



LATTELECOM  
цифровые  
решения  
из Латвии

# Атака на корпоративную инфраструктуру - до и после

11.10.2017

# 5



Центров  
Обработки данных  
Рига, Латвия

## Инфраструктура центров обработки данных группы Lattelecom

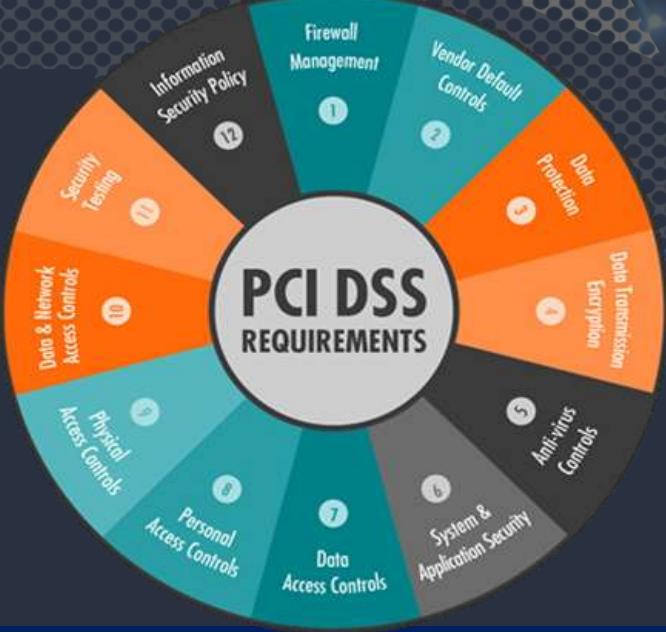
Европейский  
уровень  
безопасности

Сертификаты  
надежности



lattelecom

# PCI DSS Level1



31.07.2017

Hardware  
Infrastructure/ Network  
Physical space (co-location)  
IT Support

01.01.2018

Applications/ software  
Security services  
Systems security services



# Решение по безопасности



radware

Защита от DDoS атак

**RAPID**

Решения по управлению  
уязвимостями ИТ-систем

lattilecom

# Защита от DDoS атак



300 Gbps

Объем Internet трафика



SLA 24/7/1



Radware

lattilecom

# Решения по управлению уязвимостями ИТ-систем



Nexpose

Сканер  
уязвимостей

Appspider

Проверка безопасности  
веб-приложений

Metasploit

Тестирование  
на проникновение

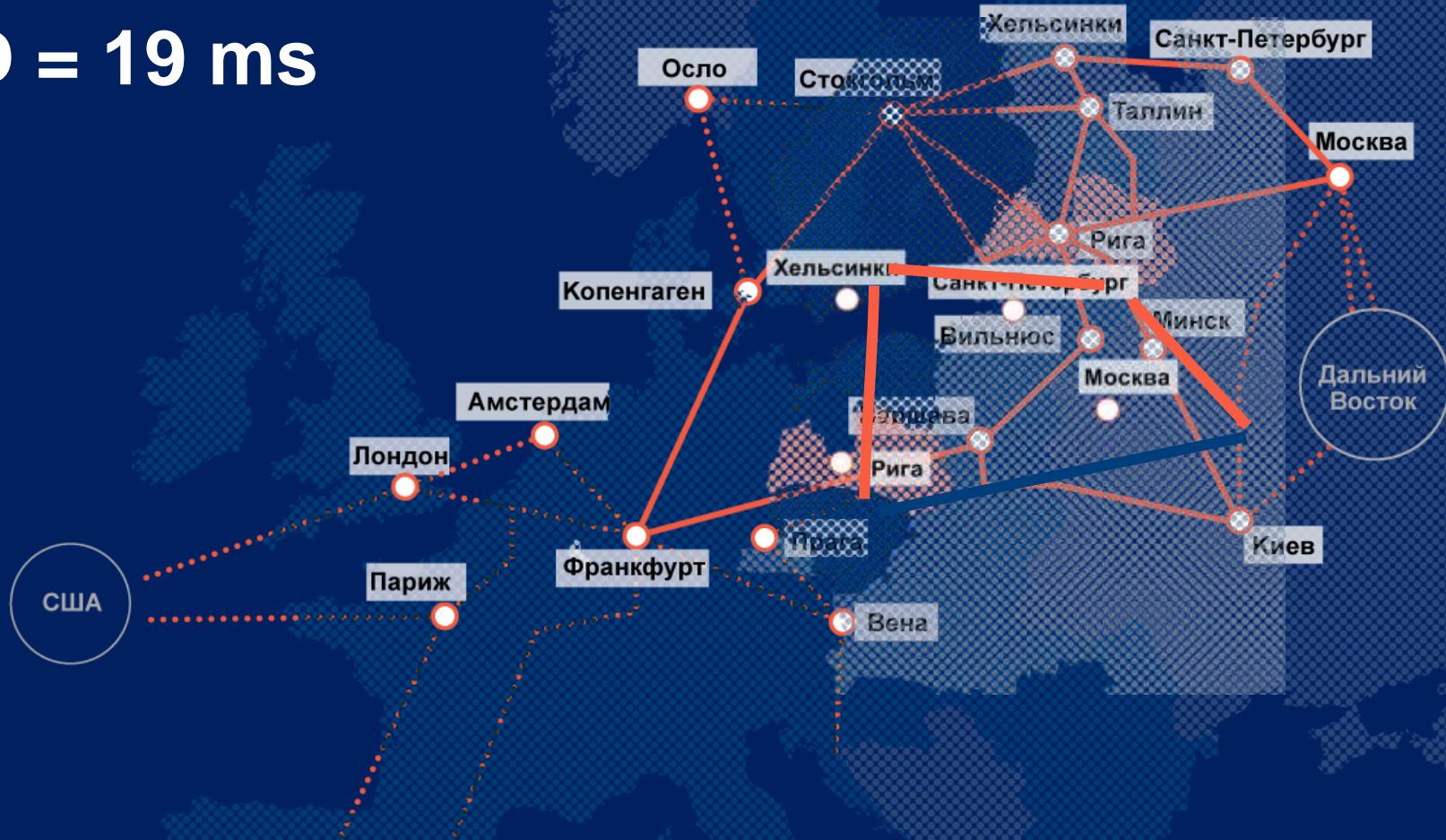
# Сеть передачи данных

9 точек присутствия



# Прямой канал

## RTD = 19 ms



# Опыт развития безопасности Инфраструктуры ЦОД'ов

2013



Первый TIER III  
Сертифицированный  
ЦОД в Северной Европе

2014



Level 2

2015



Защита от  
DDoS атак

2016



Управление  
Уязвимостями  
ИТ-систем

2017 Q2



Level 1

2017 Q3



Операторский  
ЦОД



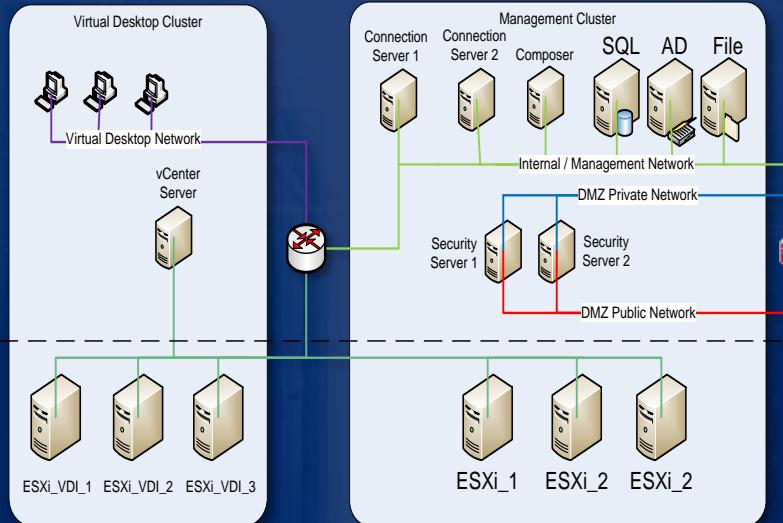
250+  
ОПЫТНЫХ  
ЭКСПЕРТОВ

# Востребованные услуги дата-центров

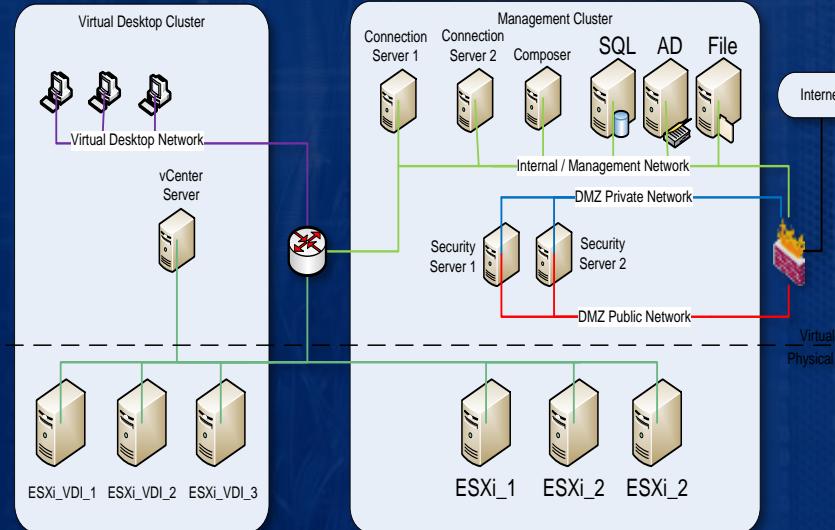




# Техническое решение



Сценарий Но.1



Сценарий Но.2

# День X

27.июня 2017

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

COMPUTER

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMaxXTuR2R1t7BwGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@postco.net](mailto:wowsmith123456@postco.net). Your personal installation key:

a8w0ff-KN4ubE-f2GcKZ-uKZpWJ-Z8mbaU-5tXMH5-z.jxgZF-yXqHPB-K3z46v-eS6qZt

If you already purchased your key, please enter it below.

Key:

# Ситуация после атаки



Все сервера  
зашифрованы



*Backup не полный*



Восстановление требует  
много времени

# Восстановление



3 дня

Восстановление  
критических  
аппликаций



2 недель

Восстановление  
основной  
функциональности



4 недель

Полное  
восстановление

# Как предотвратить подобные ситуации

## Сценарий №.1



DELL/EMC  
DataDomain  
HPE StoreOne

CAPEX  
~200 000 EUR

## Сценарий №.2



Сайт аварийного  
восстановления  
(DRS)

CAPEX  
~120 000 EUR

## Сценарий №.3



Консистентные  
снапшоты

CAPEX  
~10 000 EUR

# Выбор заказчика

Затраты



Восстановление



Несколько  
минут

Интеграция



Легко  
интегрировать и  
администрировать

# Итог

- Изменение мышления
- Компетентность
- Доверие





Спасибо за  
внимание!

