
# Практические аспекты эксплуатации NGFW

Алексей Данилов
Руководитель направления
Отдела развития продуктов ИнфоТеКС


# Мир изменился

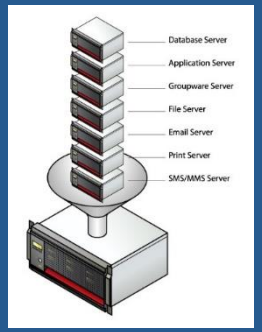
# Мир изменился


Web 2.0

Mobile Devices

Streaming video

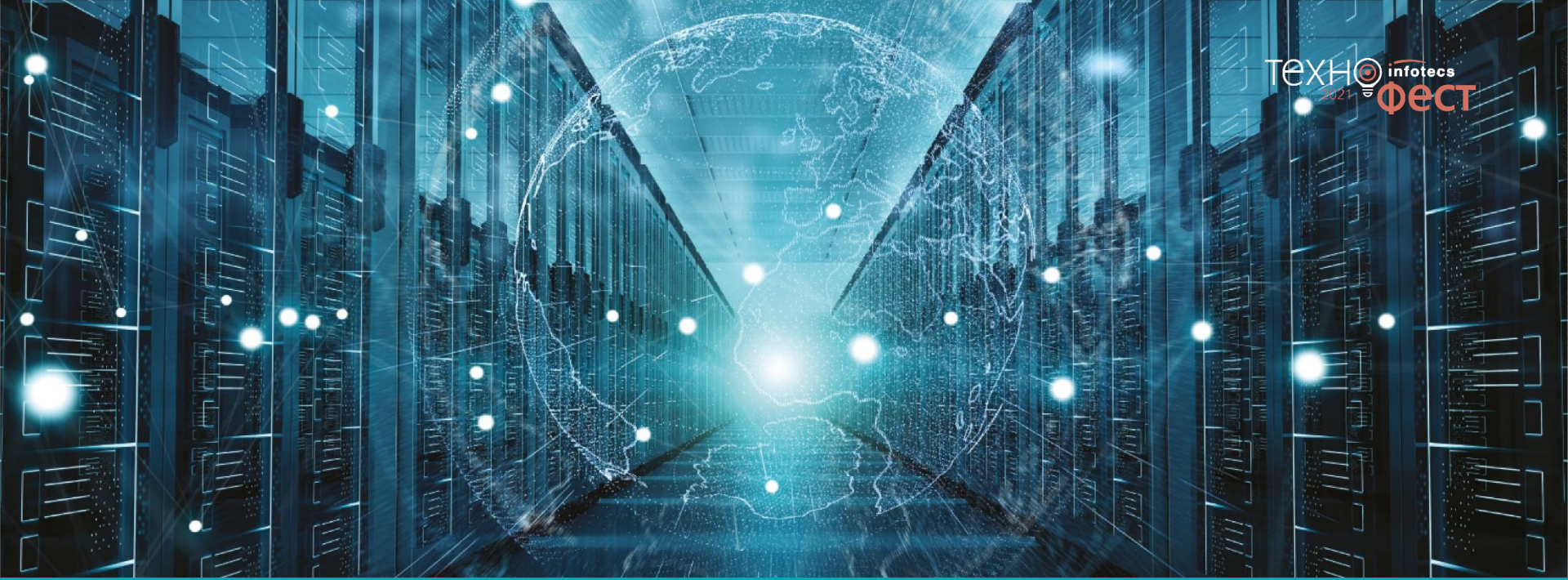
Cloud/SaaS




Virtualization

# Рабочий день сотрудника

- Чтение блогов
- Facebook, VK, Одноклассники
- Twitter
- IM/WhatsApp
- Загрузка файлов (Dropbox, Яндекс.Диск)
- Потоковое видео (YouTube, IVI)
- Потоковое аудио (Яндекс.Музыка)
- Качаем торренты
- Удаленный рабочий стол (TeamViewer, RDP)




# ViPNet xFirewall

# 7 задач

ТЕХНО infotecs 2021 ФЕСТ

Знать, что охранять

Управлять доступом

Защитить от сетевых атак

Реализовать BYOD

Защитить от вирусов

Что делать с SSL

Защита от неизвестных угроз

# ViPNet xFirewall



## Шлюзы безопасности

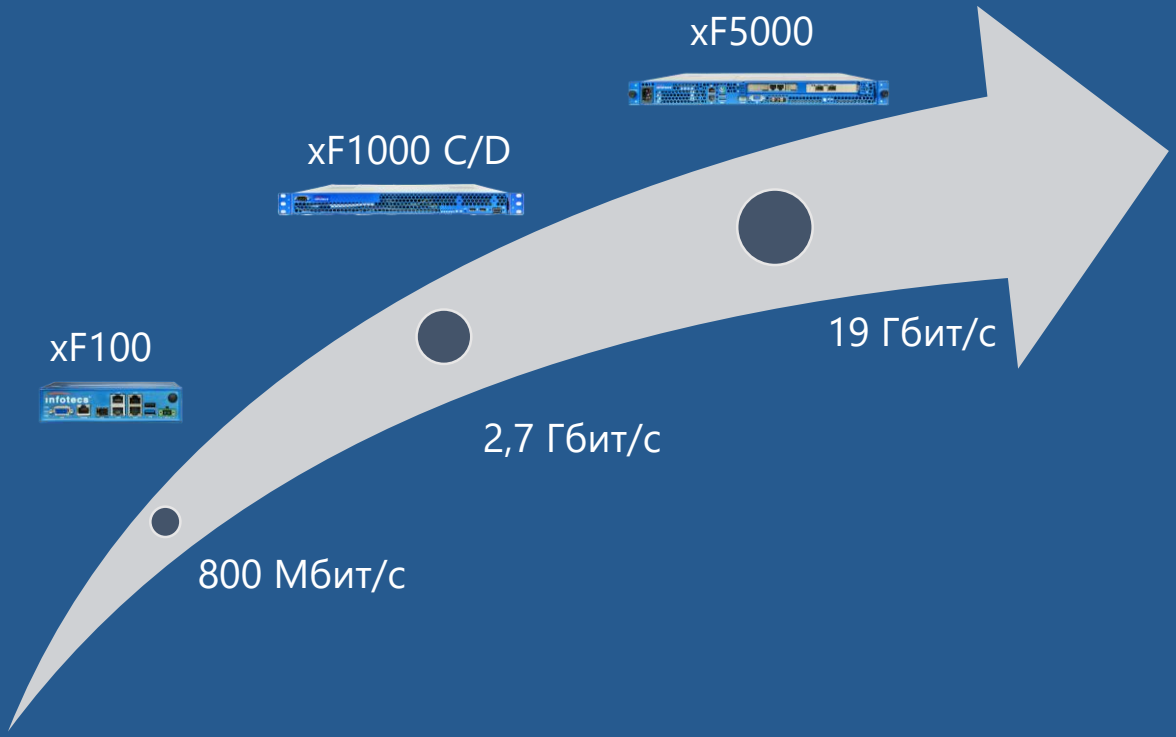
| FW/VPN | | | NGFW | IDS |
|---|---|---|---|---|
| Coordinator for Win/Linux | Coordinator KB | HW 4 поколения | xFirewall | IDS NS |

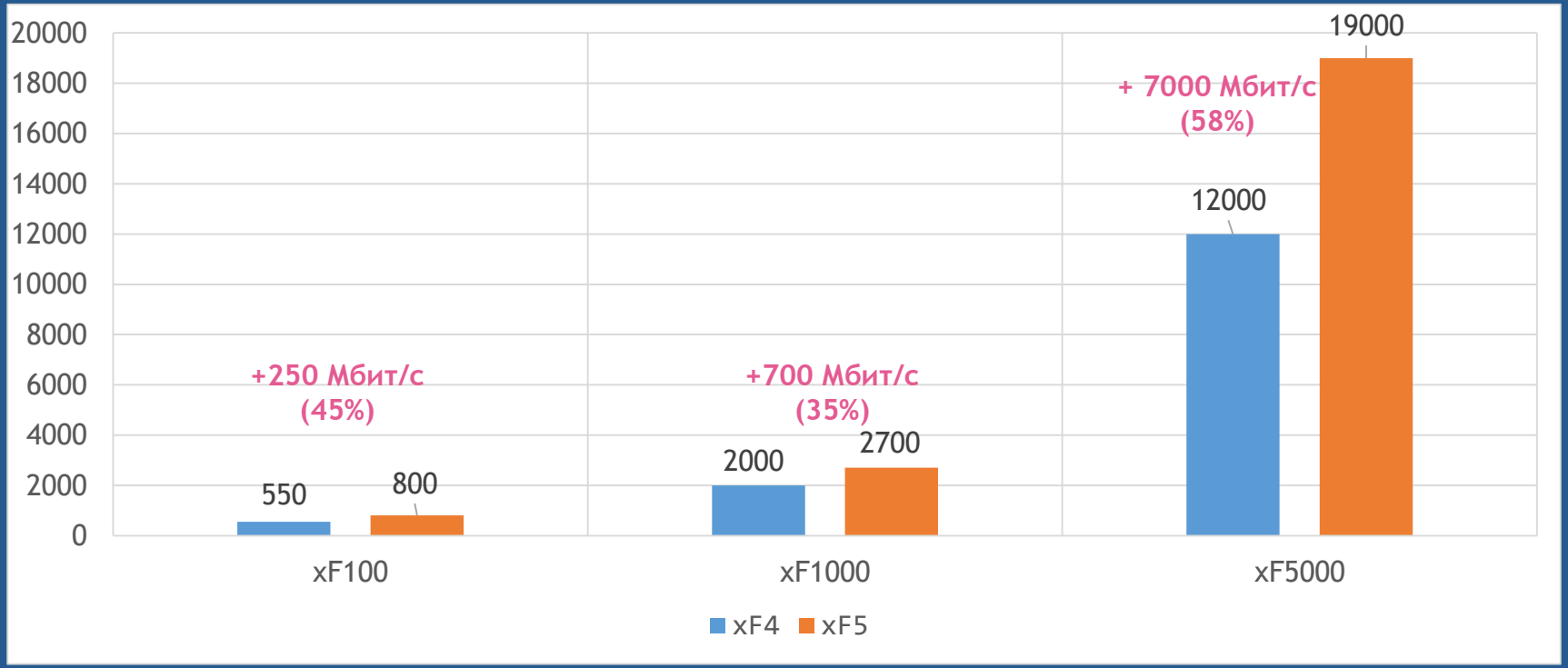
# Что такое ViPNet xFirewall

ТЕХНО infotecs 2021 ФЕСТ

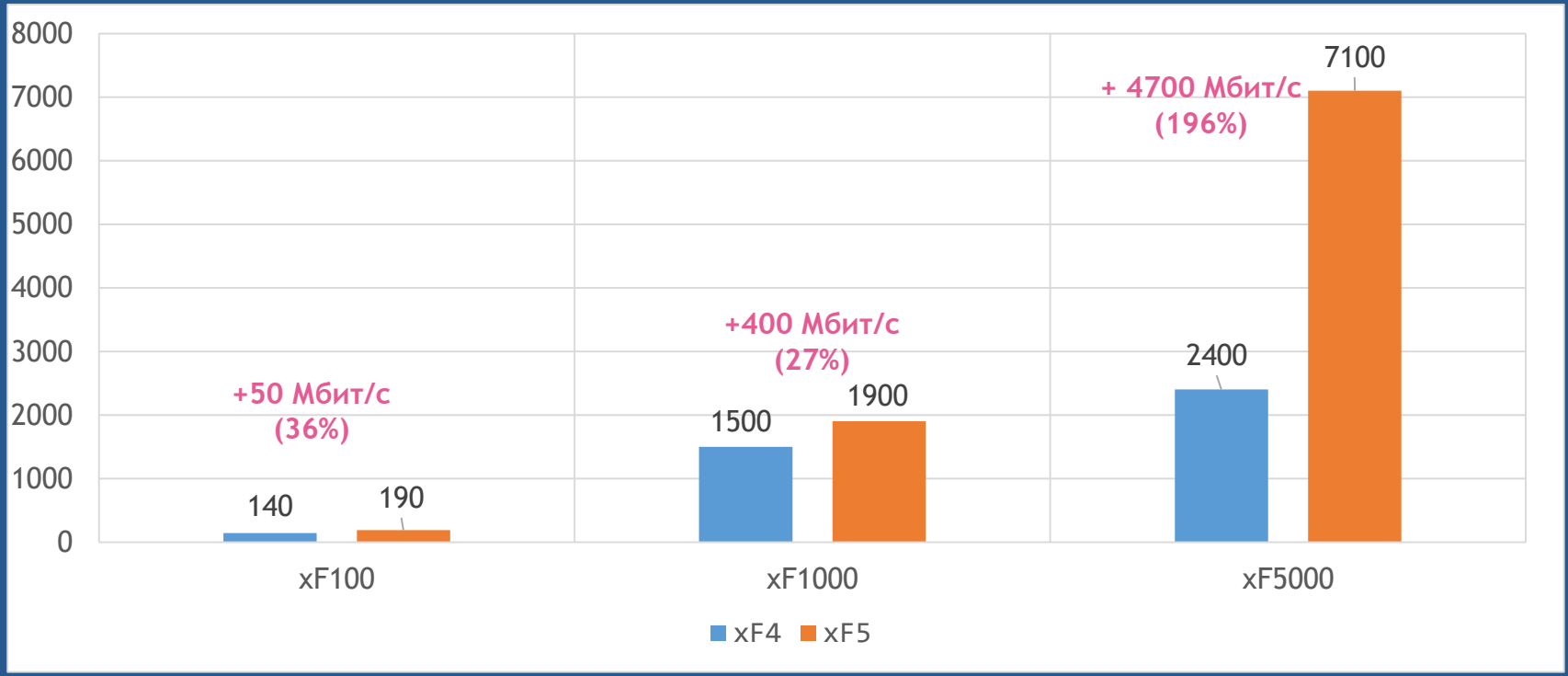
| | | |
|---|---|---|
| Сетевая платформа в составе: | Межсетевой экран | Сетевой экран приложений – DPI |
| Система предотвращения вторжений | Шлюзовой антивирус | Интеграция с Active Directory |

# ViPNet xFirewall. Платформы

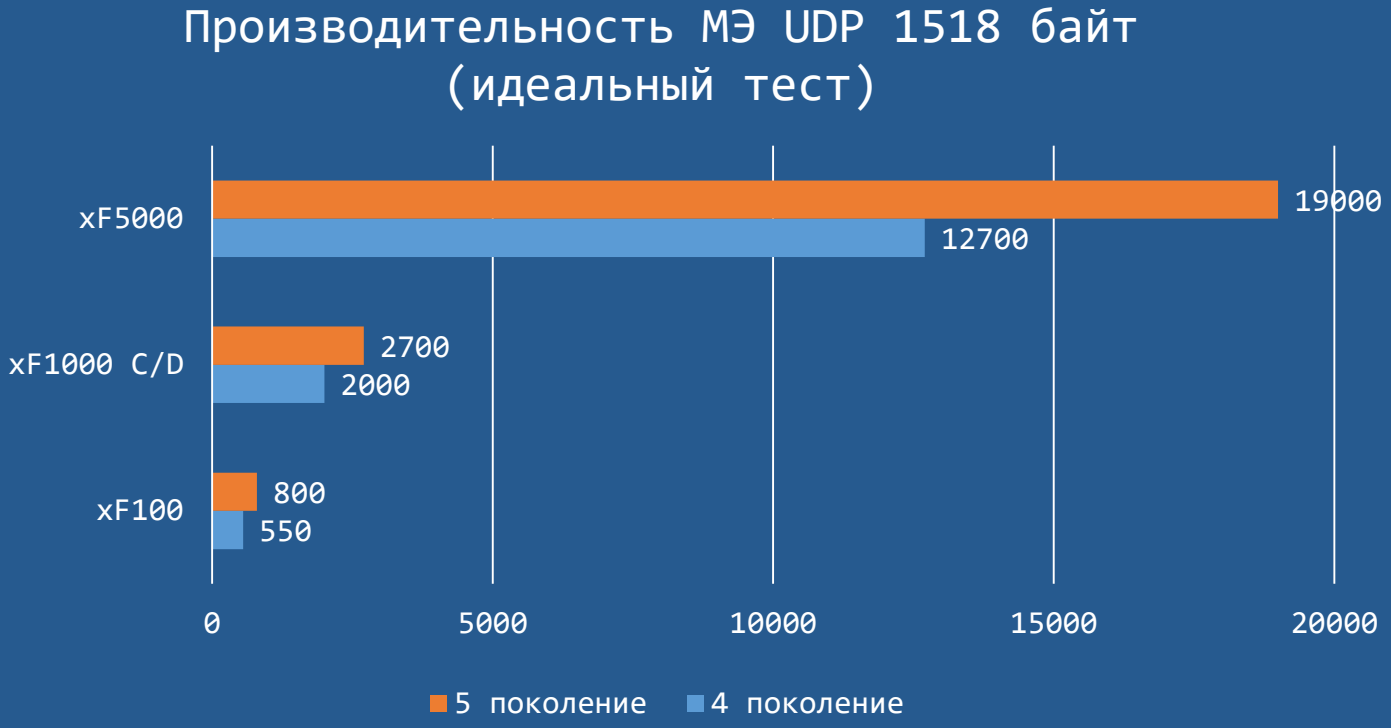



20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
+250 Мбит/с
(45%)
550
800
+700 Мбит/с
(35%)
2000
2700
+ 7000 Мбит/с
(58%)
12000
19000
xF100
xF1000
xF5000
xF4
xF5

# Производительность Application Control



# ViPNet xFirewall 5. Платформы



# Производительность

| Исполнение | xF100 | xF1000 C/D | xF5000 |
|---|---|---|---|
| Firewall, 1518 byte UDP (Mbps) | 800 | 2 700 | 19 000 |
| Firewall, TCP Multistream (Mbps) | 720 | 2 700 | 9 300 |
| AppControl (Firewall+DPI) (Mbps) | 190 | 1 900 | 7 100 |
| Firewall Throughput (64 bytes packets Per Second) | 90 000 | 1 300 000 | 4 000 000 |
| Connections per Second | 2 500 | 20 000 | 50 000 |
| Concurrent Connections | 148 500 | 990 000 | 9 900 000 |
| Users | ~ 100 | ~ 1000 | ~ 6000 |

Max UDP> Max TCP> NGFW

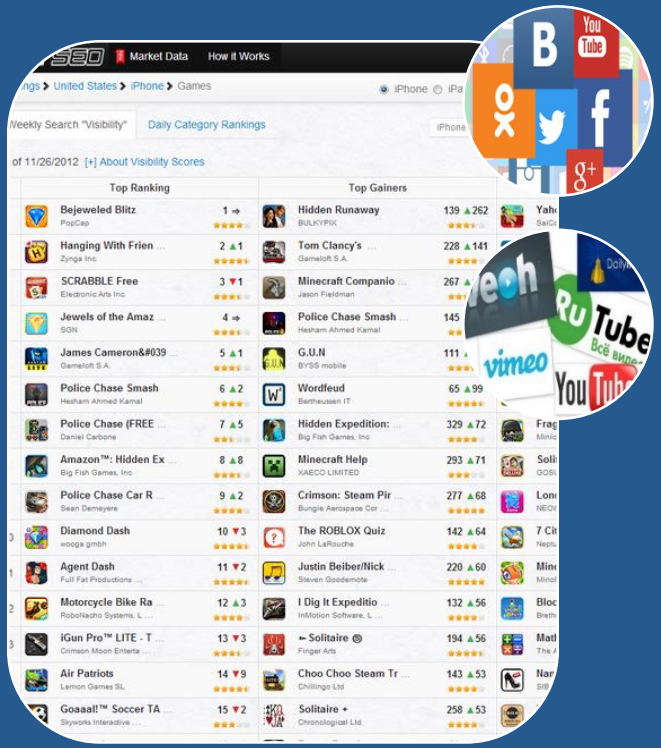
BitTorrent, HTTP, HTTP(s), Oracle DB, SMTP, SSH и др.

7,1 Gb/ 6000 users
= 1,18 Mbps/user


# Знать, что охранять

Открыл порты 80/443 == Открыл

# 2065 уникальных приложений/протоколов




95 из категории «Социальные сети»

45 – потоковое видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

# Управлять доступом

# Интеграция с Microsoft AD

## Бесклиентская идентификация

- xFirewall использует технологическую учетную запись MS AD с ее помощью производится чтение EventLog
- Синхронизация с MS AD каждые 5 секунд
- Допустимое время отсутствия связи 1800 секунд

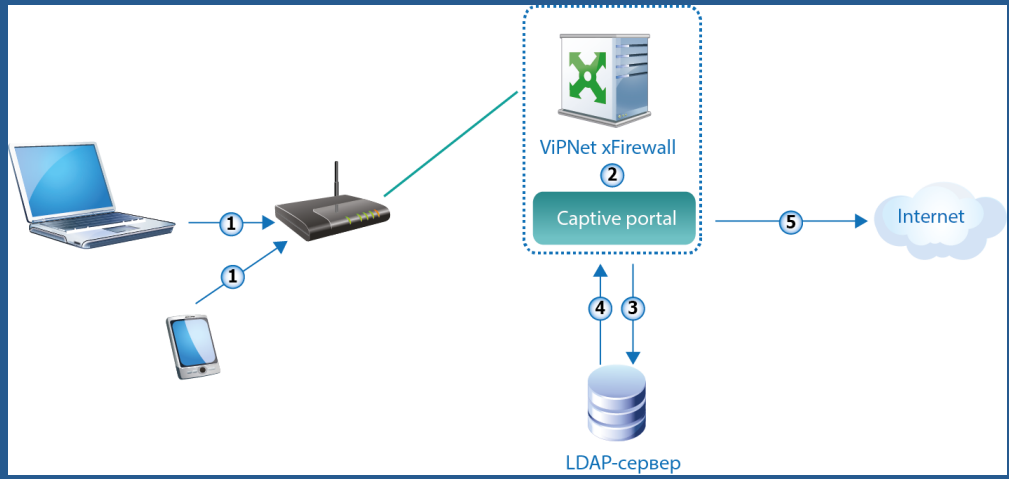
## Использование учетных записей пользователей MS AD в правилах фильтрации

- Отсутствует потребность в «привязке» пользователей к ip-адресам
- Отсутствует потребность в «привязке» пользователей к устройствам

# BYOD – принеси свое устройство и работай

# Captive portal – аутентификация с помощью браузера

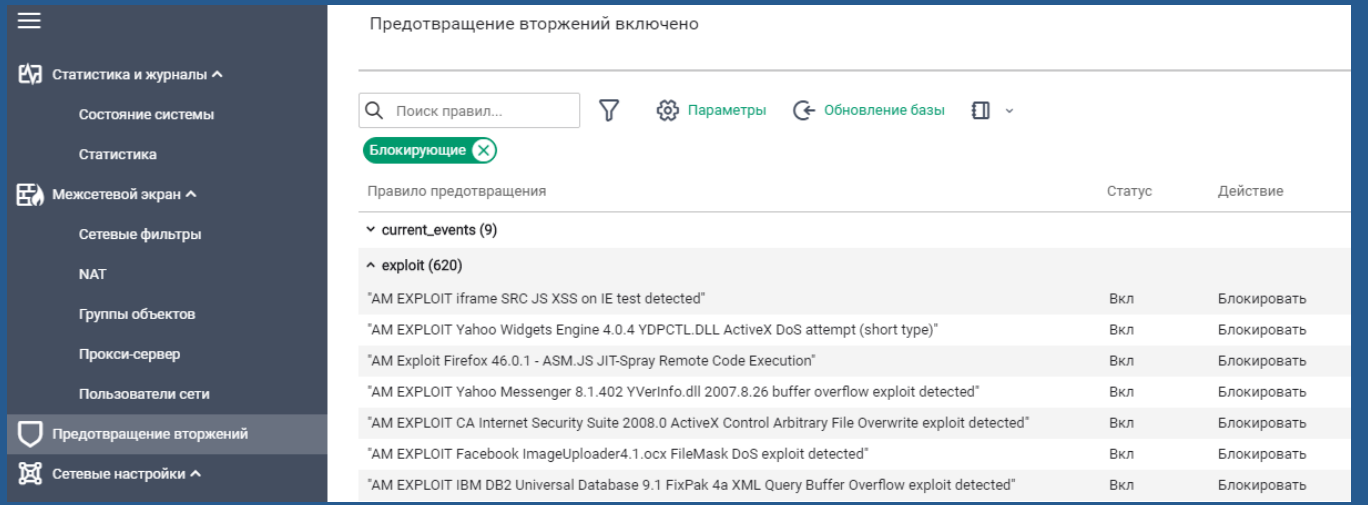
- Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства
- Предоставление контролируемого доступа подрядчикам, партнерам
- Автоматическое перенаправление на Портал аутентификации – Captive Portal

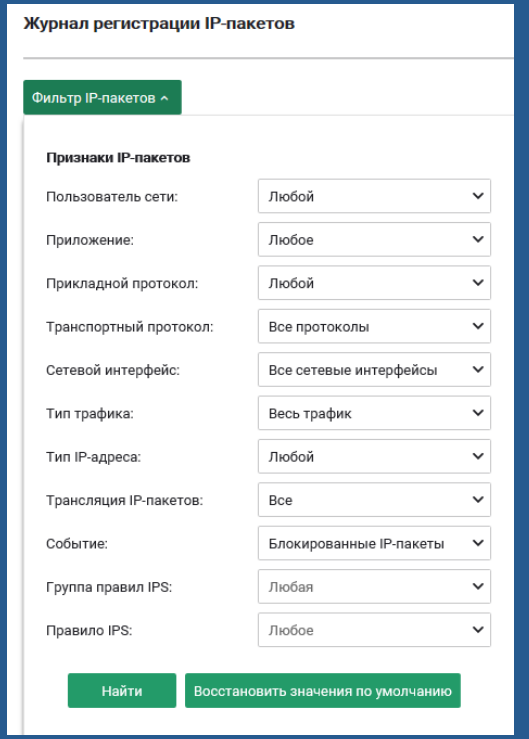



**Для таких пользователей можно создать политику с ограниченным доступом к ресурсам компании, потому что их устройства могут быть без средств защиты.**

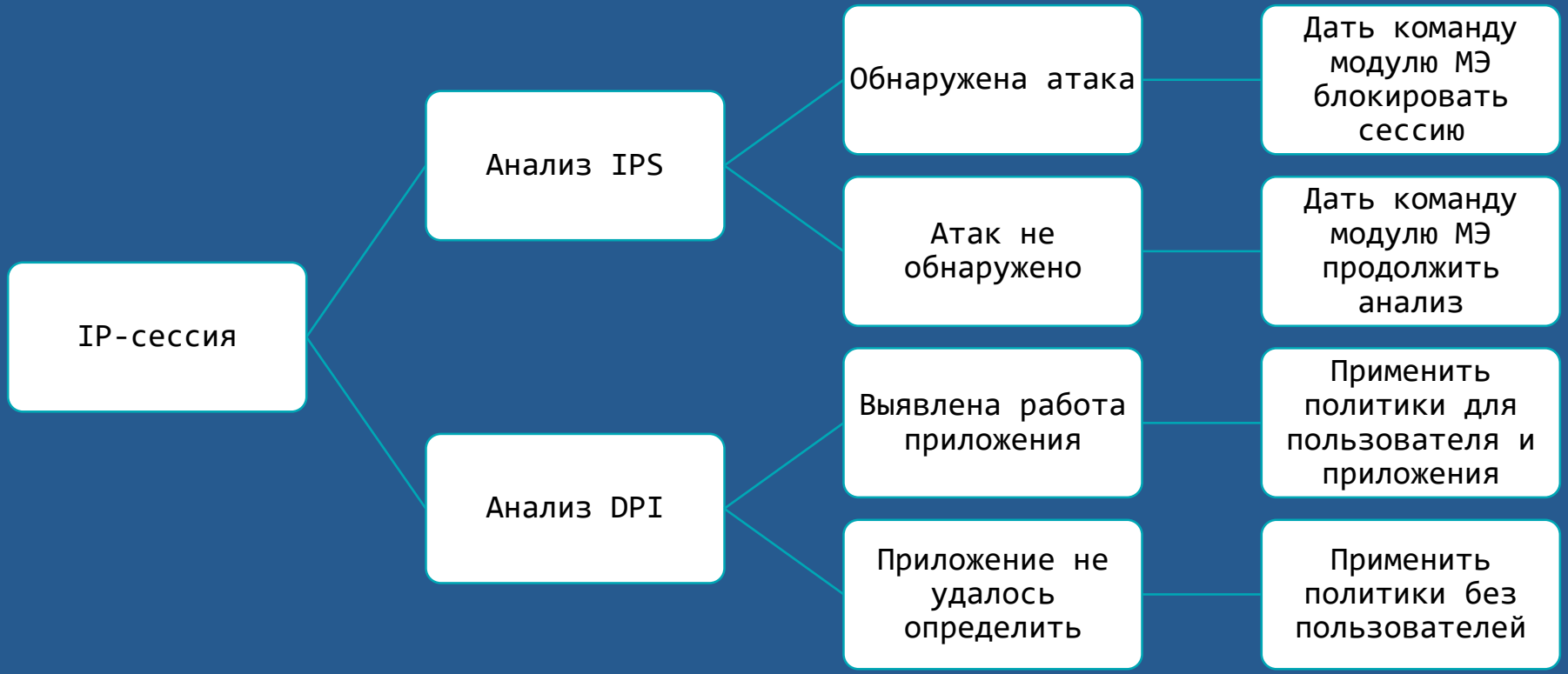
# Защита от сетевых атак

# Система предотвращения вторжений



# Порядок применения правил IPS



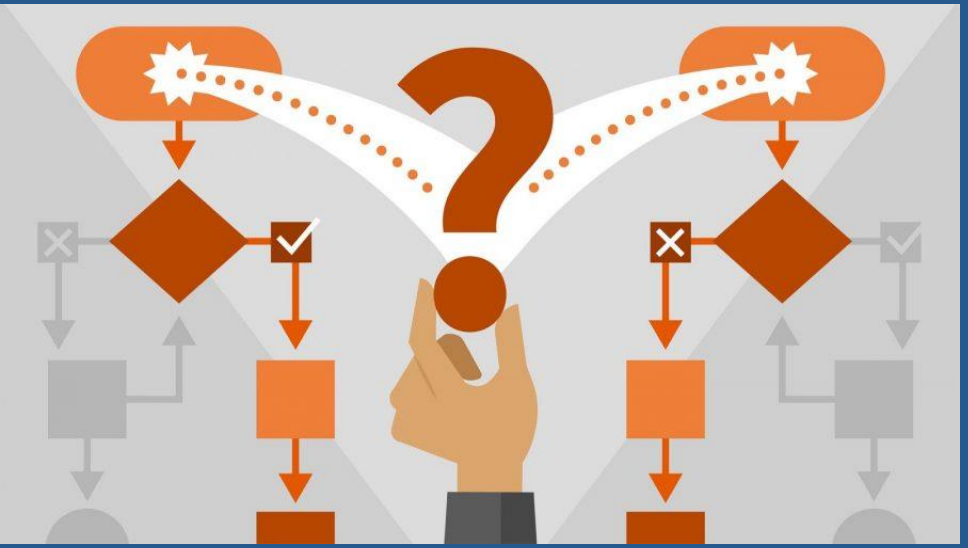
# Защита от вирусов

# Поддержка песочниц

- Тестировался сценарий проверки на содержание вредоносного контента файлов, загружаемых из сети Интернет в «песочницу» ATHENA через службу прокси-сервера xFirewall по протоколу ICAP.
- Межсетевой экран ViPNet xFirewall служит шлюзом между приложениями, функционирующими на узлах локальной сети, и внешними сетевыми ресурсами, к которым эти приложения обращаются (выполняет функции прокси-сервера).
- Система AVSOFT ATHENA работает на основе комбинации технологий мультисканера и «песочницы» для исследования файлов на подозрительное содержимое и поведение существенно повышает точность результата проверки.

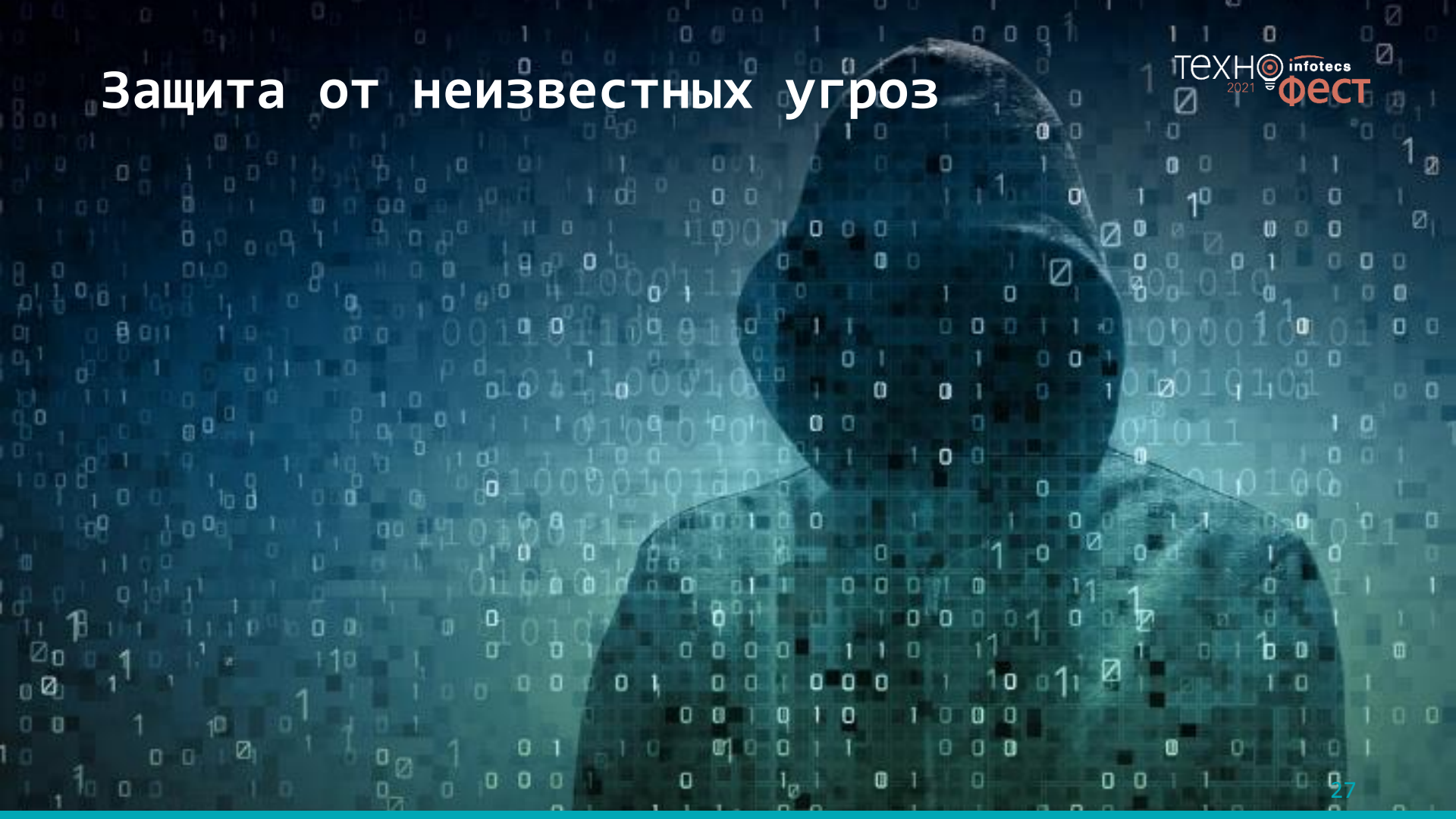
# Что делать с SSL

# Классификация SSL



- Разрешить тот SSL трафик, который известен:
  - Yandex, Google, Facebook и т.д.
- Блокировать известный SSL запрещенных политикой приложений: социальные сети, мессенджеры и т.д.
- Запретить любой неизвестный SSL трафик.

# Защита от неизвестных угроз



# ViPNet xFirewall повышает осведомленность

Максимальная видимость – фильтрация на 7 уровне ISO OSI

Защита от сетевых атак – блокировка аномалий, запретных команд

Защита от вирусных атак

Уменьшение поверхности атаки

ТЕХНО infotecs 2021 Фест

# Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow