

# ViPNet xFirewall – многогранная защита периметра

Алексей Данилов  
Руководитель направления  
Отдел развития продуктов ИнфоТеКС

The logo for infotecs, featuring a stylized orange and red arc above the word "infotecs" in a bold, dark blue sans-serif font.

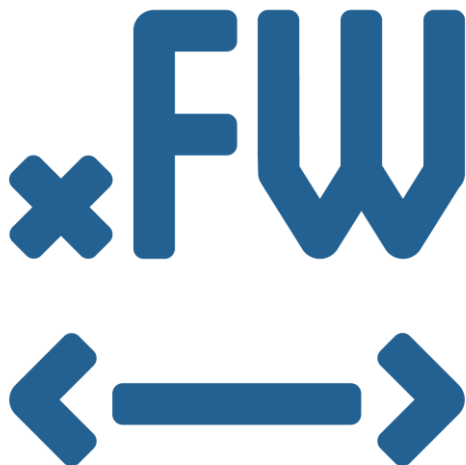


# ViPNet xFirewall

# Сертификат ФСТЭК



- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020)» – по 4 уровню доверия
- «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016)
- «Профиль защиты межсетевых экранов типа Б четвертого класса защиты ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016)
- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011)
- «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012)



2.3.1 ViPNet xFirewall 5 ... предназначен для использования в государственных информационных системах до класса защищенности К1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными и технологическими процессами до класса защищенности К1 включительно, в ИС персональных данных для обеспечения уровня защищенности персональных данных до 1 уровня включительно, в ИС общего пользования II класса.

2.3.2 ViPNet xFirewall 5 может использоваться в указанных выше системах в том числе с целью выполнения базовых и адаптированных мер защиты информации в соответствии с требованиями, утвержденными приказами ФСТЭК России №17 от 11.02.2013, №31 от 14.03.2014, №21 от 18.02.2013 и №489 от 31.08.2010.

2.3.3 Также ViPNet xFirewall 5 может использоваться в автоматизированных системах управления, ИС и информационно-телекоммуникационных сетях, которые отнесены к значимым объектам критической информационной инфраструктуры (далее – КИИ) до категории значимости К1 в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ.

# Next-generation Firewall

# Next-generation Firewall (NGFW)

Gartner®



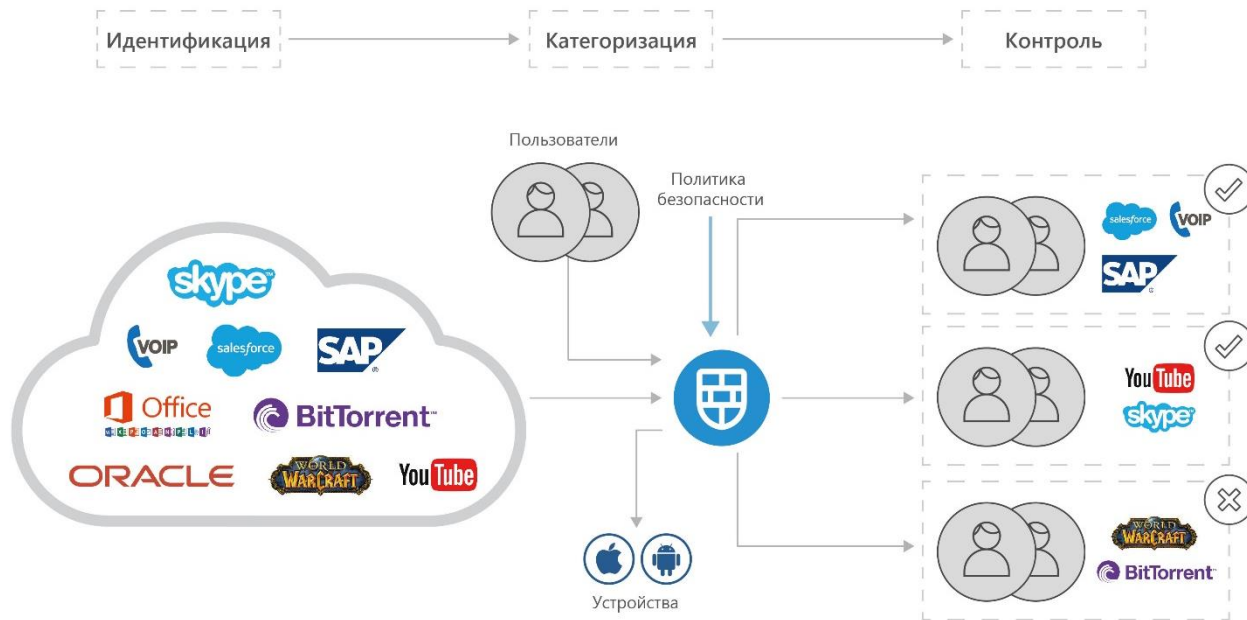
- Общепринято МЭ считать устройствами, реализующими технологию stateful packet inspection (SPI) сетевого трафика. МЭ разграничивает доступ на основе 5 параметров: адреса отправителя и получателя, порты отправителя и получателя, протокол L4.

МЭ следующего поколения (NGFW) в дополнении к общепринятому разграничению доступа предоставляет возможности по выявлению и блокировке современных угроз, таких как: вредоносное ПО, атаки уровня приложений. Согласно определению Gartner NGFW должен состоять из:

- Стандартного МЭ SPI
- Встроенной системы предотвращения атак IPS
- Системы контроля приложений
- Extrafirewall intelligence

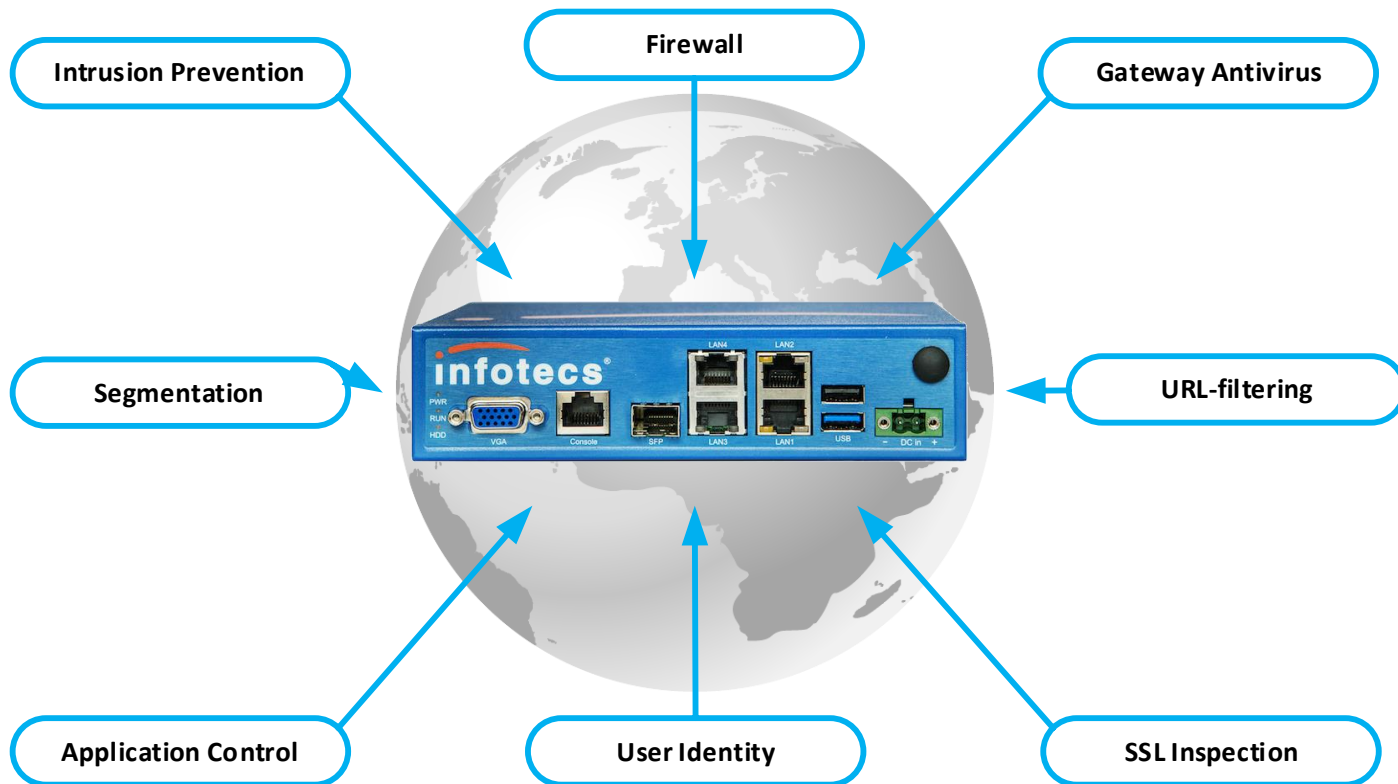
# ViPNet xFirewall

# VIPNet xFirewall с первого взгляда





# Что такое ViPNet xFirewall



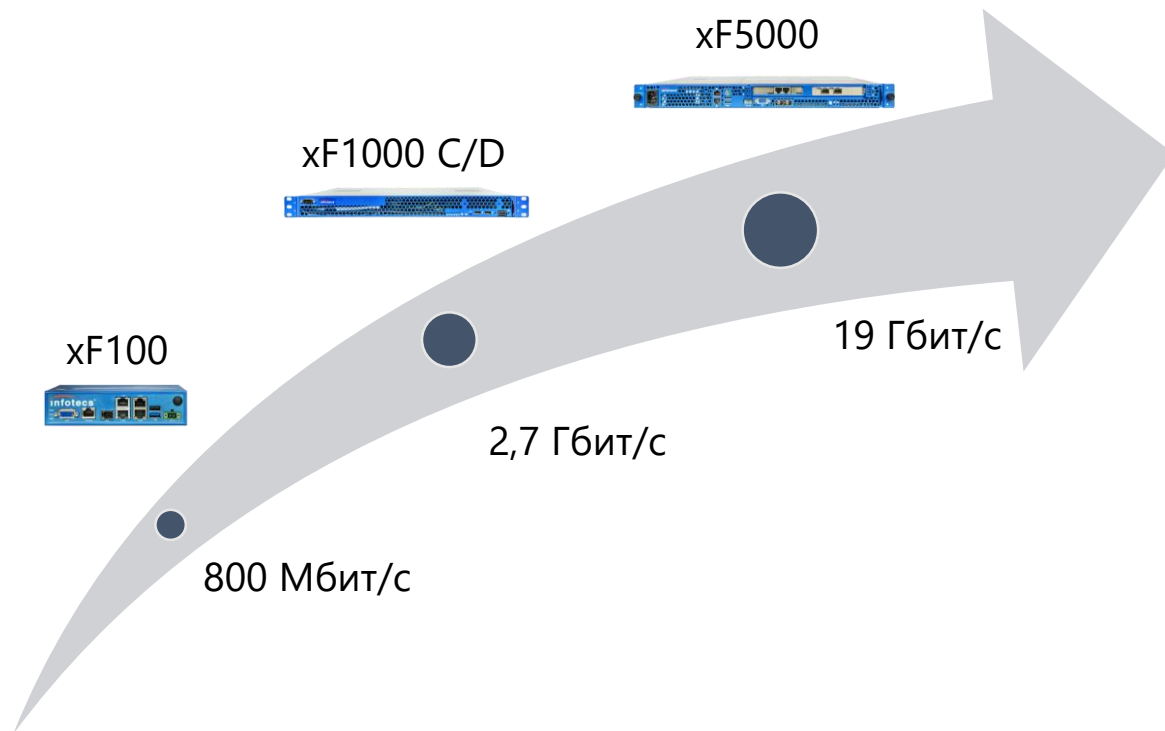
# Что нового в 5-м поколении продукта

- Система предотвращения вторжений IPS:
  - Реализована система предотвращения вторжений – IPS
  - Реализовано взаимодействие с ViPNet TIAS
  - Расширены базы решающих правил
  - Обновление базы правил IPS через прокси сервер
  - Добавлена возможность перехода к описанию правила IPS, соответствующего событию, зарегистрированному в журнале IP-пакетов.
- Улучшения МСЭ
  - Блокировка доступа к поддоменам DNS
  - Protection Tools – автоматическая блокировка источников повышенной нагрузки
  - Работа с несколькими контроллерами доменов MS AD
- Новый web-UI

# Что нового в 5-м поколении продукта

- **Расширение возможностей failover**
  - Поддержка dhcp-relay
  - Поддержка DHCP-сервера
- **Улучшение возможностей мониторинга**
  - Экспорт журнала пакетов в формате CEF по syslog
  - Информация о сработавших правилах в журнале IP-пакетов
  - Управление уровнем важности событий, регистрируемых в системном журнале
  - Поддержка SNMPv3
  - Мониторинг пассивного узла кластера по протоколу SNMP
  - Поддержка протокола Netflow v9
- **Поддержка новых аппаратных платформ из TOPP**
- **SSL Inspection**

# VIPNet xFirewall. Платформы



# Повышена производительность

В зависимости от типа платформы и типа теста производительность повышена на 35-58%



# Application Control – контроль приложений



Открыл порты 80/443 == Открыл всё!

# Более 5000 приложений/протоколов

Top Ranking		Top Gainers	
Bejeweled Blitz	1 →	Hidden Runaway	139 ▲
Hanging With Friends	2 ▲1	Tom Clancy's	228 ▲141
SCRABBLE Free	3 ▼1	Minecraft Companio	267 ▲134
Jewels of the Amaz	4 →	Police Chase Smash	145 ▲134
James Cameron's	5 ▲1	G.U.N	111 ▲
Police Chase Smash	6 ▲2	Wordfeud	65
Police Chase (FREE	7 ▲5	Hidden Expedition: ...	329 ▲
Amazon™ Hidden Ex	8 ▲8	Minecraft Help	293 ▲71
Police Chase Car R	9 ▲2	Crimson: Steam Pir	277 ▲68
Diamond Dash	10 ▼3	The ROBLOX Quiz	142 ▲64
Agent Dash	11 ▼2	Justin Bieber/Nick	220 ▲60
Motorcycle Bike Ra	12 ▲3	iDig It Expeditio	132 ▲56
iGun Pro™ LITE - T	13 ▼3	— Solitaire	194 ▲56
Air Patriots	14 ▼9	Choo Choo Steam Tr	143 ▲53
Goaaa!™ Soccer TA	15 ▼2	Solitaire +	258 ▲53

65 из категории  
«Социальные сети»

183 – потоковое  
видеовещание

- Palo Alto Networks – 3625 приложений
- Cisco – 3701 приложений

# User Identity – идентификация пользователей





# Интеграция с Microsoft AD

## Без клиентская 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

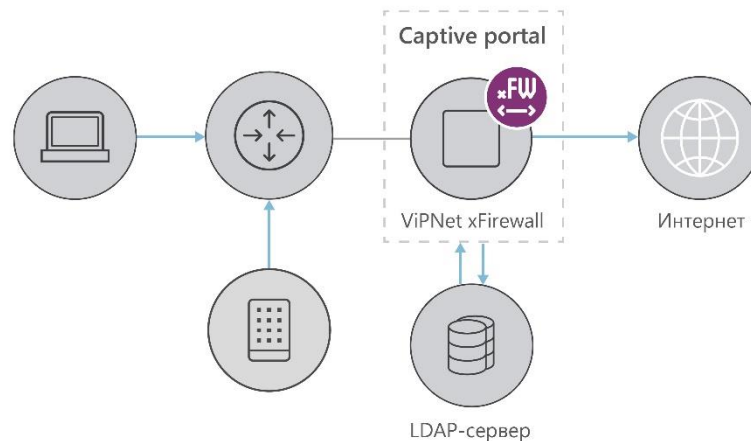




**BYOD –  
принеси свое  
устройство  
и работай**

# 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.

# Intrusion Prevention - COB



# Система предотвращения вторжений

Предотвращение вторжений включено

Поиск правил... Параметры Обновление базы ▾

**Блокирующие**

Правило предотвращения	Статус	Действие
▼ current_events (9)		
^ exploit (620)		
*AM EXPLOIT Iframe SRC JS XSS on IE test detected*	Вкл	Блокировать
*AM EXPLOIT Yahoo Widgets Engine 4.0.4 YDPCTL.DLL ActiveX DoS attempt (short type)*	Вкл	Блокировать
*AM Exploit Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution*	Вкл	Блокировать
*AM EXPLOIT Yahoo Messenger 8.1.402.YVerInfo.dll 2007.8.26 buffer overflow exploit detected*	Вкл	Блокировать
*AM EXPLOIT CA Internet Security Suite 2008.0 ActiveX Control Arbitrary File Overwrite exploit detected*	Вкл	Блокировать
*AM EXPLOIT Facebook ImageUploader4.1.ocx FileMask DoS exploit detected*	Вкл	Блокировать
*AM EXPLOIT IBM DB2 Universal Database 9.1 FixPak 4a XML Query Buffer Overflow exploit detected*	Вкл	Блокировать

### Журнал регистрации IP-пакетов

Фильтр IP-пакетов ^

**Признаки IP-пакетов**

Пользователь сети:

Приложение:

Прикладной протокол:

Транспортный протокол:

Сетевой интерфейс:

Тип трафика:

Тип IP-адреса:

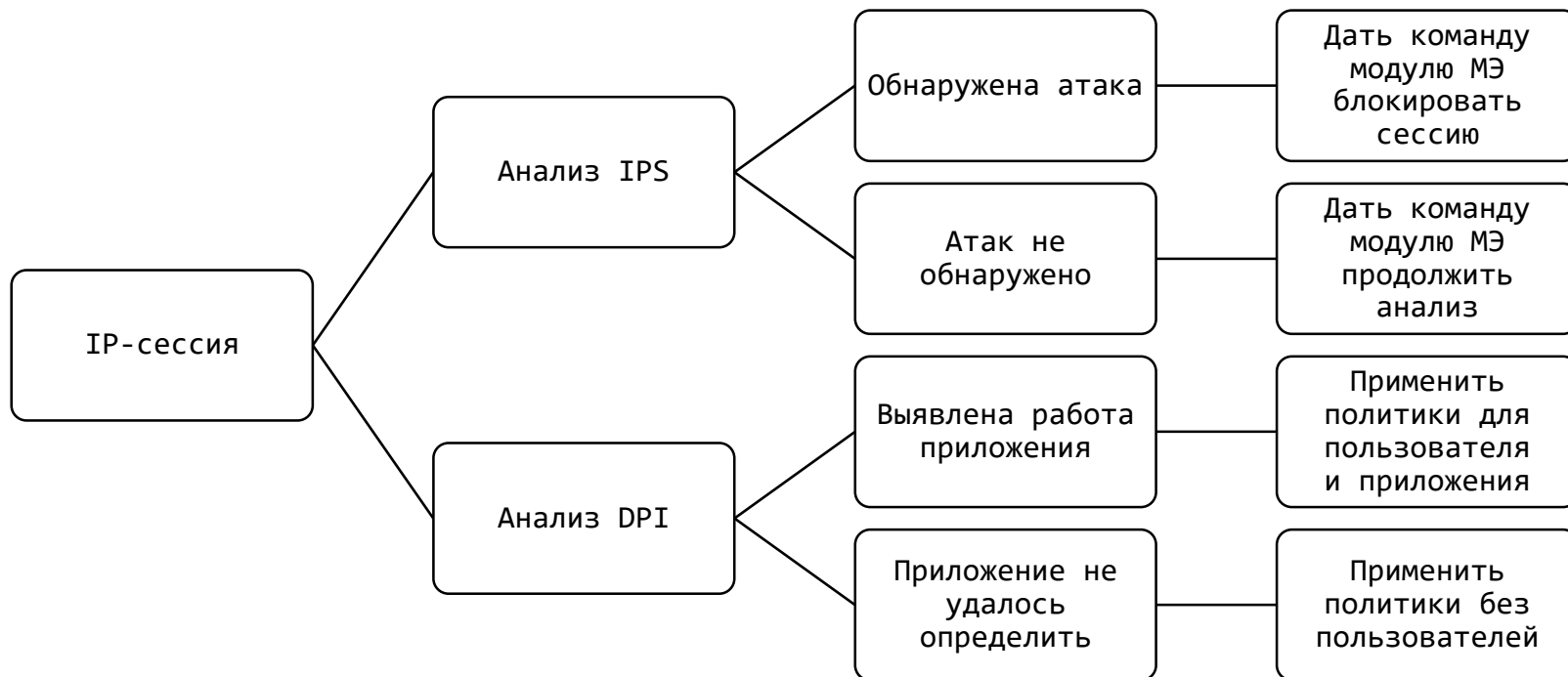
Трансляция IP-пакетов:

Событие:

Группа правил IPS:

Правило IPS:

# Порядок применения правил IPS

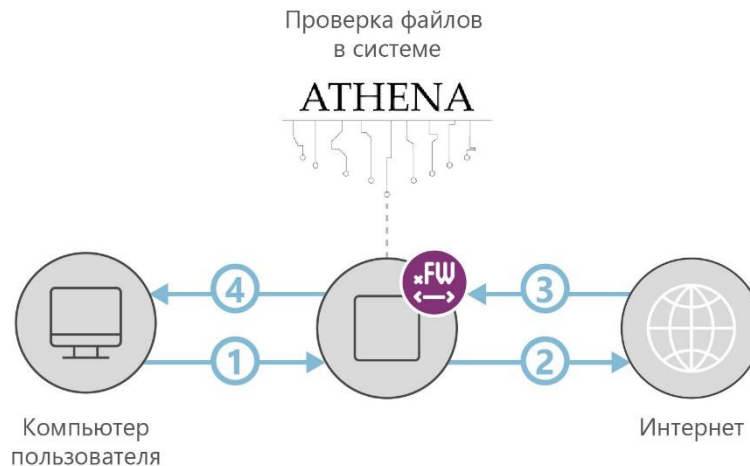


# Gateway Antivirus – шлюзовой антивирус



# 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





# SSL Inspection – анализ SSL

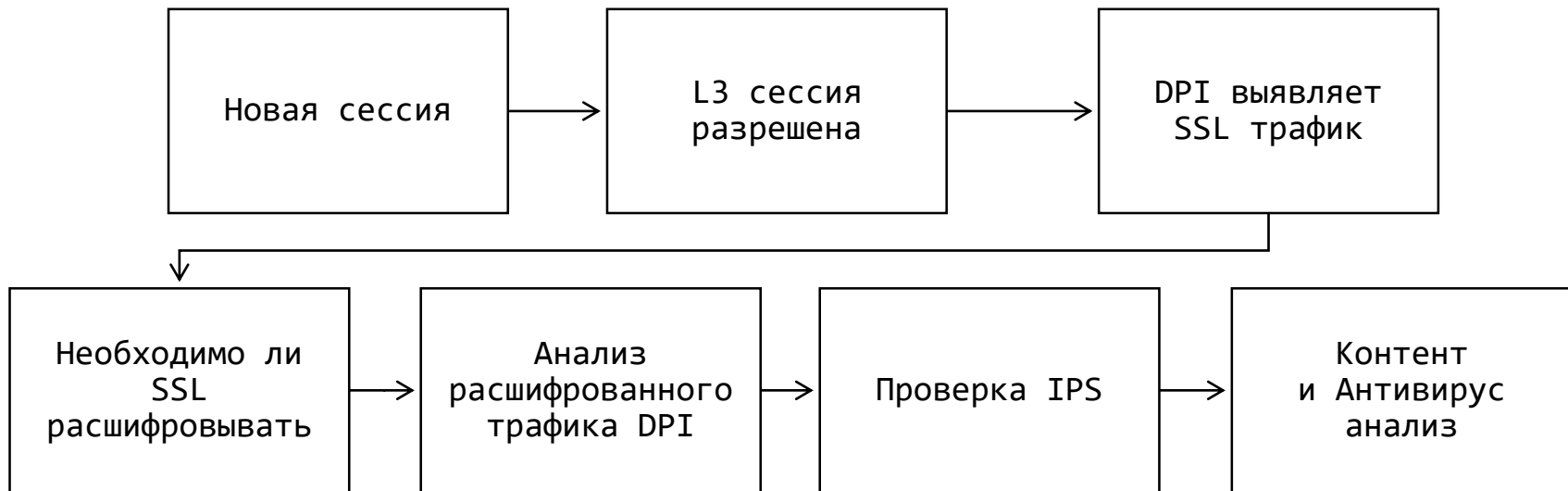


# Классификация SSL

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



# Схема проверки трафика



# Forward proxy decryption

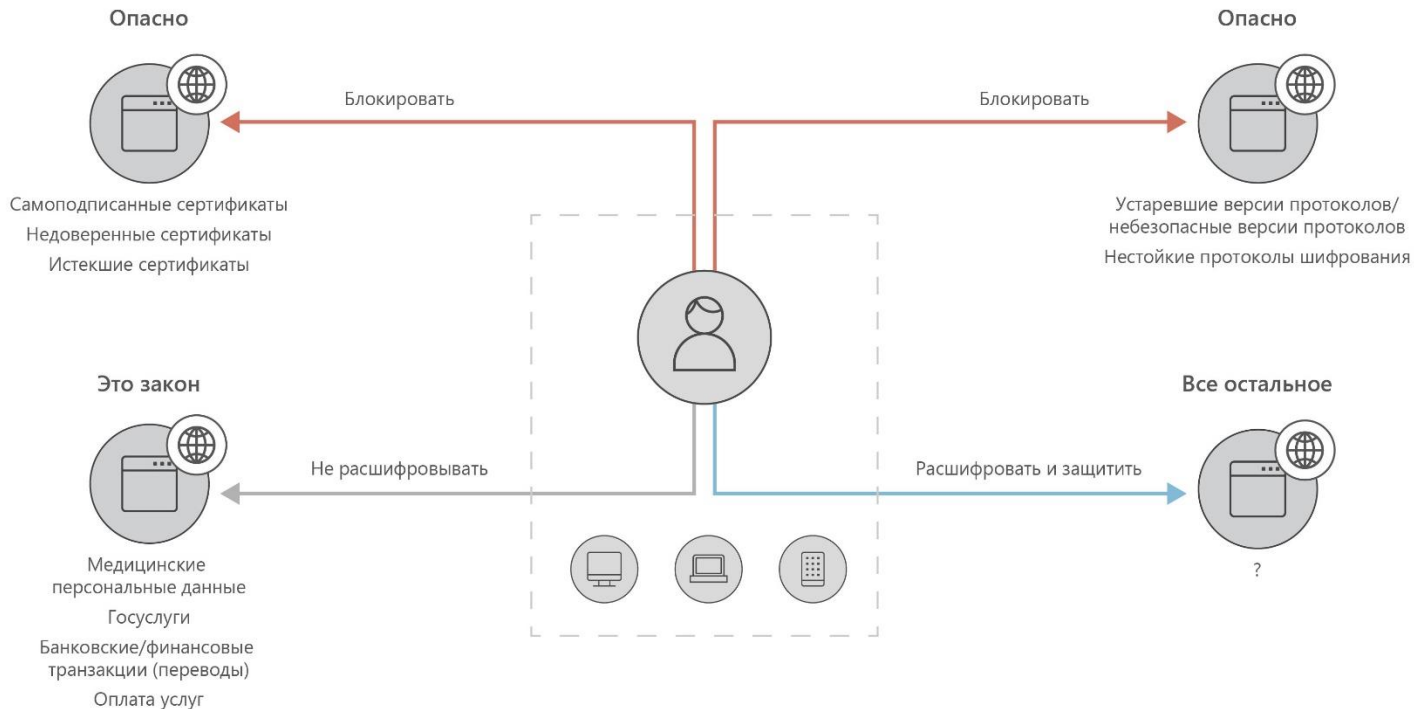
## Корневой сертификат МСЭ (Firewall)



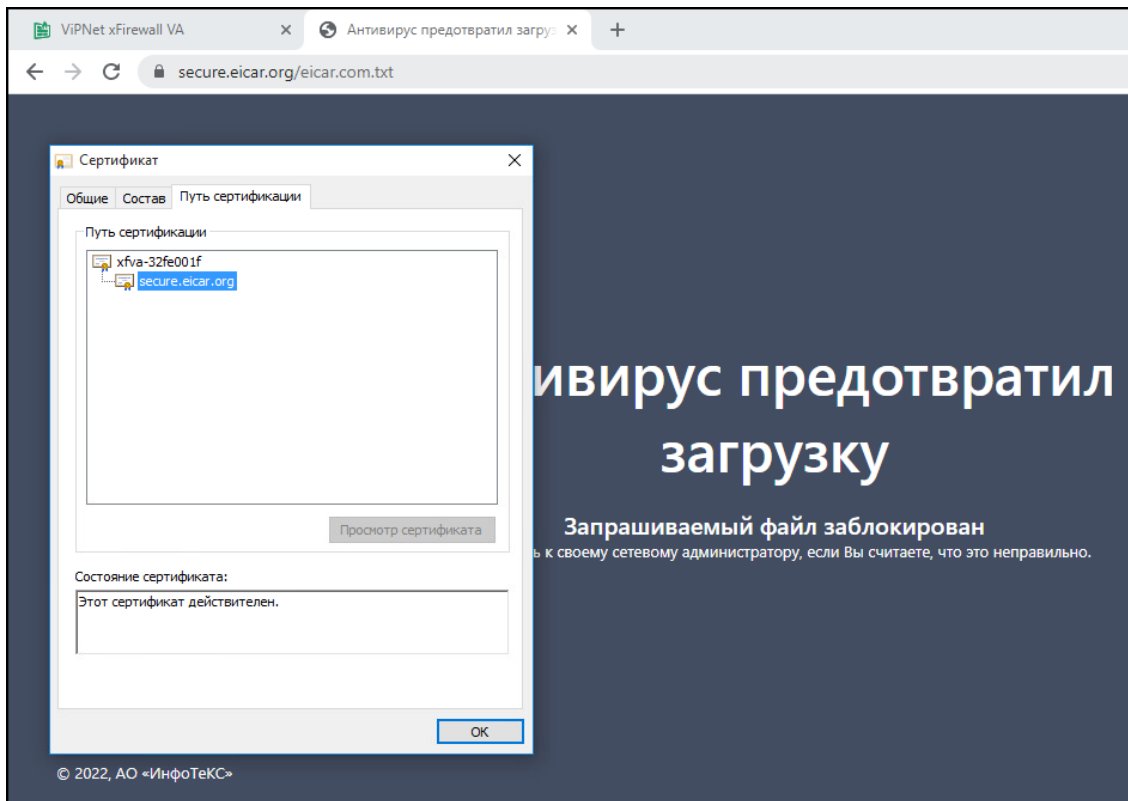
## Клиент подтверждает корневой сертификат МСЭ



# Лучшие практики SSL Inspection



# Результат



The screenshot shows a web browser window with the address bar displaying `secure.eicar.org/eicar.com.txt`. A certificate dialog box titled "Сертификат" is open, showing the "Путь сертификации" (Certification Path) with the following entries:

- xfva-32fe001f
- secure.eicar.org

Below the path, there is a "Просмотр сертификата" (View Certificate) button. The "Состояние сертификата:" (Certificate Status) section contains the text: "Этот сертификат действителен." (This certificate is valid.).

Overlaid on the browser window is a large dark blue message box with the following text:

**Антивирус предотвратил загрузку**

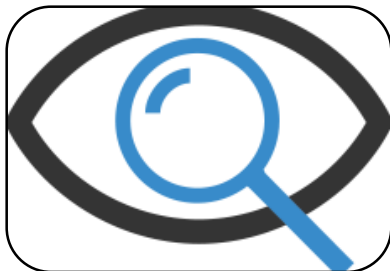
**Запрашиваемый файл заблокирован**

Обратитесь к своему сетевому администратору, если Вы считаете, что это неправильно.

At the bottom left of the screenshot, there is a copyright notice: © 2022, АО «ИнфоТекС»

# Защита от неизвестных угроз

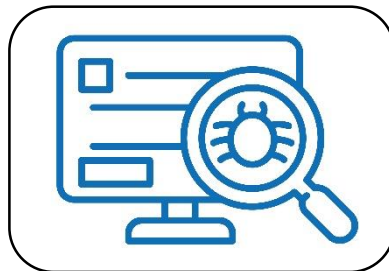
# ViPNet xFirewall - повышает осведомленность



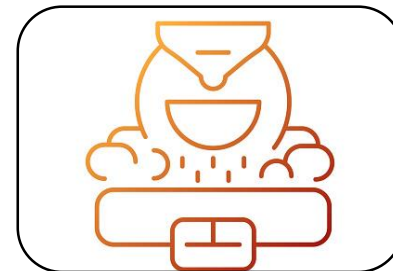
Максимальная  
видимость -  
фильтрация на 7  
уровне ISO OSI



Защита от сетевых  
атак - блокировка  
аномалий, запретных  
команд



Защита от вирусных  
атак



Уменьшение  
поверхности атаки



ТЕХНО infotecs  
2022 ФЕСТ

Спасибо за внимание!

Информационный  
партнер



---

Подписывайтесь на наши соцсети



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



[t.me/infotecs\\_news](https://t.me/infotecs_news)



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