



DDoS – несколько советов по выбору защиты

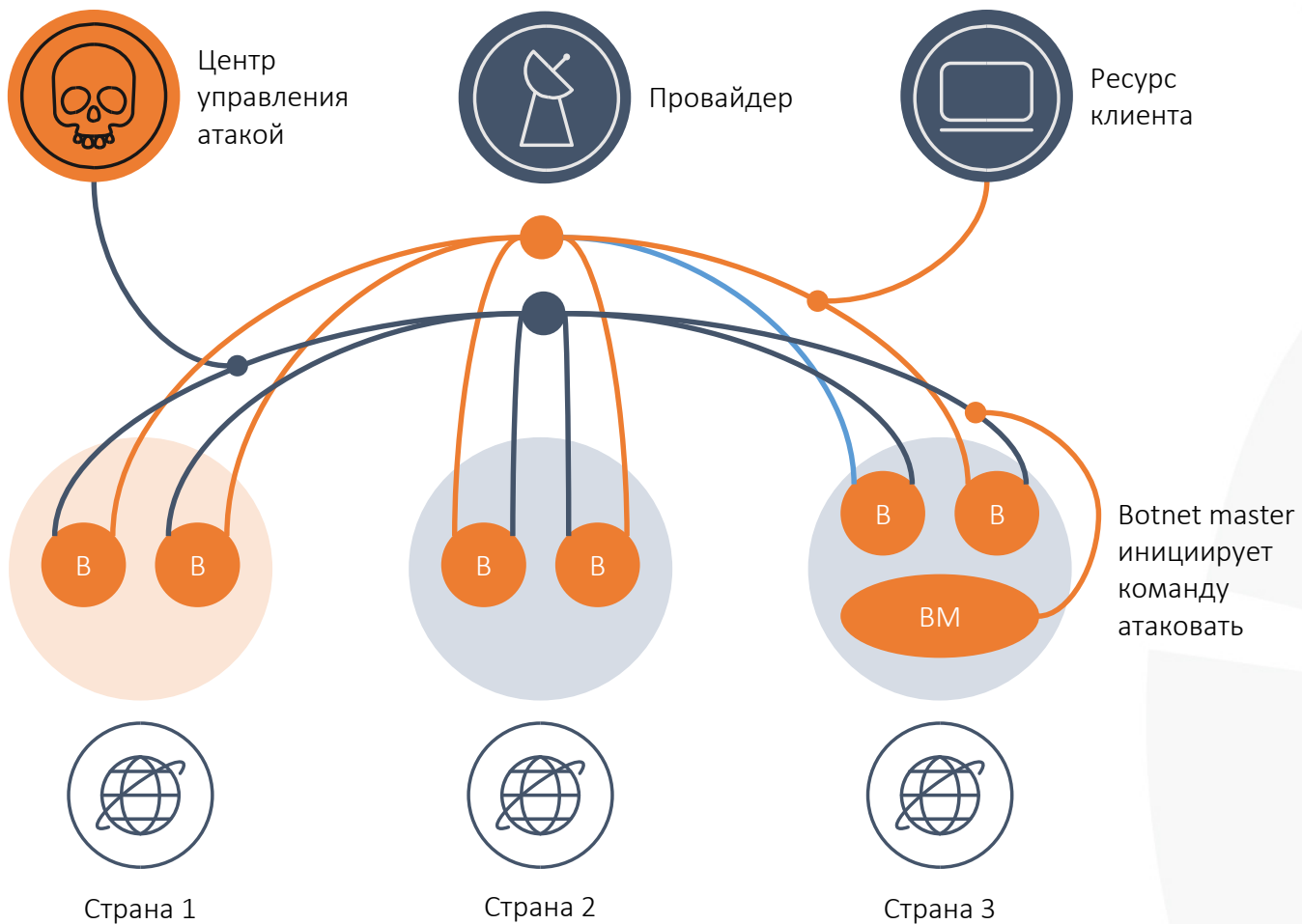
или чем вообще отличаются
сервисы ИБ

Иван Мирошниченко

Оглавление

- Вступление
- Что такое DDoS
- Статистика
- Какие бывают компании защищающие от DDoS
- Что они обещают
- Что на самом деле
- Основные критерии

WTF DDoS?

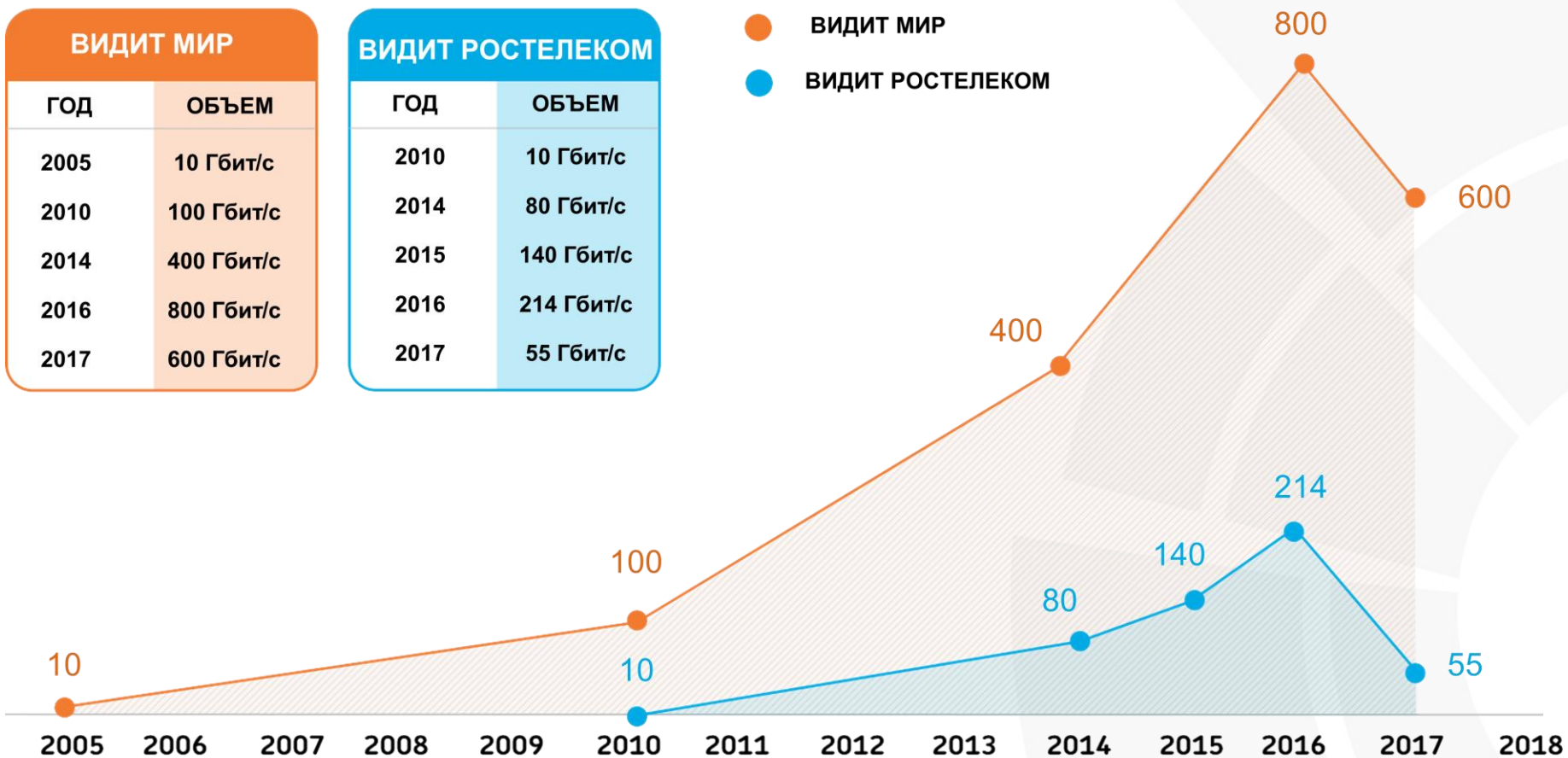


Что мы видим

ВИДИТ МИР	
ГОД	ОБЪЕМ
2005	10 Гбит/с
2010	100 Гбит/с
2014	400 Гбит/с
2016	800 Гбит/с
2017	600 Гбит/с



ВИДИТ РОСТЕЛЕКОМ	
ГОД	ОБЪЕМ
2010	10 Гбит/с
2014	80 Гбит/с
2015	140 Гбит/с
2016	214 Гбит/с
2017	55 Гбит/с

- ВИДИТ МИР
- ВИДИТ РОСТЕЛЕКОМ



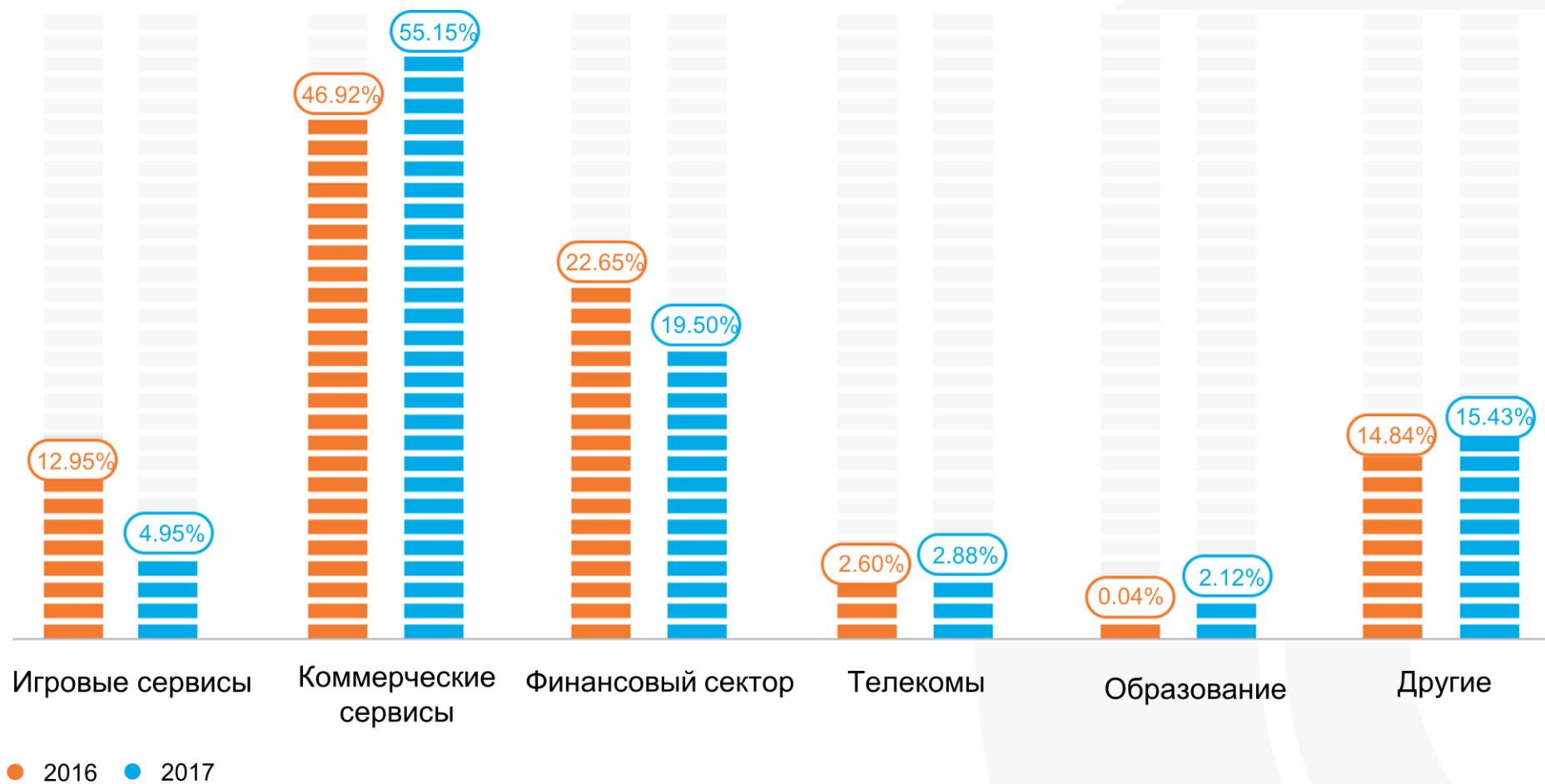
Что мы видим 2018

Summary

Severity Level:	Max Severity Percent:	Max Impact of Alert Traffic:	Direction:	Misuse Types:
 High  Fast Flood	316,038.0% of 30 Mbps Top Misuse Type: DNS Amplification	450.5 Gbps/44.3 Mpps at Managed Object Boundary	Incoming	ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification

- **450 Gbps!** По данным системы глобального мониторинга Atlas компании Arbor Networks за 2017-й год, доля атак подобной мощности составляет менее 0.001%
- DDoS-атака на Dtel.RU длилась более **15 часов**. По данным упомянутого отчета Arbor Networks, со столь продолжительными атаками в 2017 году сталкивался лишь 1% компаний
- **Клиенты Дагомыс-Телеком атаку не заметили**

Что мы видим. Отрасли



Куда бежать

ИДЕКС ✕ Найти

Поиск Картинки Видео Карты Маркет Новости ТВ онлайн Музыка Ещё

🚩 Kaspersky DDoS Protection – Ваш бизнес не остановить!
 KES Расширенный KES Стандартный KES Cloud Все продукты для бизнеса
[anti-ddos.kaspersky.ru](#) > защита-от-ddos-атак реклама
Защита от DDoS-атак для малого и среднего бизнеса! Не оставайся без защиты!
 20 лет спасаем мир · Официальный сайт · Надежная защита · 14 дней бесплатно
 Контактная информация · 8 (800) 200-22-33 · круглосуточно

🛡️ Защита от DDoS с гарантией – Без договора и предоплаты!
 Защита сайта Хостинг + Защита DDoS Защита IP Подключение за 10 мин.
[stormwall.pro](#) > Защита-от-DDoS-атак реклама
 Отразим текущую DDoS атаку и поможем определиться с выбором подходящего тарифа!
 Контактная информация · 8 (800) 550-89-39 · круглосуточно
 м. Славянский бульвар

🏠 Мощная защита от DDoS-атак – Быстрая активация
 Продукты Cloudflare Защита от DDoS-атак CDN Web Application Firewall
[cloudflare.com](#) > Защита-от-DDoS реклама
 Установка за 5 мин. Единая цена. Ультрамощная защита от DDoS-атак. Подключите!

🌐 Мгновенная защита от DDoS! – Технологии Beeline «Бизнес»!
 Быстрая реакция Защита Безопасность Поддержка
[beeline.ru](#) > DDoS-Защита реклама
 Мгновенное отражение DDoS-атак на сайты, мобильные приложения и оборудование.
 Контактная информация · 8 (800) 770-76-61 · пн-пт 10:00-18:00

Чаты с организациями по запросу защита от DDoS

StormWall.pro - защита от DDoS атак
 Отвечает ≈ 1 мин

Техподдержка Timeweb
 ≈ 1 мин

EFSOL
 ≈ 1 мин

ГиперХост
 ≈ 1 мин

Хостинг SRVGAME.RU

Признаки. Про бизнес

1. Регулятор не заблокирует?!
2. Тестовый период – а вдруг не взлетит... (но обязательно посмотреть возможности ЛК и отчетов)
3. Доступность техподдержки экспертного уровня в режиме 24/7 на русском языке
4. Трафик атаки не тарифицируется! (сегодня Ростелеком не тарифицирует и легитимный трафик)
5. А сколько стоит выделенный канал, и возможен ли он?
6. SLA?!

Признаки. Про технологии

1. А узлы-то есть поблизости?
2. Сколько их вообще, и какая их мощность, сколько аплинков?
3. А выделенный канал вообще возможен?
4. Какое время перевода трафика?
5. И снова о языке техподдержки...
6. Что с защитой DNS?
7. Опять SLA на false positives? А судьи кто?

И наконец

ТЕСТИРОВАТЬ!

Спасибо!

i.miroshnichenko@rt-solar.ru