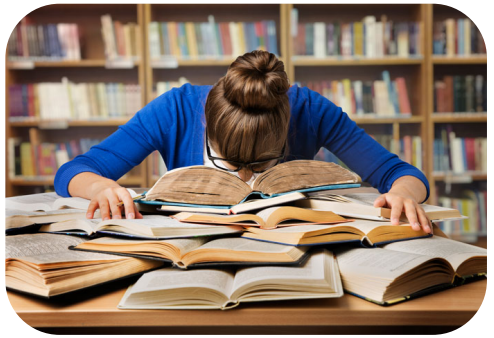
Сетевая безопасность следующего поколения

APT – целенаправленная атака

Целевая кибератака

Продолжительность

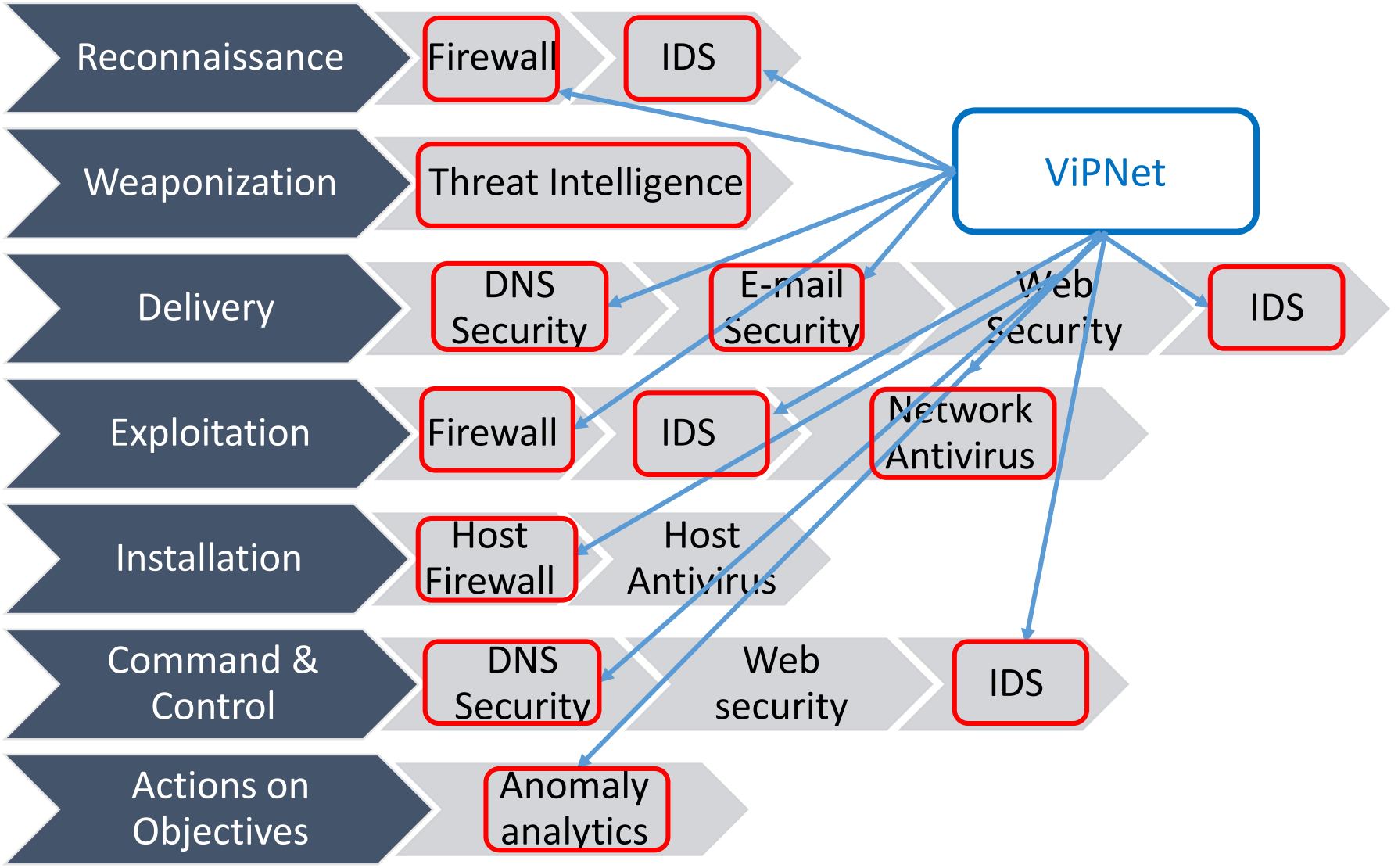


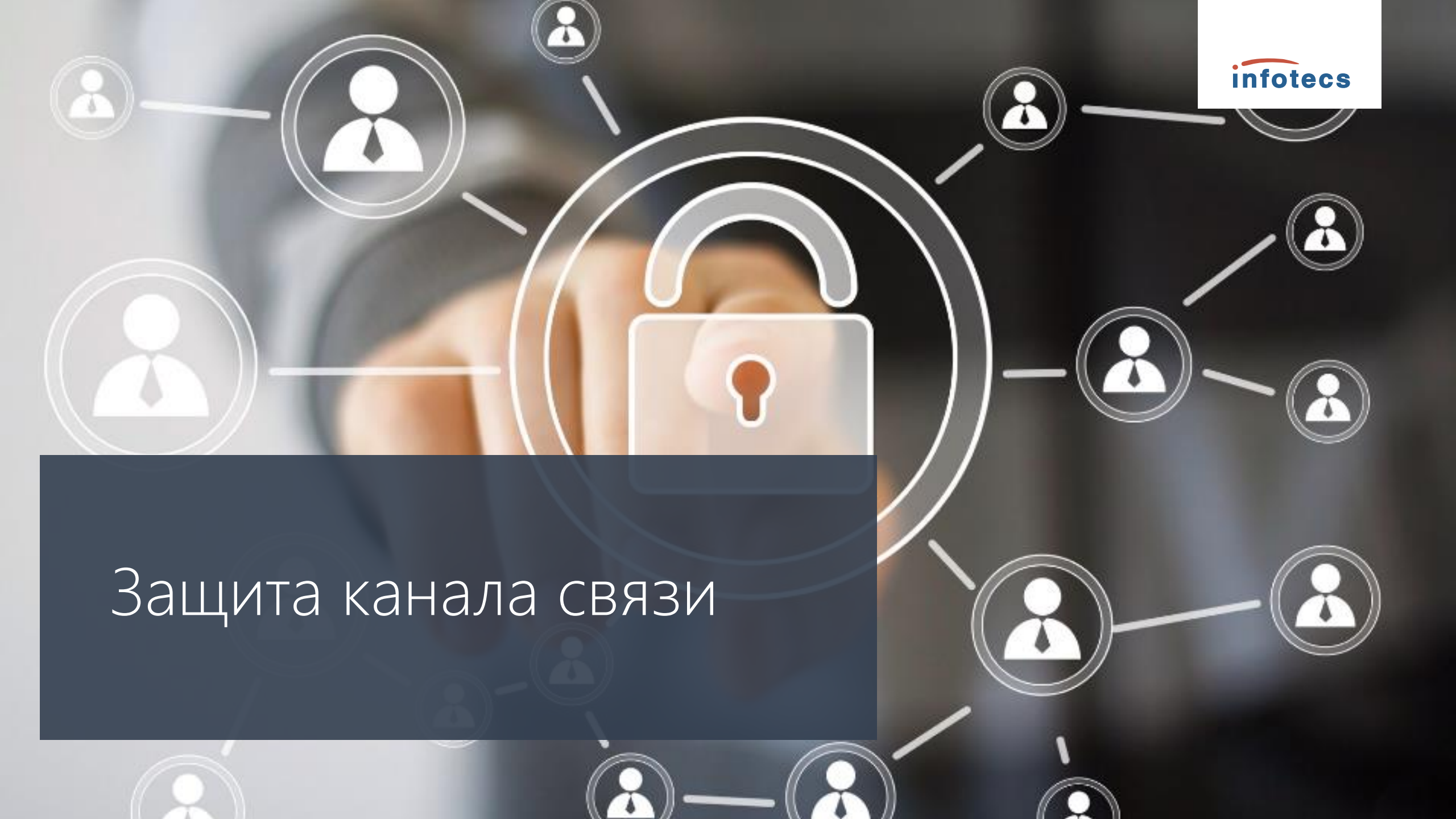
Длительный период подготовки

Методы социальной инженерии

Атаки нулевого дня (zero-day exploits) на оборудование

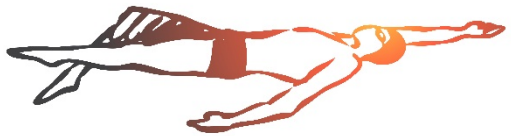
Advanced Persistent Threats





Защита канала связи

Спортивное плавание – 4 вида

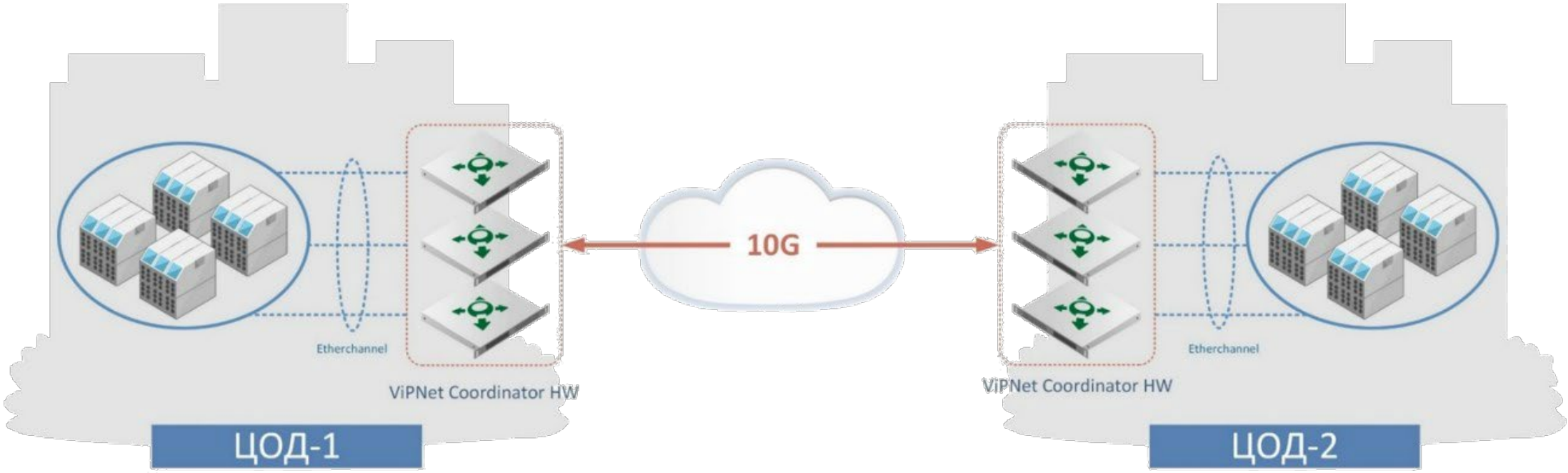


- Баттерфляй
- Кроль на спине
- Способы спортивного плавания
- Кроль на груди
- Брасс

Защита каналов связи (L3 VPN) - кроль

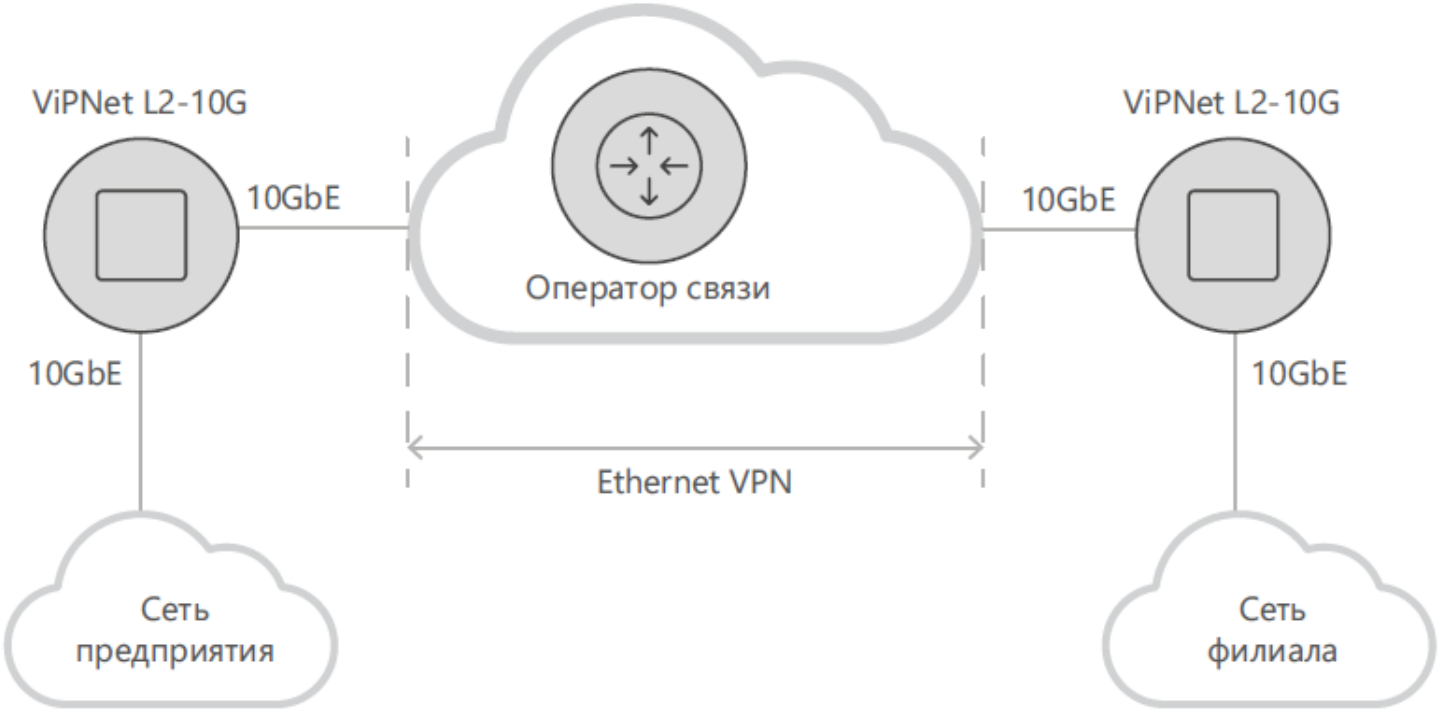
- ✓ Защита периметра сети
- ✓ Объединение распределенных сетей
- ✓ Предотвращение НСД к информации

Защита каналов связи (L2 через L3 VPN) - баттерфляй



Кол-во пар HW	Max UDP (1417 byte), Mbps	Max UDP (8917 byte), Mbps
1 пара HW5000 (2 шт)	5 673	9 374
2 пары HW5000 (4 шт)	12 200	18 552

Защита каналов связи (L2 VPN) - баттерфляй



Кол-во пар шлюзов	**Max UDP (78 byte), Mbps**	**Max UDP (1500 byte), Mbps**	**Max UDP (9000 byte), Mbps**	**Latency,** us
1 пара L2-10G (2 шт)	7 176	9 769	9 948	3,5

Защита каналов связи (L1 VPN) – кроль на спине

- Канал: Оптика, OTN с форматом кадра OTU2 (10Gbit/s)
- Шифрование на уровне L1 со скоростью 10G
- Отсутствие снижения производительности, независимо от размера пакета
- Отсутствие потерь
- Низкая задержка в линии

Защита каналов связи (L4 VPN) - брасс

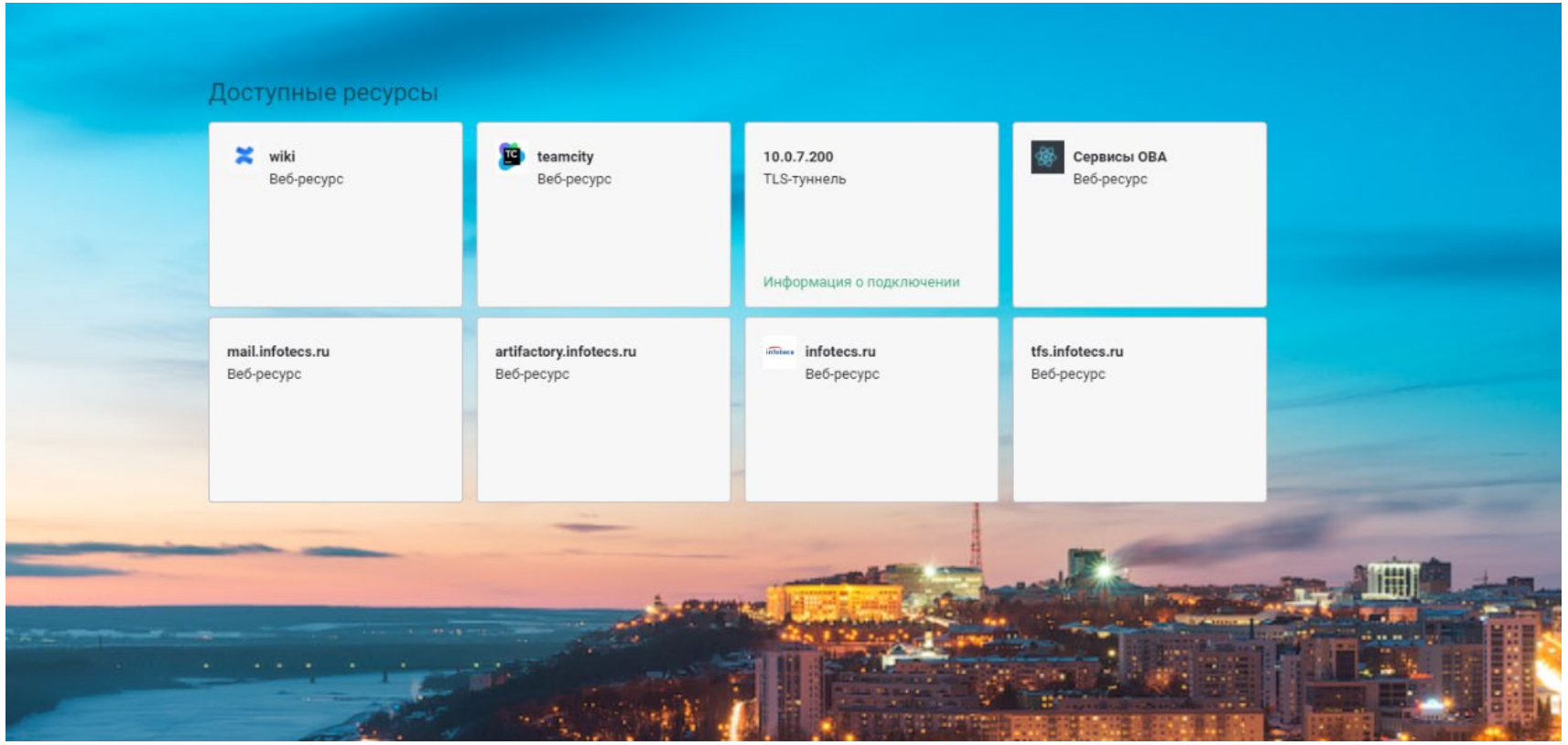
- Совместная работа с ViPNet PKI Client версии 1.3.
- Для протоколов RDP, SMTP, POP3, IMAP, WebDAV и др.
- Поддержка всех браузеров: Chrome, Firefox, Edge, IE

Подключение клиентов

Пользовательскую страницу можно выполнить в корпоративном стиле заказчика

Клиентское ПО:

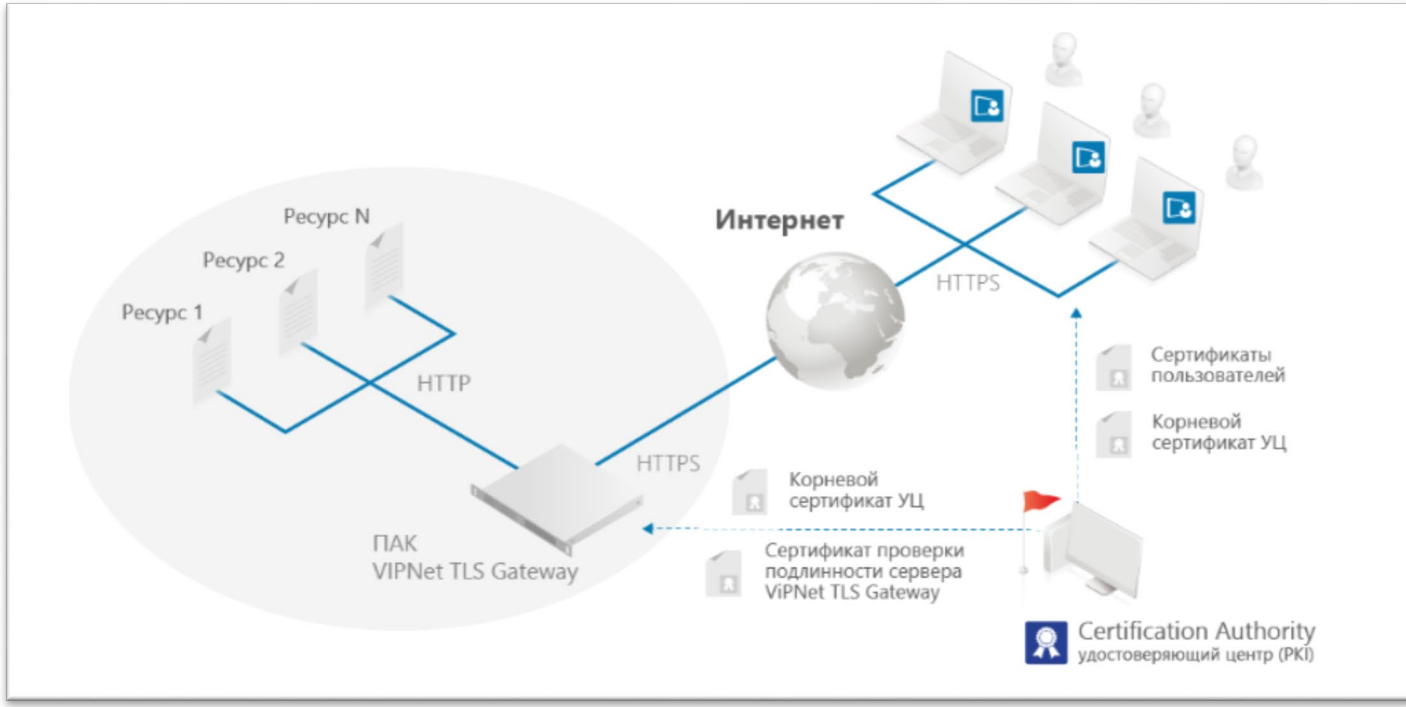
- ViPNet CSP
- ViPNet PKI Client
- СКЗИ (ГОСТ TLS)



ViPNet PKI Client: модули

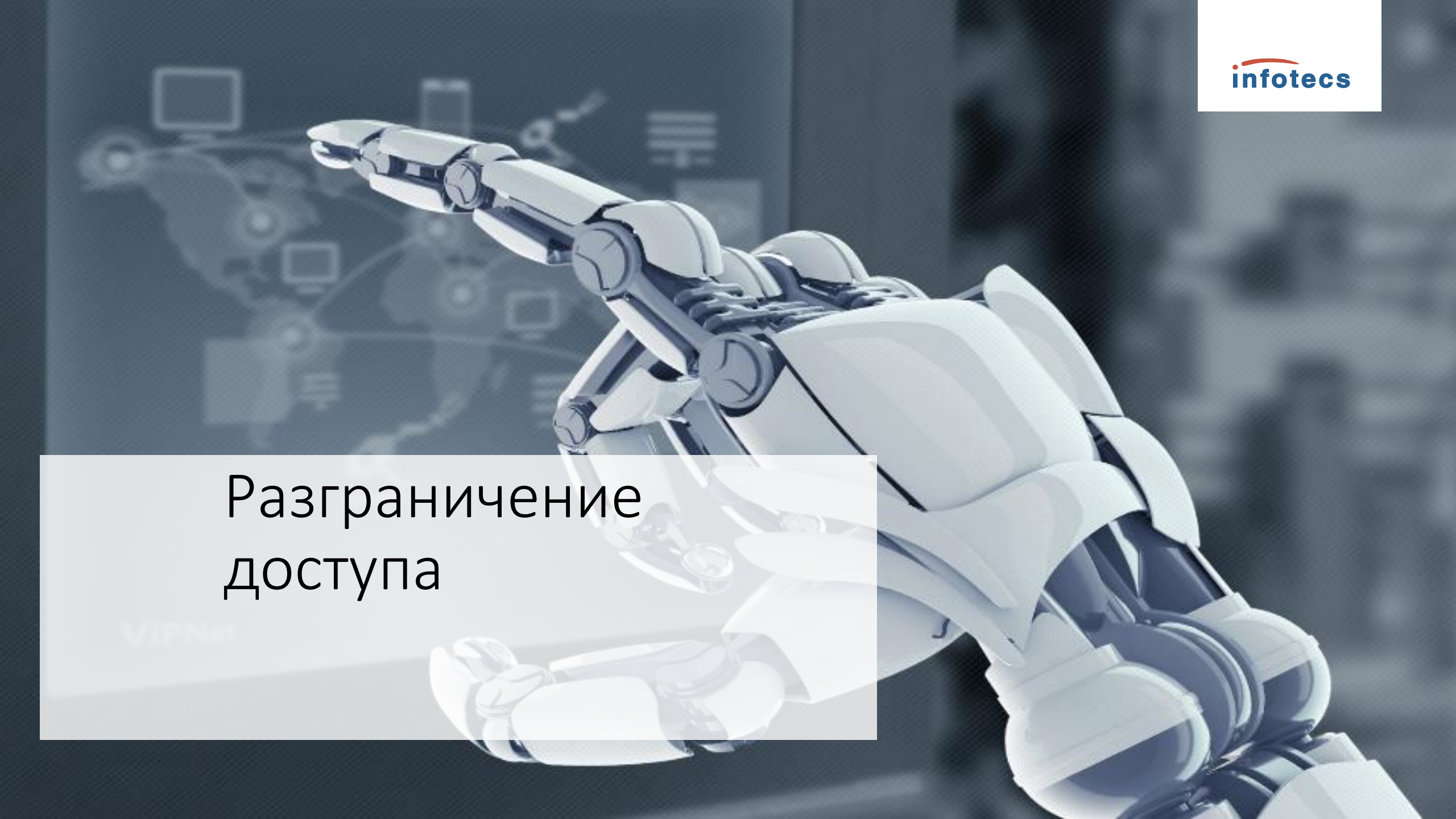
TLS Unit:

- Локальный TLS-proxy
- Совместим с ViPNet TLS Gateway и TLS-шлюзами других производителей (использующих библиотеки КриптоПРО)
- TLS-туннель для TCP-трафика



ViPNet TLS Gateway

Название исполнения	TLS VA	TLS 500	TLS 1000	TLS 5000
Предельная пропускная способность в режиме обратного HTTPS-прокси (Мбит/с)	зависит от характеристик аппаратного обеспечения	до 300	до 750	до 2900
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси	зависит от характеристик аппаратного обеспечения	до 4700	до 8900	до 28000
Максимальное число внешних клиентов (сертификатов)	определяется лицензией	до 3000	до 5000	до 20000



Разграничение доступа

7 задач

- Знать что охранять
- Управлять доступом
- Защитить от сетевых атак
- Реализовать BYOD
- Защитить от вирусов
- Что делать с SSL
- Защита от неизвестных угроз

ViPNet xFirewall

infotecs®

Шлюзы безопасности

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

Что такое ViPNet xFirewall

Сетевая платформа в составе:

Межсетевой экран

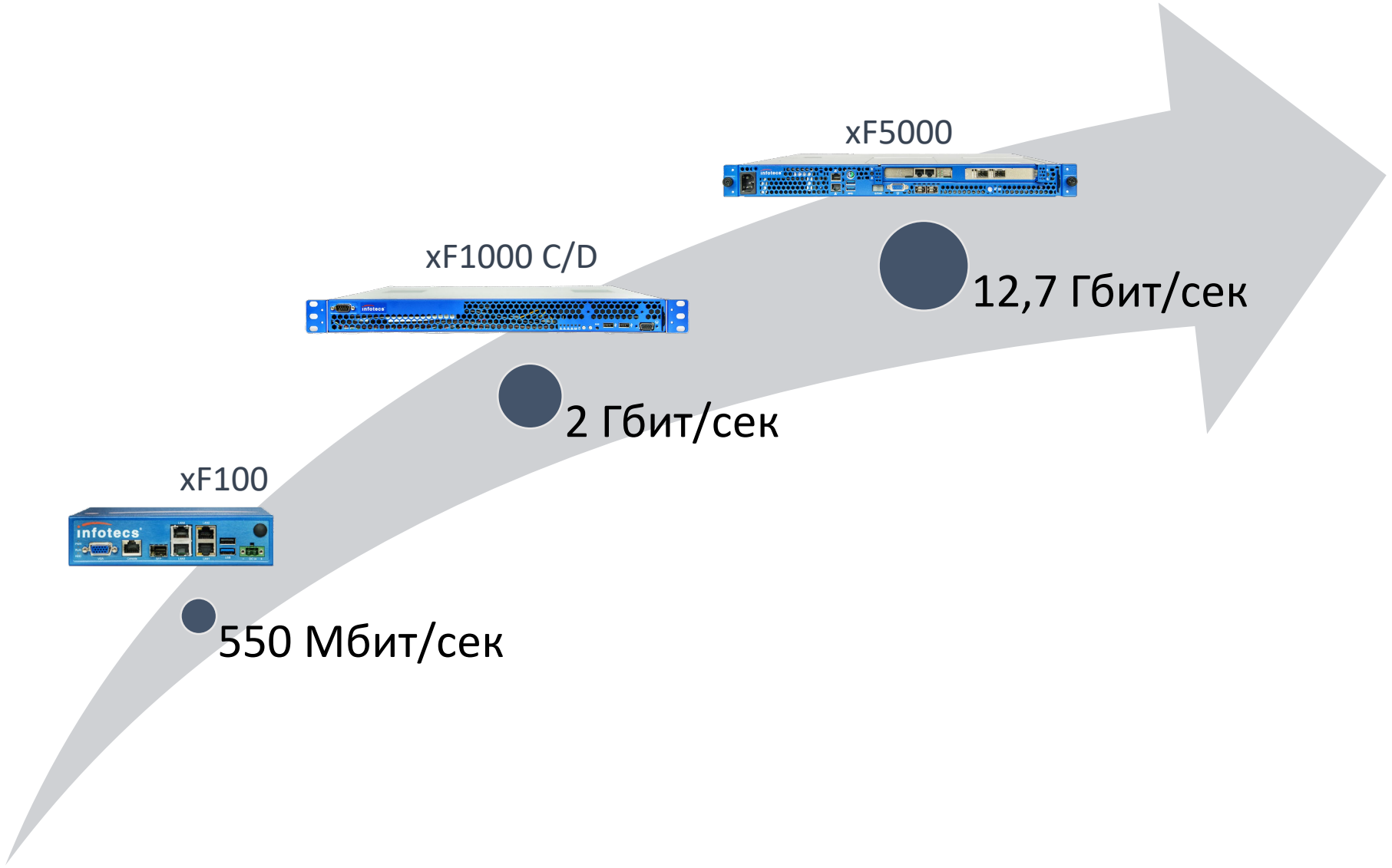
Сетевой экран приложений - DPI

Система предотвращения вторжений

Шлюзовой антивирус

Интеграция с Active Directory

ViPNet xFirewall. Платформы



Производительность

Исполнение	xF100 	xF1000 C/D 	xF5000 
Firewall, 1518 byte UDP (Mbps)	550	2 000	12700
Firewall Throughput (Packets Per Second)	71 000	960 000	1 000 000
Firewall, TCP Multistream (Mbps)	550	2 000	9300
NGFW Througput (Mbps)	140	1 500	2 500
Connections per Second	2 500	19 500	17 500
Concurrent Connections	149 900	990 000	9 900 000

№ 1 - Знать что охранять

- Открыл порты 80/443 == Открыл всЁ!

2065 уникальных приложений/протоколов

95 из категории «Социальные сети»

45 – потоковое видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

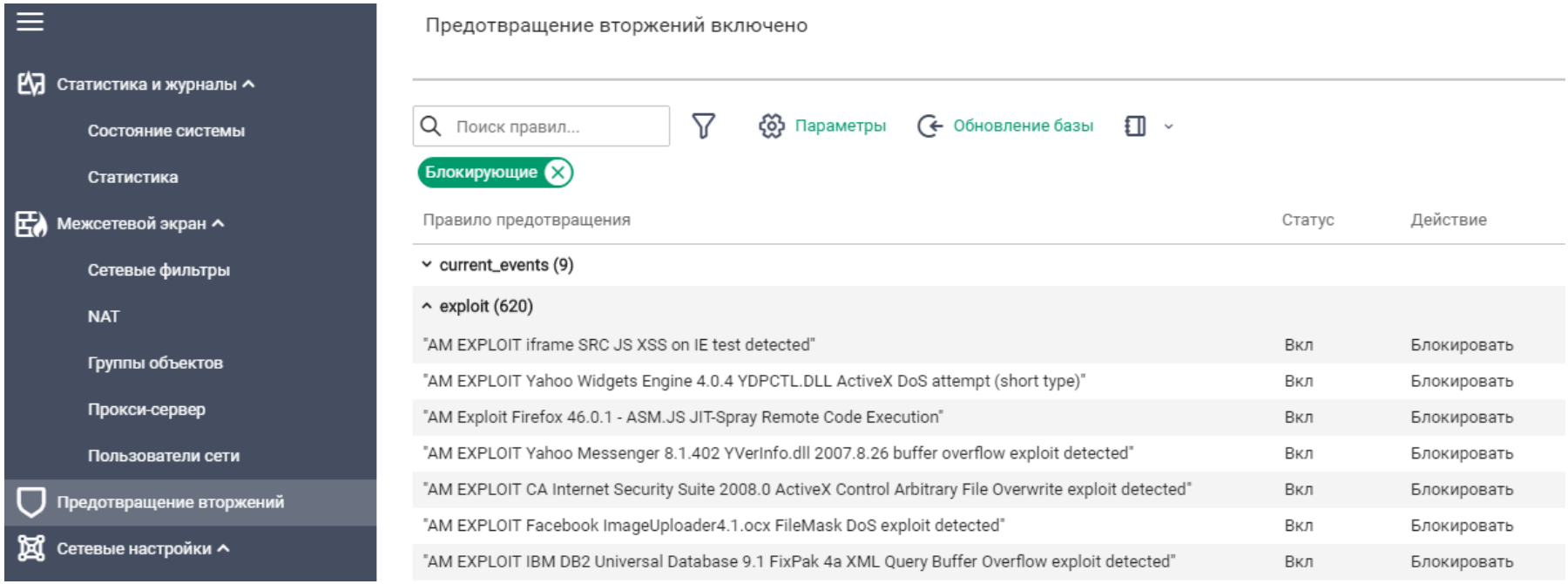
№2 - Управлять доступом

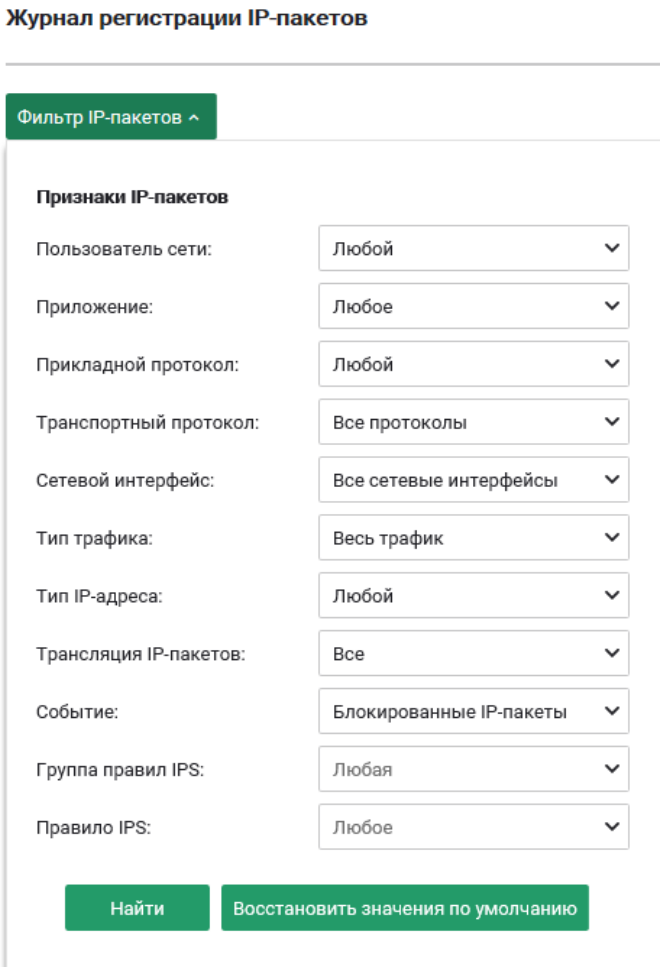
Интеграция с MS AD

№3 – Защита от сетевых атак

ViPNet xFirewall 5.0

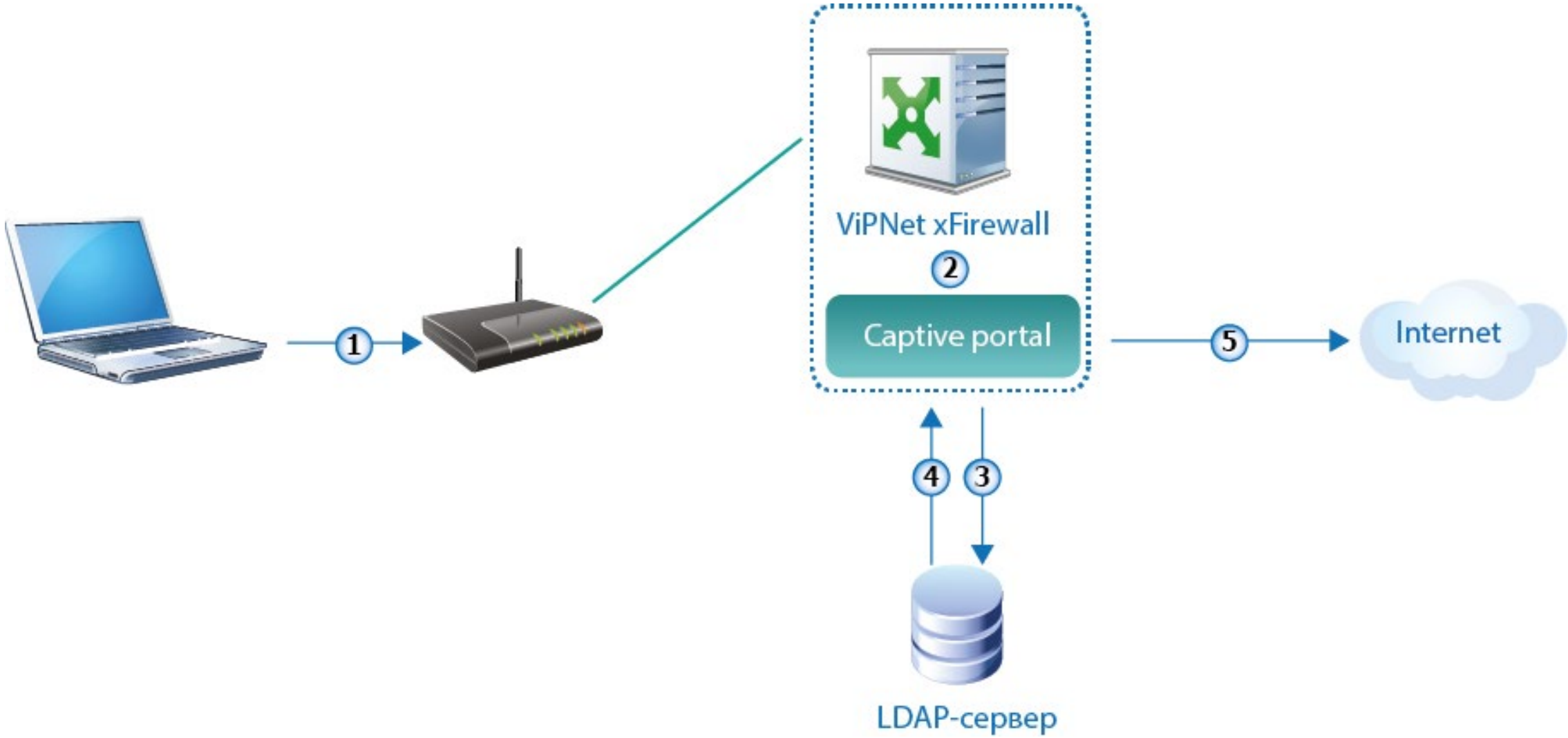
Релиз весной 2019 года.





№4 - BYOD

Captive portal

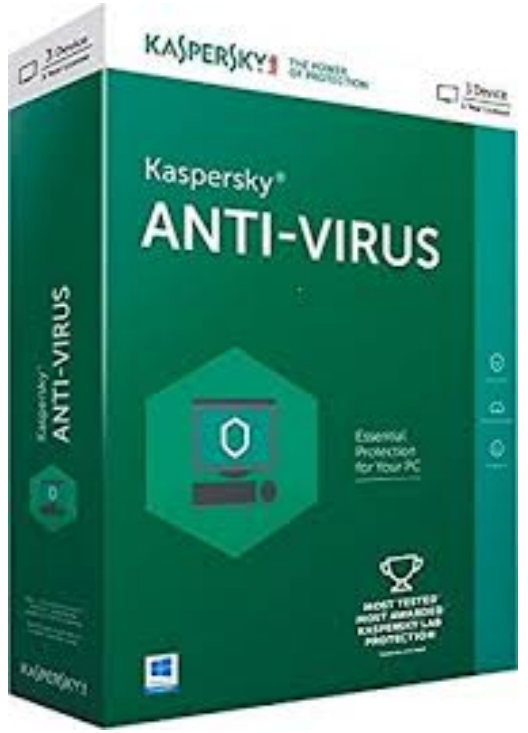


№5 – Защита от вирусов

Антивирус Касперского для Proxy Server

Антивирус Касперского для Proxy Server — это решение для защиты HTTP- и FTP-трафика, проходящего через прокси-сервер.

Приложение обеспечивает защиту пользователей при работе с интернет-ресурсами, удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP и FTP.



№6 – Что делать с SSL

Если нельзя запретить – нужно возглавить

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

№7 – 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

Сертификация

ФСТЭК на соответствие требованиям к МЭ типа А, Б 4 класса

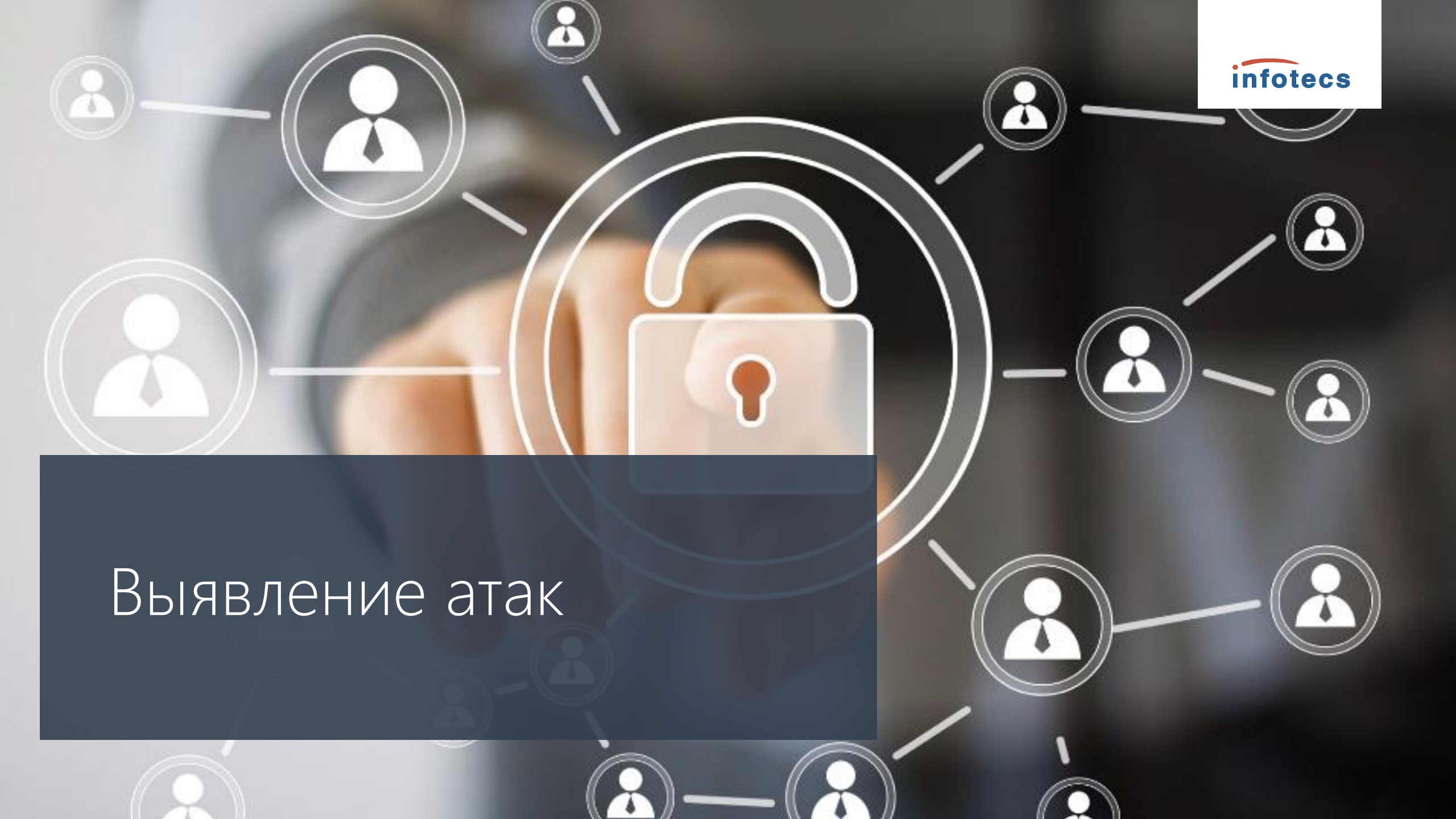
В чем польза от ViPNet xFirewall

Комплексная защита от 7 бед сетевой безопасности

Снижение объема Интернет трафика за счет блокирования ресурсов развлекательного характера

МЭ типа А, Б 4 класса по новым требованиям ФСТЭК

Сравним по возможностям с западными аналогами



Выявление атак

Методы обнаружения

Обн
злоуп

ужение
малий

Обнаружение следующего поколения

Old School Versu… …y Products

Old School Rule Ba…

- SIEM broad scope monitoring
- Intrusion detection and prevention
- Database and File audit, DLP
- Identity access management
- Antivirus and anti-malware protection

…w School Analytics

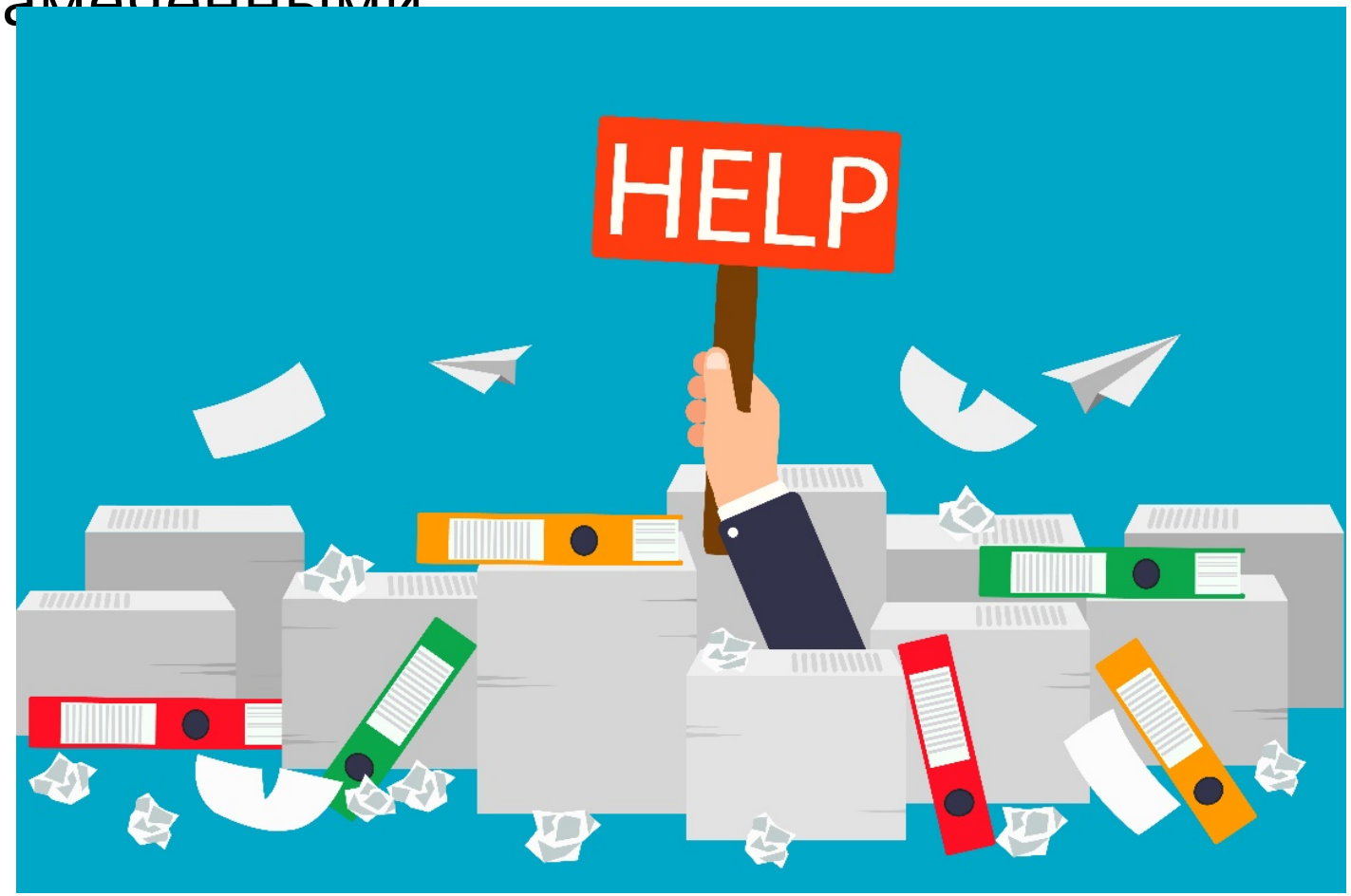
- UEBA broad scope analytics
- Network traffic analytics
- Data and File access and exfiltration analytics
- Identity analytics
- Advanced analytics for endpoint

Add advanced analytics

Add platform features

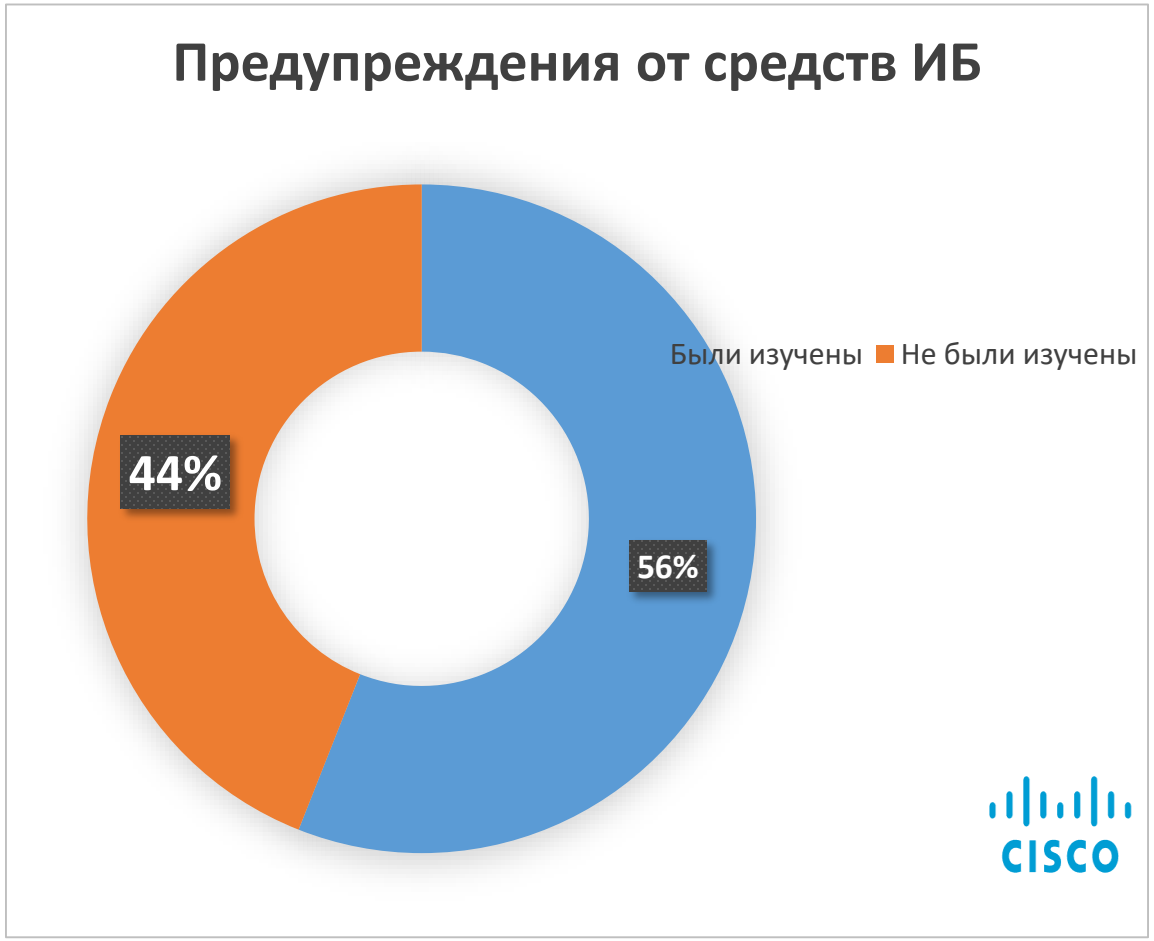
Gartner

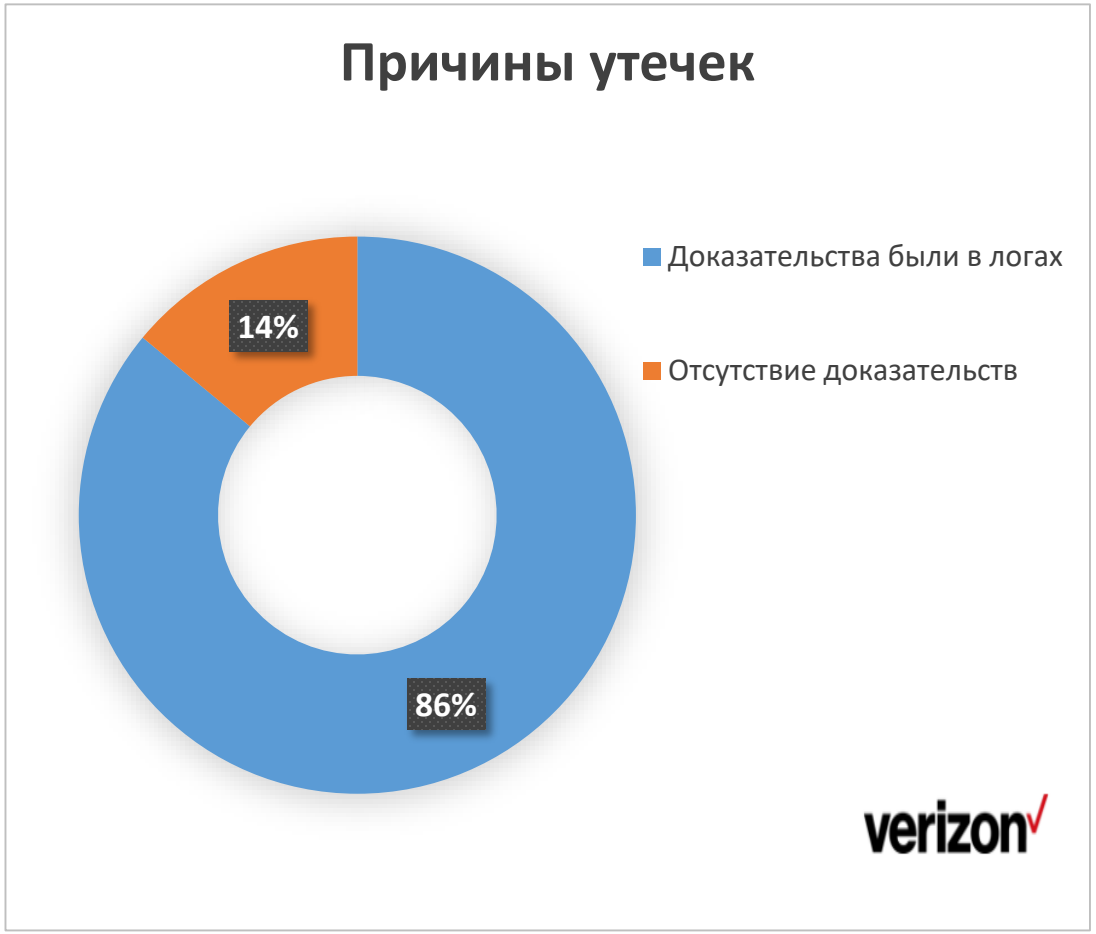
Важные события остаются не замеченными



Средства ИБ создают «информационный шум»!

Результаты исследований



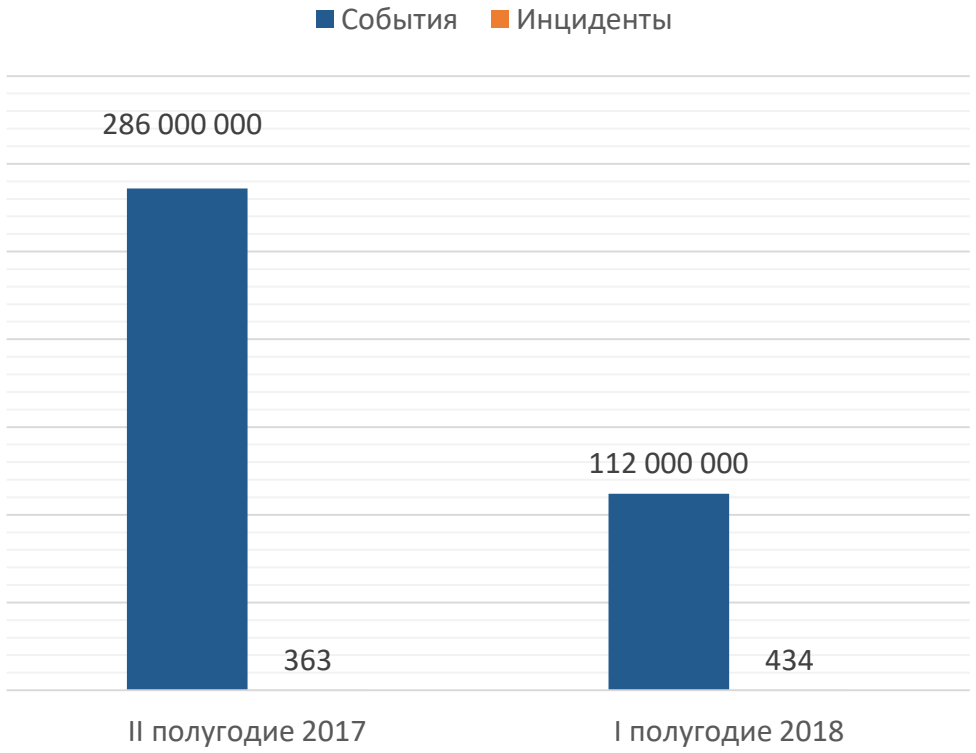


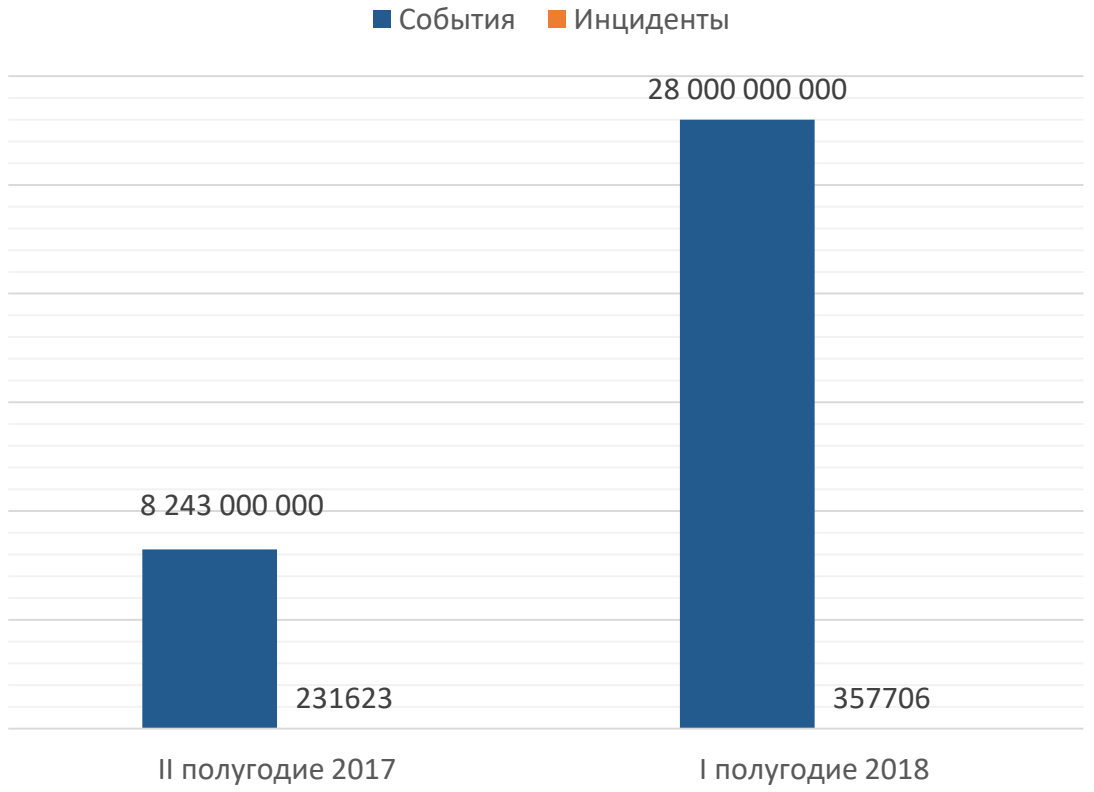
Причины неудовлетворенности системой SIEM

Сколько событий обрабатывает SOC?

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

SOLAR SECURITY software&services





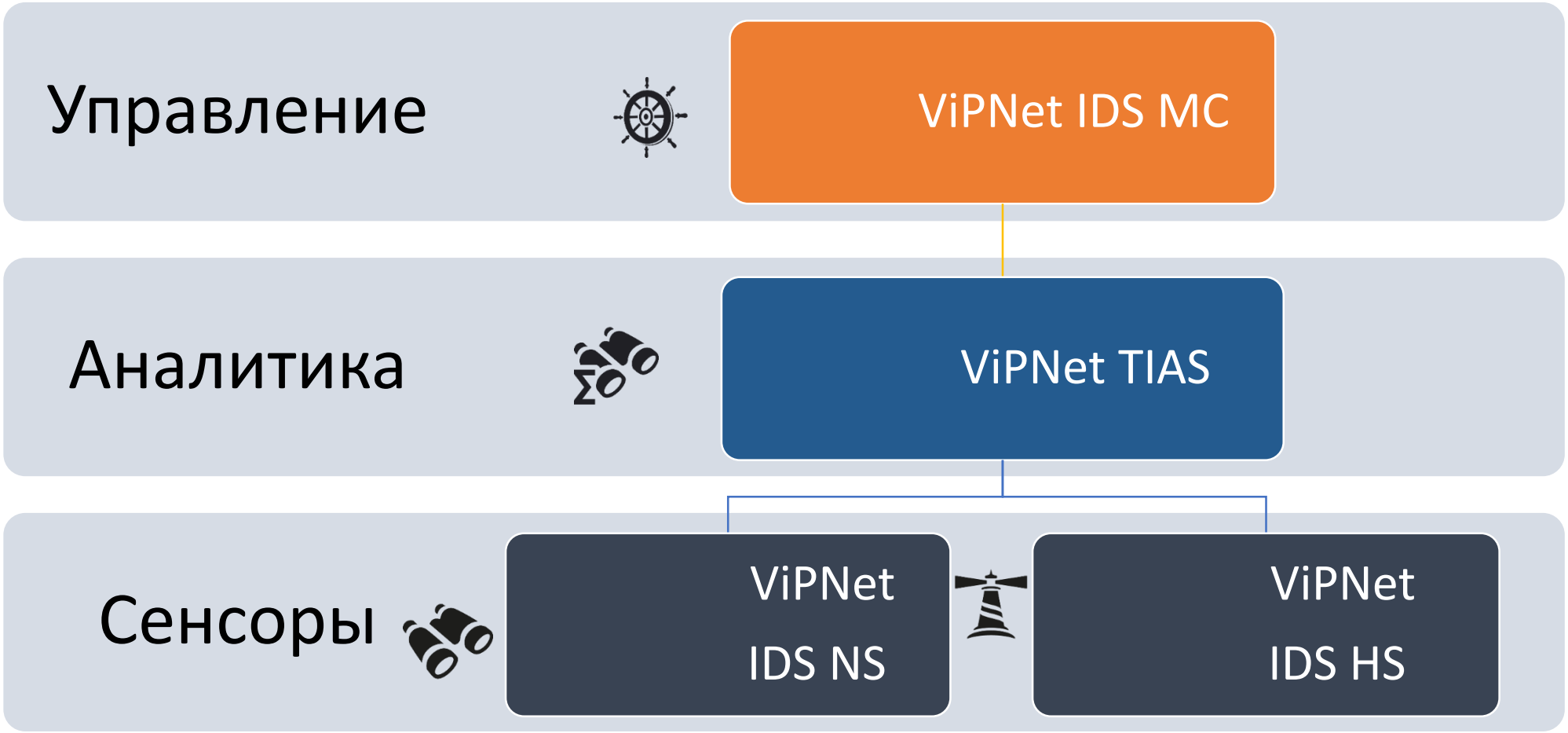
Что нужно

Экспертиза - опыт

Автоматизация

Решение от ИнфотеКС

Решение по обнаружению угроз и вторжений



Решаемые задачи

Непрерывный процесс анализа событий

Адекватная реакция на произошедшие события

Быстрое устранение последствий инцидента

Извлечение полезных уроков

Сенсоры

ViPNet IDS NS

✓ Система обнаружения вторжений уровня сети

ViPNet IDS HS

✓ Система обнаружения вторжений уровня узла

Система управления IDS MC

- ✓ **Управление** структурой и настройками сенсоров;
- ✓ **Управление** конфигурациями правил;
- ✓ **Мониторинг** работоспособности сенсоров;
- ✓ **Обновление:**
  - баз решающих правил;
  - баз сигнатур вредоносного ПО;
  - экспертных данных;

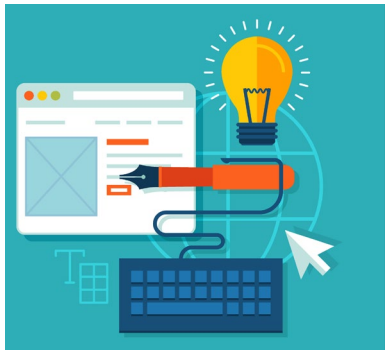
Сценарий обработки событий

Как это работает?

События ИБ

Threat Intelligence

Модуль анализа
ViPNet TIAS



Инциденты ИБ

Статистика и
отчеты

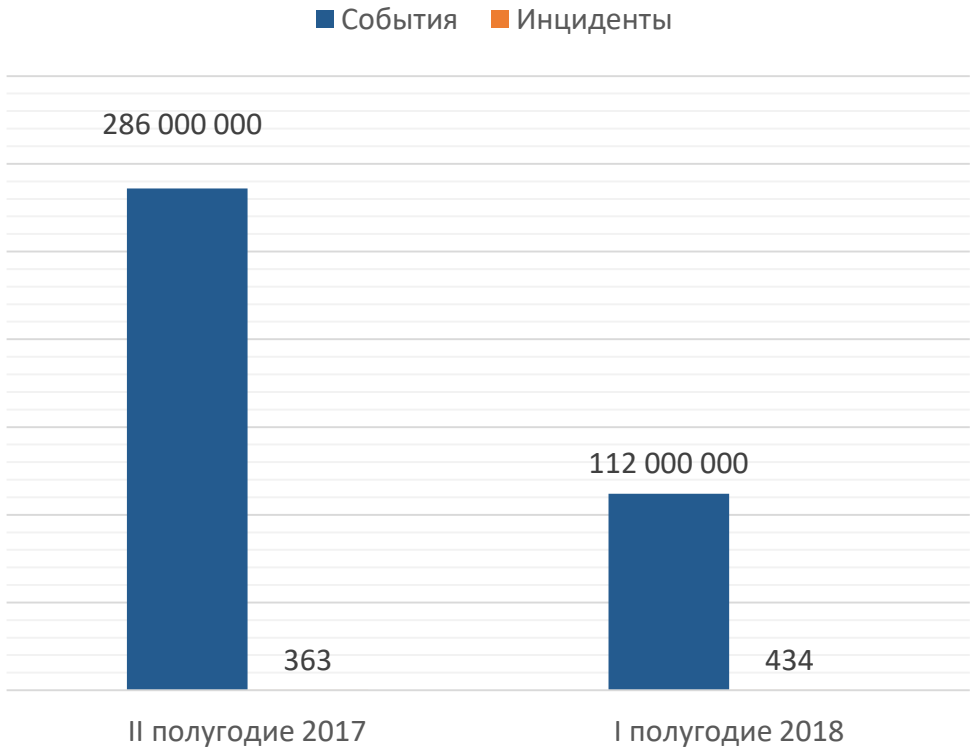
Комбинирование двух методов

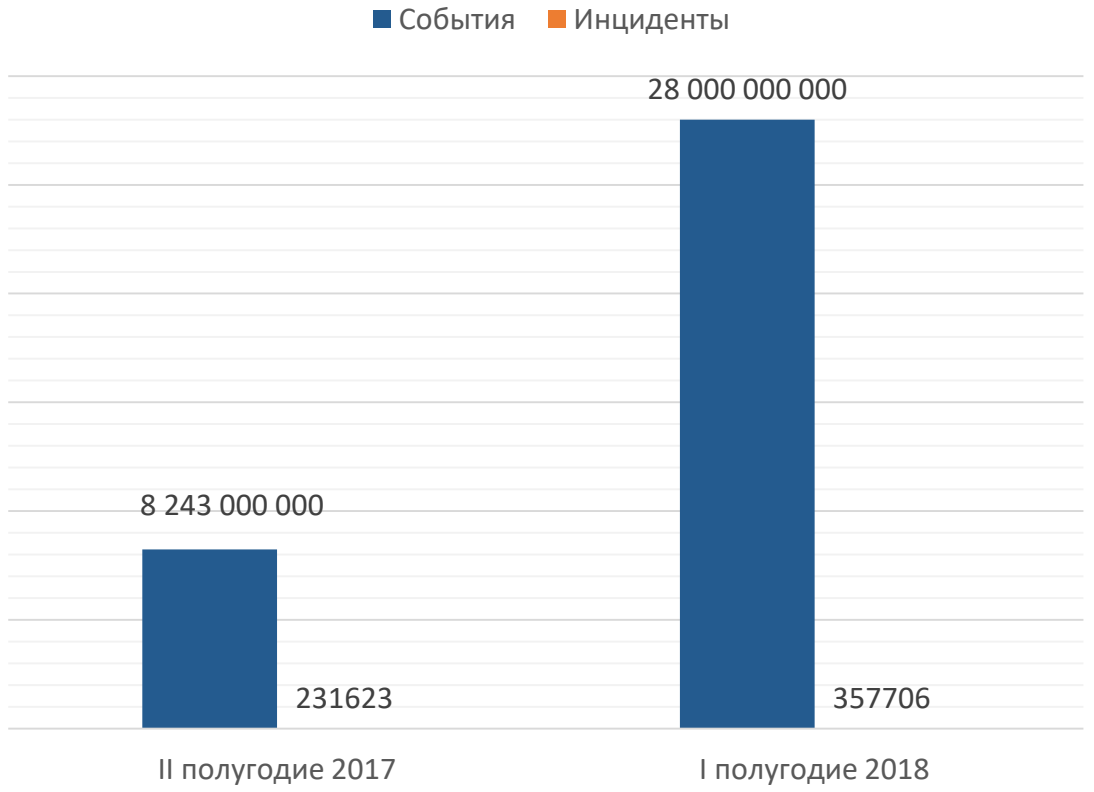
- **Сигнатурный метод** – на основе метаправил выявления инцидентов
- **Эвристический метод** – на основе машинного обучения математической модели принятия решений

Сколько событий обрабатывает SOC?

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

SOLAR SECURITY software&services






infotecs
Спасибо!

Продукты

Экосистема

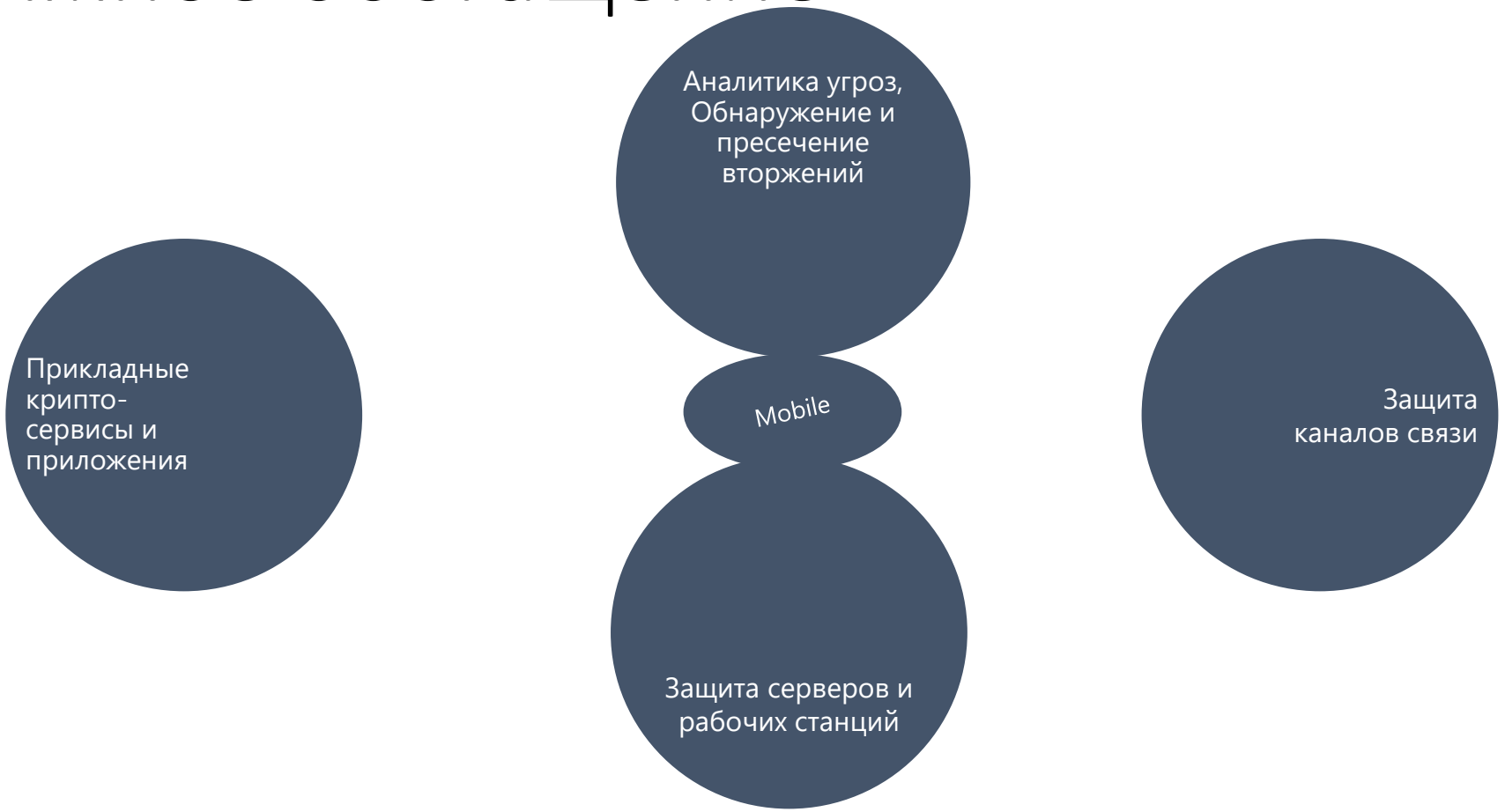
- Доверие
- Анализ активности
- Сегментация подключений и защита каналов
- Права и политики
- Адаптация к предметной области

Продукты

Сетевая безопасность
Network Security

- ViPNet VPN
- ViPNet IDS MC
  ViPNet TIAS
  ViPNet IDS NS
  ViPNet IDS HS
- ViPNet TLS Gateway
  ViPNet PKI Client

Взаимное обогащение



Идеальная СОВ

Покрывает все классы атак

Покрывает все уровни

Адаптивна к неизвестным атакам

Масштабируется

Является открытой

встроенные механизмы реагирования

защищённой от атак на компоненты

Threat Intelligence -

это регулярно и системно собирать информацию об угрозах, улучшать и обогащать её, применять эти знания для защиты и делиться с теми, кому они могут быть полезны

Знания об угрозах:

- ✓ **Индикаторы** атак и компрометации;
- ✓ **ТТП -** тактики, техники, процедуры;
- ✓ **Информационный обмен:**
- ✓ СОПКА, ФСТЭК, RU-CERT;
- ✓ **Опыт клиентов -** верифицированная и обезличенная информация