

Сергей Дурягин



# Импортзамещение Реалии, а не сказки



# Реалии

## Технологии на шаг впереди злоумышленников



### Нобелевская премия 2022 года

«За эксперименты в области квантовых технологий»  
(в т.ч. для квантовой криптографии)



### Сертификат ФСБ России на СКЗИ

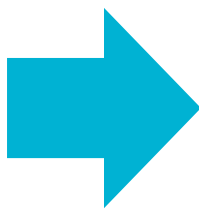
«Система квантового  
распределения ключей ViPNet  
QSS»

ИнфоТеКС – единственный производитель средств  
квантового распределения ключей и шифраторов

# Реалии. Нулевое доверие?

## Иностранные компании

- 1 Межсетевые экраны (NGFW)  
Fortinet, Cisco, Check Point, Palo Alto...
- 2 Защищенный удаленный доступ и  
защита каналов связи (VPN)  
Cisco, Check Point, Palo Alto...
- 3 Защита порталов/PKI/УЦ  
SSL/Microsoft CA...
- 4 Мессенджеры  
Slack, WhatsApp...



# Ненулевое доверие? Российские компании



## Декабрь 2022 г. ГК InfoWatch

ГК InfoWatch первой заявила о готовности начала продаж на российском рынке межсетевого экрана нового поколения InfoWatch ARMA NGFW для корпоративного сектора

## Январь 2023 г. «Позитив Технолоджис»

Мы создаем собственный межсетевой экран следующего поколения (next-generation firewall, NGFW), инвестиции более 750 млн рублей

## Апрель 2023 г. «РТК-Солар»

«У нас сегодня то, что у других – завтра».

**Solar NGFW** – импортонезависимый межсетевой экран для настоящего Enterprise

# Сказки

Гладко было на бумаге ...

Он умел делать всё,  
но у него ничего  
не получалось

# Сказки

Пропускная способность «на картинке»,  
т.е. на сайте

Кто, как и что считает? В попугаях?



| Пропускная<br>способность | UserGate<br>E1000 | UserGate<br>E3000 | UserGate<br>F800 |
|---------------------------|-------------------|-------------------|------------------|
| МЭ, UDP                   | до 25 Гбит/с      | до 30 Гбит/с      | до 60 Гбит/с     |
| МЭ, трафик<br>EMIX        | до 27 Гбит/с      | до 40 Гбит/с      | до 40 Гбит/с     |
| МЭ с DPI                  | до 15 Гбит/с      | до 18 Гбит/с      | до 40 Гбит/с     |

# Реалии

## Пропускная способность при нагрузочном тестировании

### Реальность в тестах заказчика:



| Нагрузочное тестирование | ViPNet xFirewall | Континент  | UserGate   |
|--------------------------|------------------|------------|------------|
| 1 правило                | 2.9 Гбит/с       | 3 Гбит/с   | 3.2 Гбит/с |
| 501 правило              | 1.9 Гбит/с       | 0.3 Гбит/с | 0.6 Гбит/с |
| 1001 правило             | 1.3 Гбит/с       | 0.2 Гбит/с | 0.5 Гбит/с |

# Не сказки

## Базы решающих правил для COV

### Cisco

(VRT, Talos)

Более 30 000  
сигнатур

ZeroDay сигнатуры

Страна  
происхождения:  
США



### ET

(Emerging Threats Pro)

Более 30 000  
сигнатур

ZeroDay сигнатуры

Страна  
происхождения:  
США



### ~~StoneSoft~~



### ИнфоТеКС

(AM Rules)

Более 24 000  
сигнатур (14 000  
собственных)

ZeroDay сигнатуры

Страна  
происхождения:  
Россия



# Доверие к заявленному функционалу

## SSL инспекция

Алгоритм работы:

1. Расшифровка SSL трафика
2. Определение угрозы
3. Блокировка угрозы



## Реальность

Алгоритм работы:

1. Расшифровка SSL трафика
2. А надо было?
3. А надо было?

# Доверие к базам решающих правил (БРП)



Февраль 2022 – отключение иностранных сервисов обновления БРП

## Snort / Suricata / антивирус

- Движок IDS/IPS?
- Используемые сигнатуры для IDS/IPS?
- Кол-во сигнатур IDS/IPS?
- Используемый антивирус?
- Кол-во антивирусных баз?

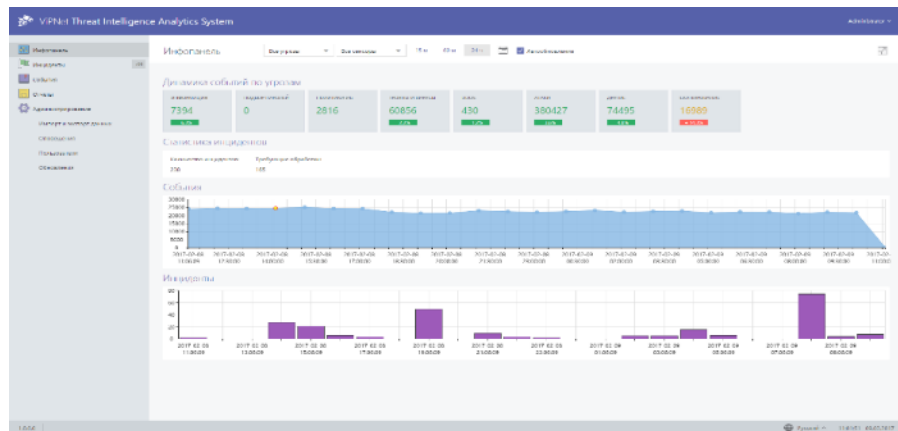
## Реальность

АО «Перспективный мониторинг»  
(ГК «ИнфоТеКс»):

- Advanced Monitoring - АМ
- Более **14 000** собственных АМ-сигнатур
- Антивирус Касперского

# Реалии

## Зарекомендовавшие себя решение TIAS + xFirewall



- сбор и анализ событий от сенсоров
- автоматическое выявление инцидентов
- оповещение об инцидентах
- инструменты для проведения расследований
- формирование отчетов



# Реалии.

## Госструктуры + коммерческий сектор

Здравствуйте, это такси. Я подъехал, выходите.

Но я не заказывала такси!

Сейчас тяжелые времена,  
мы ищем клиентов сами.



# Ответы на вопросы

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)

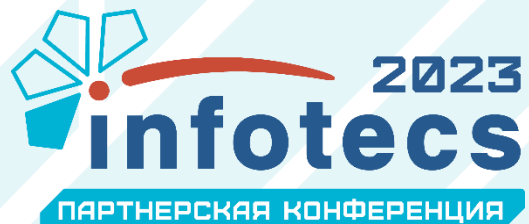


[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)





# Спасибо за внимание!

Сергей Дурягин  
Александр Реунов  
Иван (За)Лихвацких

При поддержке



m<sup>≡</sup>rlion

AXOFT

РУТОКЕН  
КОМПАНИЯ ПРАКТИВ

