регулированию с учетом трансграничного характера услуг необходимы.**

Самой главной ценностью должны быть пользователи.

Взгляд в прошлое

В марте 2000 года в Лиссабоне на встрече глав государств-членов ЕС была озвучена Европейская стратегия развития информационных и телекоммуникационных технологий (ICT) на период до 2010 года. Документ получил название Лиссабонской стратегии и обозначение i2010.

Цели i2010:

- **создание на базе государств ЕС наиболее конкурентно способного общества в мире**

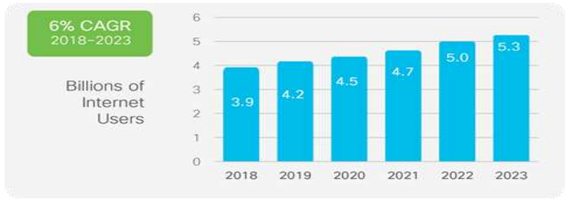
- **обеспечение полной занятости всего населения Европы к 2010 году.**

Одно важных направлений i2010 - формирование информационного сообщества стран – членов ЕС.

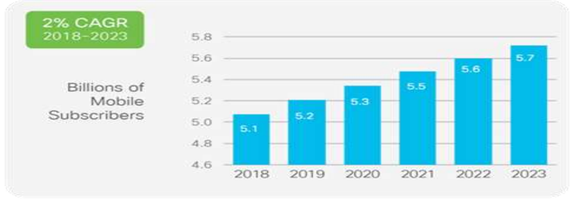
- **Цель формирования информационного сообщества стран – членов ЕС - повышение качества жизни всех граждан Европейского сообщества через активное внедрение информационных и телекоммуникационных технологий в повседневную жизнь.**

Несколько цифр из Cisco Annual Internet Report (2018–2023) White Paper

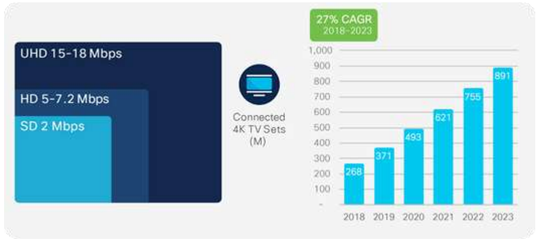
Рост числа пользователей Интернет во мире



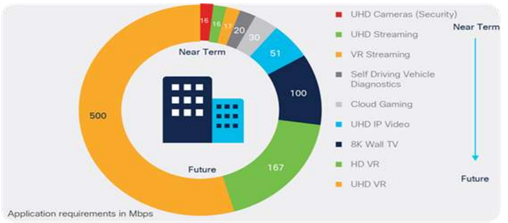
Рост числа абонентов мобильной связи в мире



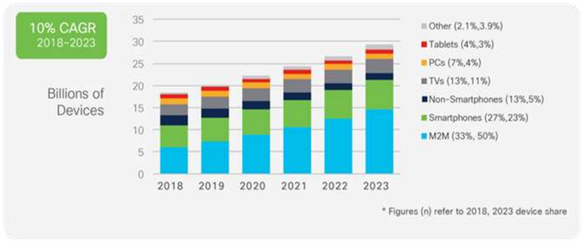
Повышение разрешения видео: к 2023 году 66 процентов подключенных плоских телевизоров будут с разрешением 4K.



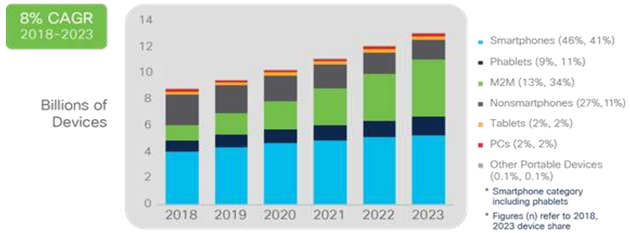
Распределение пропускной способности доме будущего



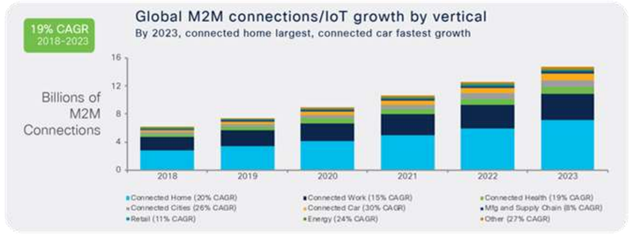
Рост числа устройств и подключений по всему миру



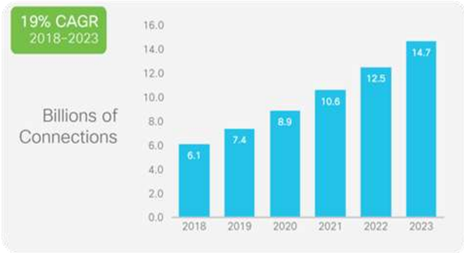
Рост числа мобильных устройств и подключений во всем мире



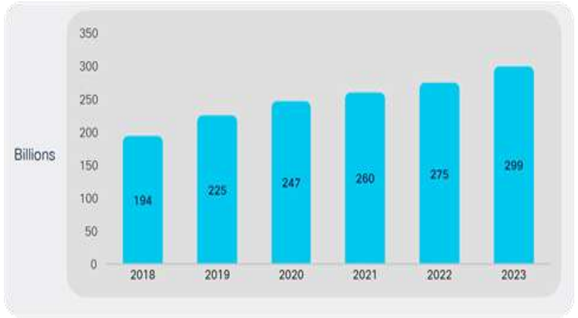
Глобальный рост M2M-подключений по отраслям



Рост числа подключений M2M в мире

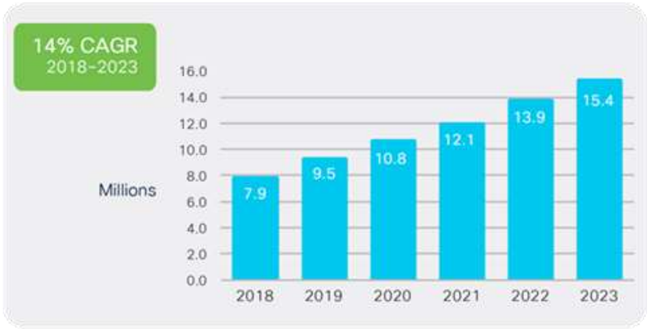


К 2023 году будет загружено около 300 миллиардов мобильных приложений



Количество DDoS-атак: к 2023 году количество атак увеличится вдвое, до 15,4 млн.

Пользователи ожидают, что их опыт работы в сети будет всегда доступен и всегда безопасен, а их личные и деловые активы - в безопасности.

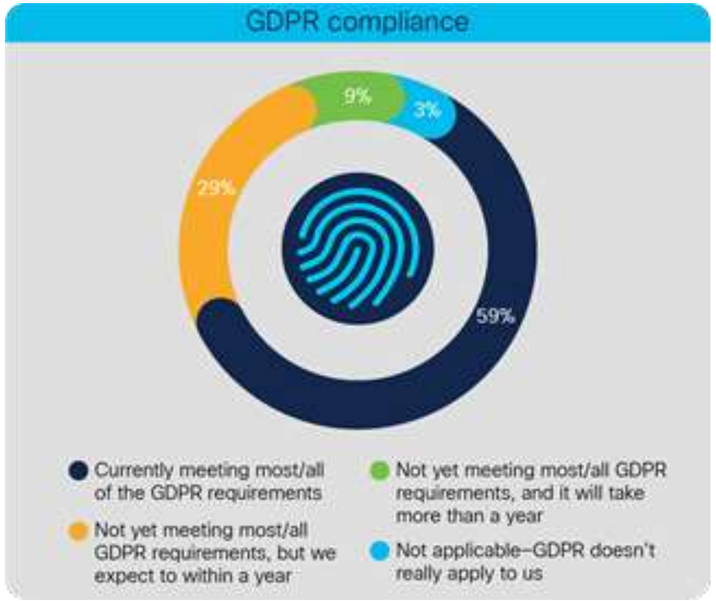




https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

О тонких маркетинговых ходах в регуляторной бюрократии

Насколько хорошо ваша компания соблюдает действующие Общие правила защиты данных (GDPR) согласно Cisco Annual Internet Report (2018–2023) White Paper ?

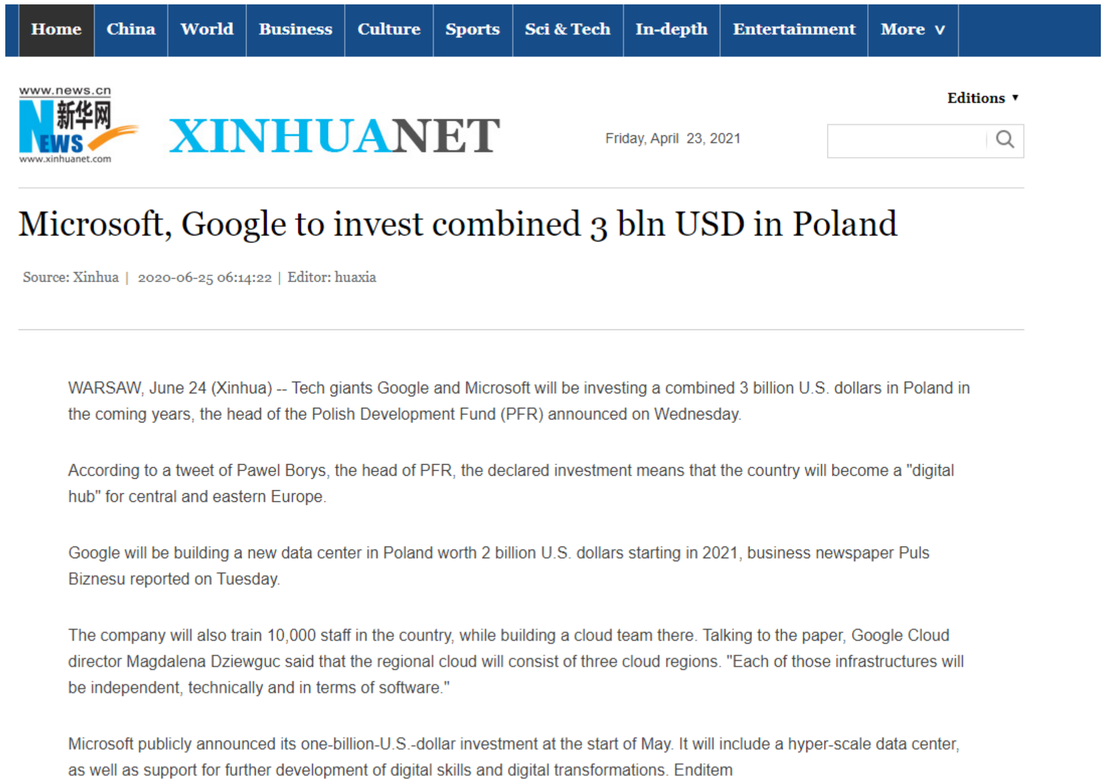


Согласно сравнительному исследованию конфиденциальности данных Cisco за 2019 год, 59 процентов глобальных компаний указали, что сегодня они соответствуют всем или большей части требований GDPR. Еще 29 процентов заявили, что они будут готовы к GDPR в течение года, а 9 процентов заявили, что на подготовку потребуется больше года. Хотя GDPR применяется к предприятиям в ЕС или к обработке персональных данных, собранных о лицах, находящихся в ЕС, только 3 процента респондентов в глобальном опросе указали, что они не верят, что GDPR применяется к их организациям.

Источник: Максимизация отдачи от инвестиций в конфиденциальность данных, Cisco, январь 2019 г. [Процент респондентов: N = 3,206]

В GDPR была предпринята попытка учета трансграничного характера услуг, но GDPR распространяет свое действие только на европейских пользователей. Следуя логике GDPR каждая страна мира должна принять аналогичный акт для защиты персональных данных своих пользователей.

Об инвестициях ИТ-гигантов



Home | China | World | Business | Culture | Sports | Sci & Tech | In-depth | Entertainment | More ∨

www.news.cn 新华网 NEWS www.xinhuanet.com XINHUANET

Editions ▾

Friday, April 23, 2021

Microsoft, Google to invest combined 3 bln USD in Poland

Source: Xinhua | 2020-06-25 06:14:22 | Editor: huaxia

WARSAW, June 24 (Xinhua) -- Tech giants Google and Microsoft will be investing a combined 3 billion U.S. dollars in Poland in the coming years, the head of the Polish Development Fund (PFR) announced on Wednesday.

According to a tweet of Pawel Borys, the head of PFR, the declared investment means that the country will become a "digital hub" for central and eastern Europe.

Google will be building a new data center in Poland worth 2 billion U.S. dollars starting in 2021, business newspaper Puls Biznesu reported on Tuesday.

The company will also train 10,000 staff in the country, while building a cloud team there. Talking to the paper, Google Cloud director Magdalena Dziewguc said that the regional cloud will consist of three cloud regions. "Each of those infrastructures will be independent, technically and in terms of software."

Microsoft publicly announced its one-billion-U.S.-dollar investment at the start of May. It will include a hyper-scale data center, as well as support for further development of digital skills and digital transformations. Enditem

Технологические гиганты Google и Microsoft в ближайшие годы инвестируют в Польшу в общей сложности **3 миллиарда долларов США**, заявил в среду глава Польского фонда развития (PFR).

Согласно твиту главы PFR Павла Бориса, заявленные инвестиции означают, что страна станет «цифровым центром» для Центральной и Восточной Европы.

Google будет строить новый центр обработки данных в Польше стоимостью 2 миллиарда долларов США, начиная с 2021 года, сообщила во вторник деловая газета Puls Biznesu.

Компания также обучит 10 000 сотрудников в стране и создаст там облачную команду. В беседе с газетой директор Google Cloud Магдалена Дзевгуц сказала, что региональное облако будет состоять из трех облачных регионов. «Каждая из этих инфраструктур будет независимой технически и с точки зрения программного обеспечения».

Microsoft публично объявила о своих инвестициях в один миллиард долларов США в начале мая. Он будет включать в себя гипермасштабный центр обработки данных, а также поддержку для дальнейшего развития цифровых навыков и цифровых преобразований. Enditem

На конференциях часто указывают на то, что из-за геополитики в России никогда не будет ЦОД глобальных ИТ-гигантов, а, соответственно, и инвестиций такого уровня. Все ограничится небольшими выносами в виде некрупных узлов и кэширующих серверов CDN.

Нужны ли России такие инвестиции, и какова их цена?

В логике бизнеса ИТ гиганты не делятся на западных и восточных. Имея страну происхождения, они действуют «вне Вестфальской модели мира».

России нужны свои игроки, действующие «вне Вестфальской модели мира». Для реализации этого необходимо «умное», гибкое, настраиваемое регулирование, разумный уровень конкуренции на внутреннем рынке, в том числе с глобальными игроками и кооперация с ними в продвижении собственных интересов.

О том, почему невозможно строительство Интернет на доверии, и почему вопрос перехода от доверия к авторизации может быть решен только при кооперации всех участников

IPv4 Routing Table					Growth		
	Jan-18	Jan-19	Jan-20	Jan-21	2018	2019	2020
Prefix Count	699,000	760,000	814,000	860,000	9%	7%	6%
AS Count	59,700	63,100	66,800	70,400	6%	6%	5%

Table 2 — IPv4 routes data.

Статистика IPv4 BGP за период 2018 – 2020 согласно отчета BGP 2020 https://blog.apnic.net/2021/01/05/bgp-in-2020-the-bgp-table/

IPv6 Routing Table					Growth		
	Jan-18	Jan-19	Jan-20	Jan-21	2018	2019	2020
Prefix Count	47,700	62,400	79,400	109,130	23%	22%	28%
AS Count	14,500	16,470	18,600	21,600	14%	14%	14%

Table 3 — IPv6 routes data.

Статистика IPv6 BGP за период 2018 -2020 согласно отчета BGP 2020 https://blog.apnic.net/2021/01/05/bgp-in-2020-the-bgp-table/

В ближайшее время число миллиона маршрутов (IPv4 и IPv6 вместе) достигнет одного миллиона.

Источник: https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/

O BGP Hijacking

BGP Hijacks

In 2020, BGPStream collectors identified 2,477 BGP hijack events, including three major incidents:

- April — Rostelecom (AS12389) hijack
- July — ATLDC – Tulix Systems, Inc (AS10990) hijack
- September — Telstra (AS1221) hijack

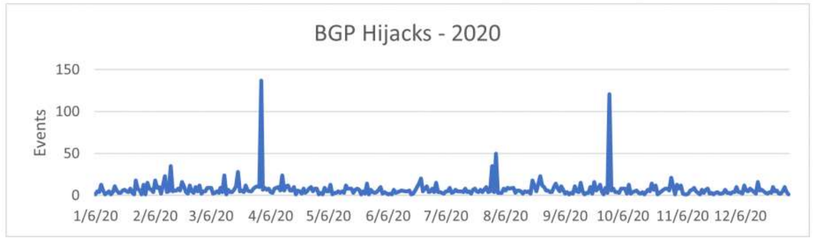


Figure 1 — BGP hijacks in 2020.

BGP Leaks

Another category of events is BGP leaks. In 2020, there were 1,396 events identified as leaks, including two major incidents:

- CONVERGE-AS17639 Converge ICT Solutions (PH) leaking prefixes from Korea
- CONVERGE-AS17639 Converge ICT Solutions (PH) leaking prefixes from Korea, India, and Brazil.



Figure 2 — BGP leaks in 2020.

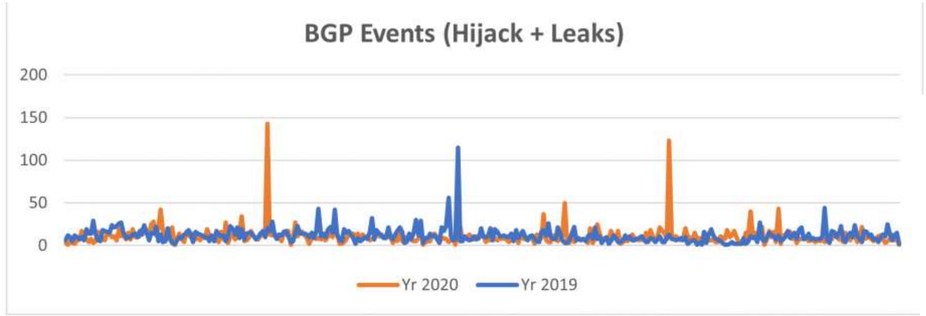


Figure 3 — BGP events comparison (both hijacks and leaks).

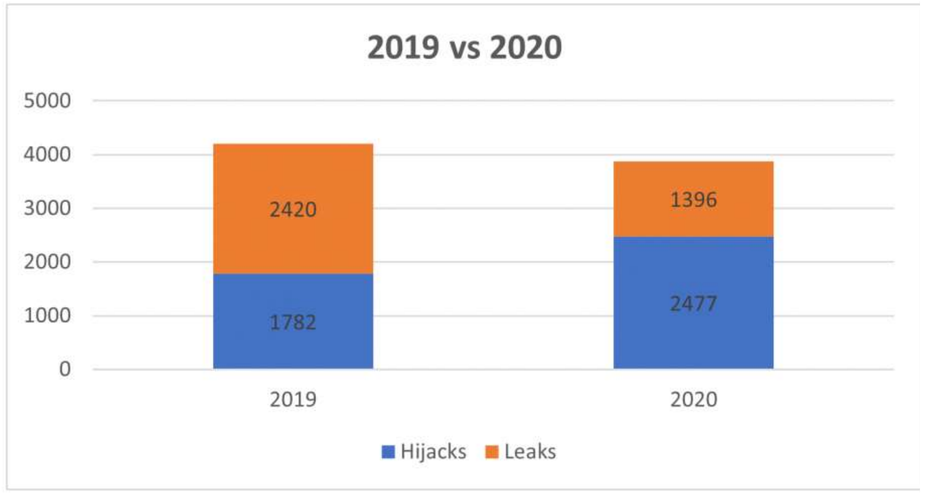


Figure 4 — Comparison of 2019 and 2020 BGP incidents.

BGP Hijacks

Description	2019	2020
Total Events	1782	2477
Impacted ASN	1147	1509
Possible Culprit ASN	864	997
Impacted Prefixes	1685	2357
IPv6 Prefixes	79	132
IPv4 Prefixes	1606	2225

Table 4 — BGP hijacks in 2019 and 2020

BGP Leaks

Description	2019	2020
Total Events	2420	1396
Impacted ASN	1957	885
Possible Culprit ASN	629	337
Impacted Prefixes	2638	1081
IPv6 Prefixes	0	0
IPv4 Prefixes	2638	1081

Table 5 — BGP leaks in 2019 and 2020.

https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/

Обвинить нельзя оправдать



«Маршруты интернет-трафика управляются протоколом пограничного шлюза (BGP).

BGP контролирует путь, которым интернет-трафик перемещается из одной сети автономной системы (AS) в другую на пути к месту назначения.

У каждой AS есть свой номер (ASN).

По состоянию на февраль 2020 года было зарегистрировано более 94000 AS.

Существует множество возможных маршрутов от источника к месту назначения - BGP определяет лучший маршрут в любой момент времени.

Устройства с поддержкой BGP объявляют или передают информацию о маршрутах, которые они могут предложить устройствам BGP в соседних сетях.

Эти сети затем передают эту информацию своим соседним сетям. Таким образом, изменения в «лучших маршрутах» распространяются в Интернет.

BGP был впервые создан в 1989 году и начал широко использоваться в 1994 году. В этот период Интернет был основан на доверии.

В случае объявления одной сетью нового «лучшего маршрута», это объявление принимается соседними сетями и повторно объявляется.

Захват интернет-трафика на основе BGP может быть очень простым - устройство BGP, которое захватывает, объявляет своим соседям, что они должны отправить определенный трафик по некорректному маршруту.

Считается, что большинство угонов происходят случайно.

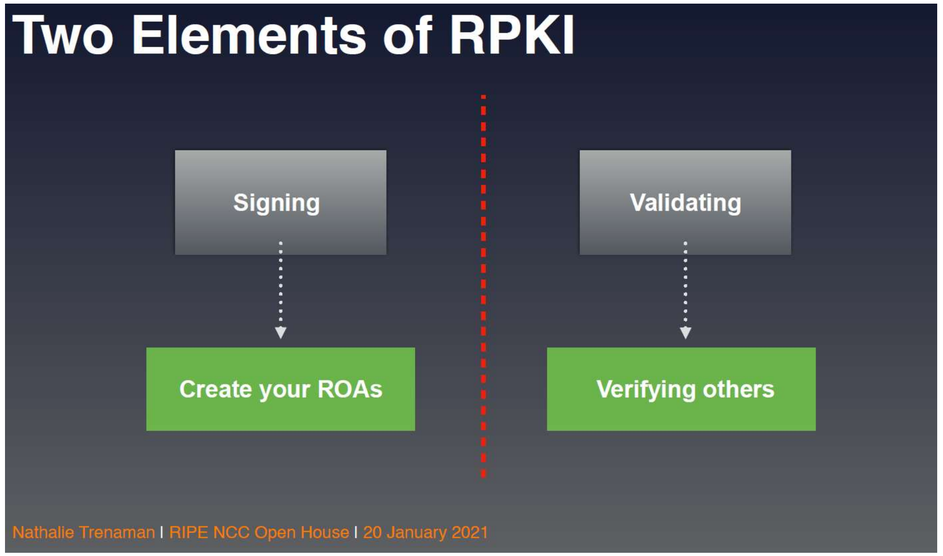
Основная проблема в том, что отличить случайную опечатку от запланированной практически невозможно.

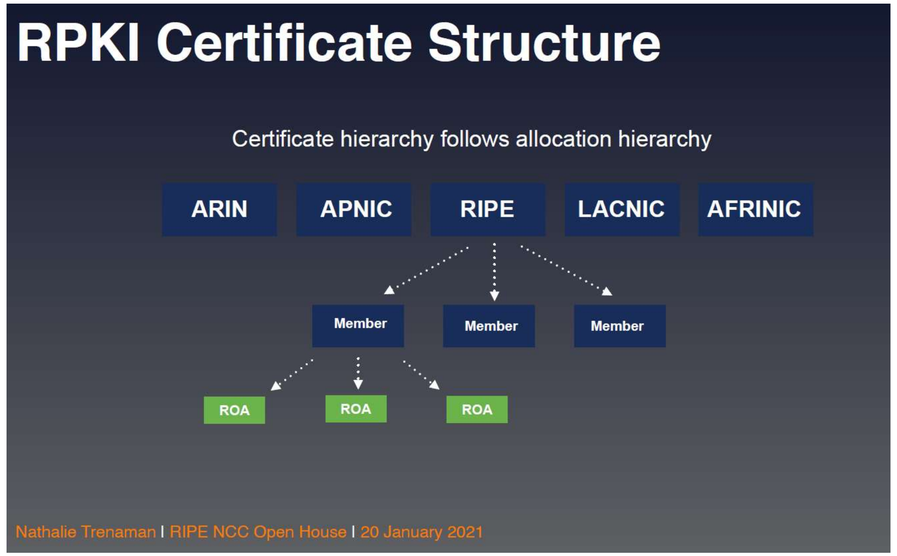
«Учитывая текущую геополитическую напряженность, любой захват BGP, исходящий из России или Китая, неизбежно вызовет удивление, а обе страны являются серийными угонщиками.»

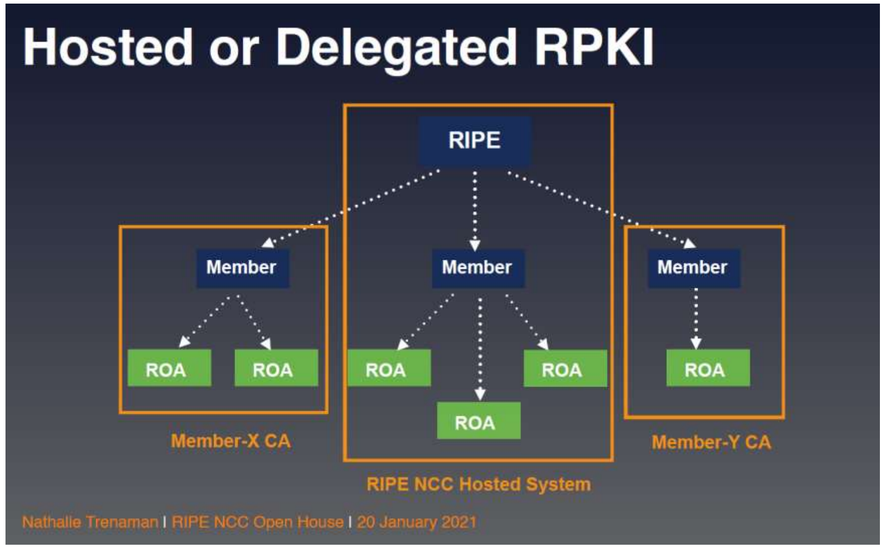
«Любопытно, что в 2017 году одному из крупных операторов России удалось случайно перехватить маршруты крупных финансовых организаций.».

В инциденте 2020 года большинство затронутых префиксов были зарегистрированы в ARIN: Amazon, Akamai, Cloudflare и т. д.

Повышение безопасности BGP с помощью Resource Public Key Infrastructure (RPKI)







О переходе от «доверия» к «авторизации» и о кооперации игроков рынка



Figure 6 — Charts of routing completeness. Source: MANRS Observatory.

Приведенные графики демонстрируют тенденцию к увеличению действительных ROA и сокращению недействительных ROA. В январе 2019 года было только 10% действительных ROA, 85% неизвестных (не найдено) и 5% недействительных. Сегодня у нас около 28% действительных ROA (около 180000 IPv4 и 31000 IPv6) в таблице глобальной маршрутизации и только 1% недействительных.

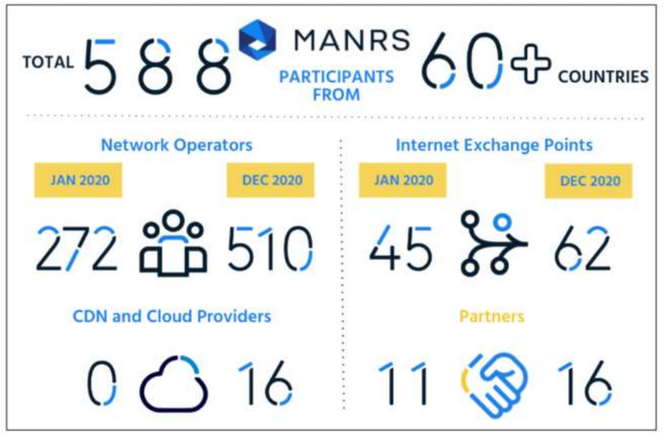


Figure 8 — Summary of 2020 MANRS progress.

В 2020 году наблюдался впечатляющий рост участия MANRS, а это означает, что теперь все больше людей осознают проблемы, которые может создать небезопасная маршрутизация, если не решить ее должным образом. Благодаря сотням инициатив по привлечению сообщества и созданию потенциала, MANRS помог многим людям принять RPKI и другие технологии, которые могут повысить общую безопасность маршрутизации, по одной сети за раз.

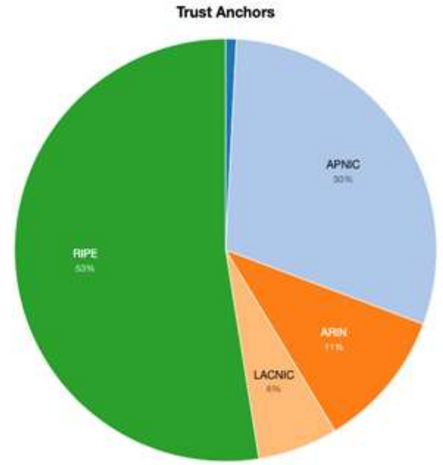
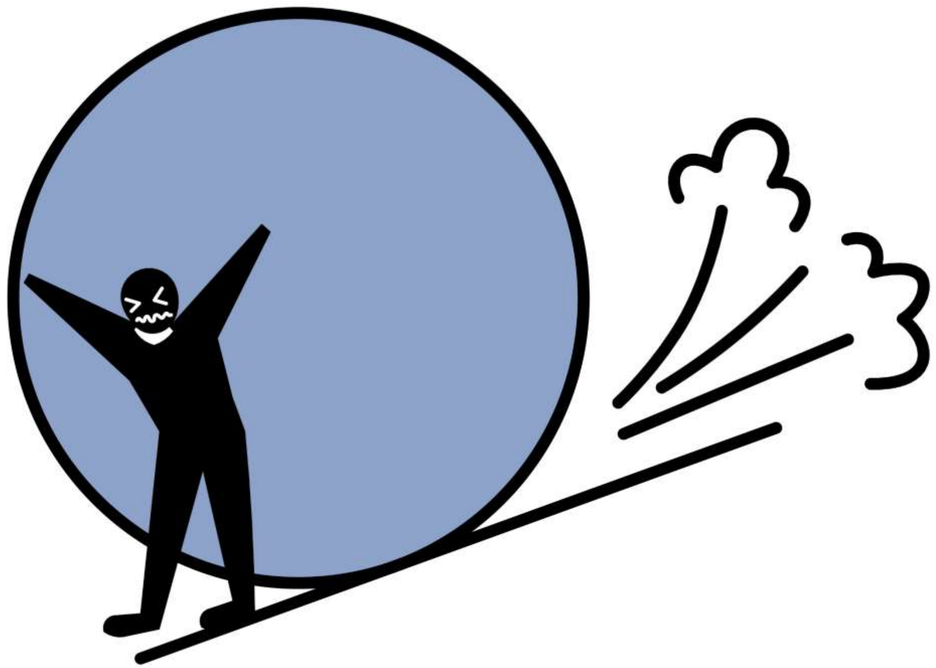


Figure 7 — Trust anchors by RIR (via rpki.cloudflare.net).

Статус ROA для региональных Интернет регистратур (RIR). RIPE выходит вперед, APNIC и остальные RIR быстро догоняют его.

https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/

Вместо заключения



Отставание



Неправильное решение,
ставшее фатальным

Благодарю за внимание