The background of the slide is a photograph of a businessman in a dark suit and blue tie, holding a large, metallic, 3D-rendered gear. The gear is highly detailed, showing its teeth and internal structure. The image is semi-transparent, allowing the text to be overlaid. The overall color palette is cool, with blues and greys.

Сетевая безопасность следующего поколения

APT – целенаправленная атака



Целевая
кибератака



Продолжительность



Длительный период
подготовки

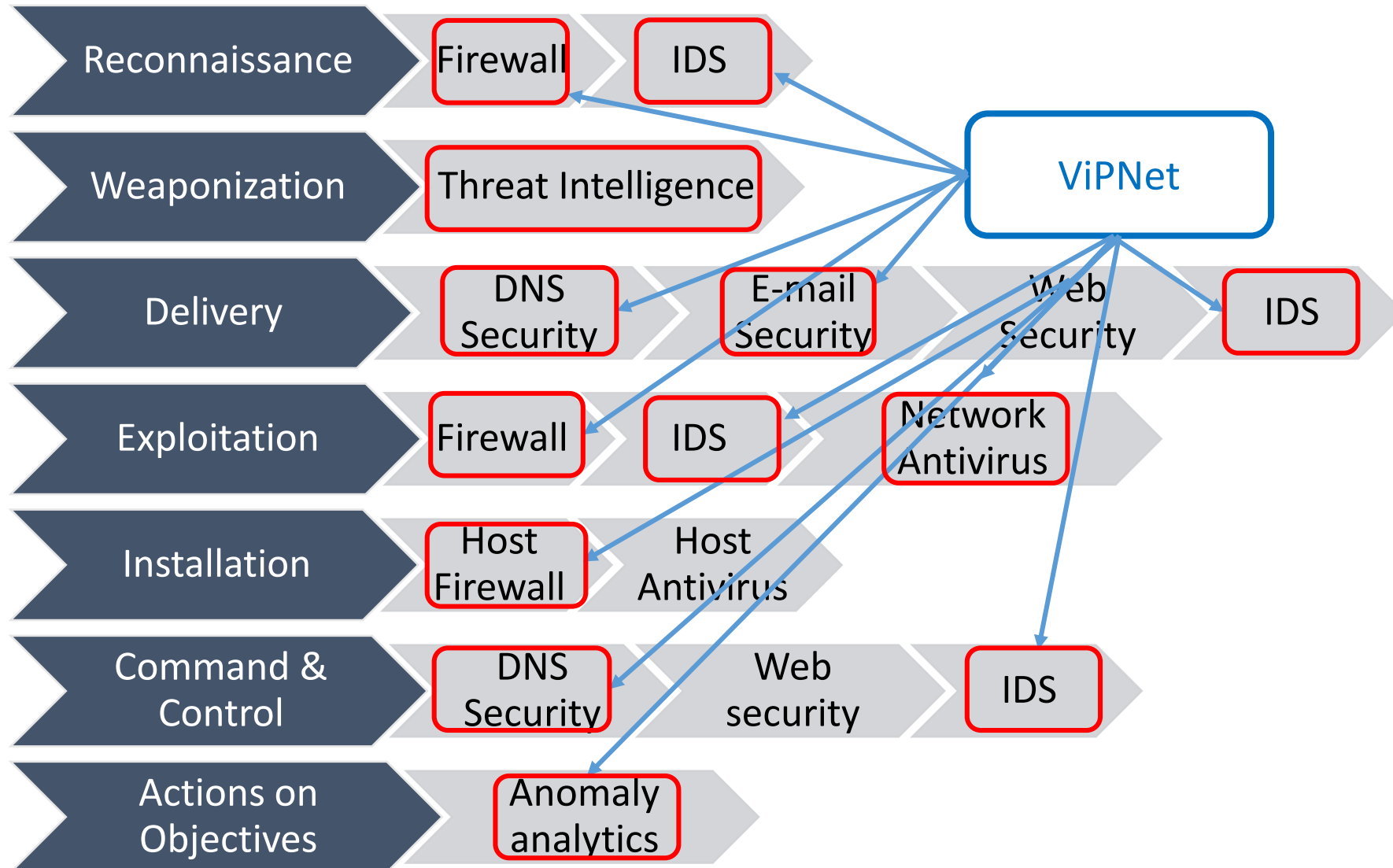


Методы
социальной
инженерии



Атаки нулевого дня (zero-day
exploits) на оборудование

Advanced Persistent Threats



The background of the slide is a network diagram. It consists of several white circular icons, each containing a stylized person in a suit and tie. These icons are connected by thin white lines, forming a network structure. In the center of the diagram is a large, prominent icon of an open padlock, symbolizing security or protection. The entire graphic is overlaid on a blurred background of a person's hands holding a smartphone.

Защита канала связи

Спортивное плавание – 4 вида



Баттерфляй

Кроль на спине

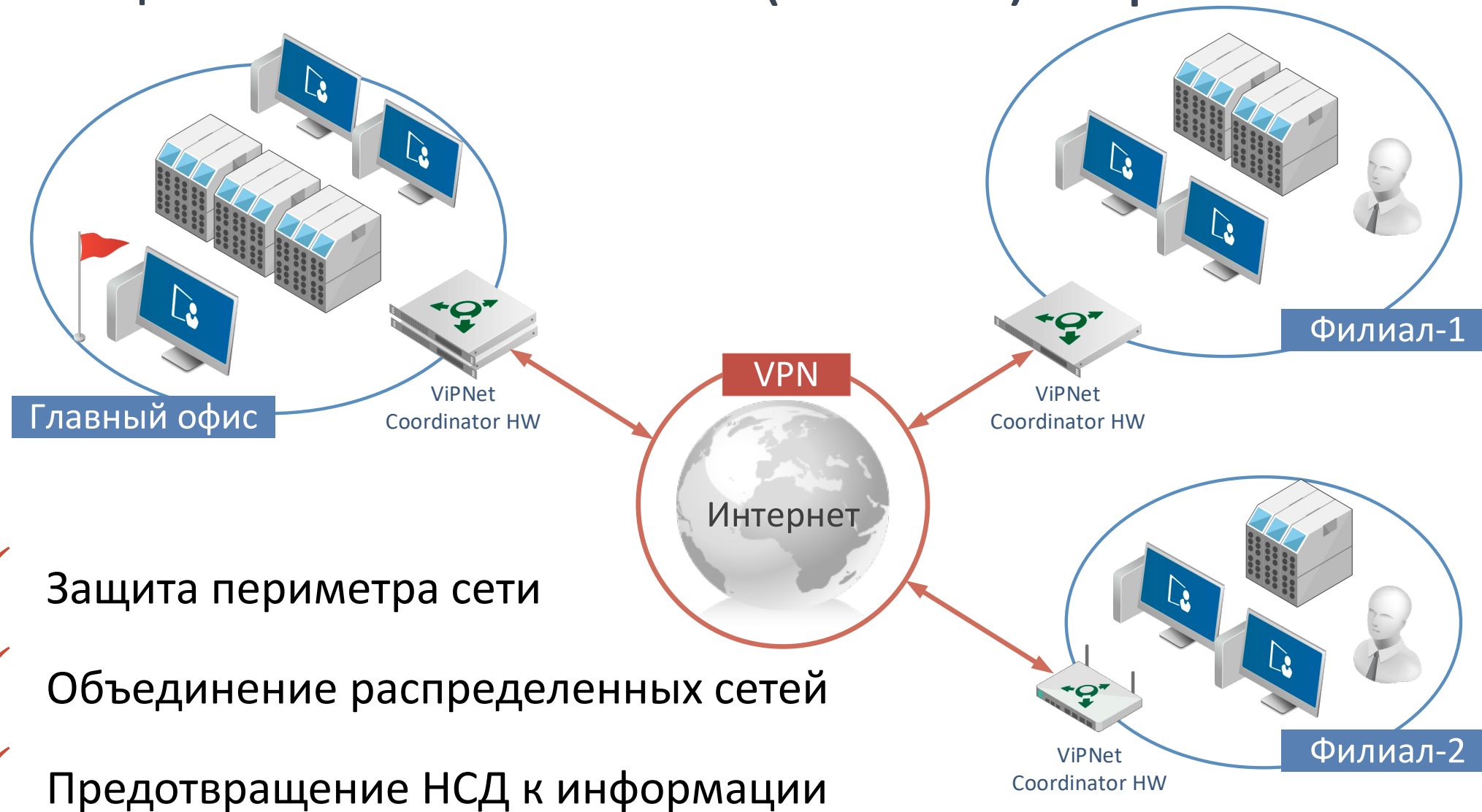
Способы спортивного плавания

Кроль на груди

Брасс

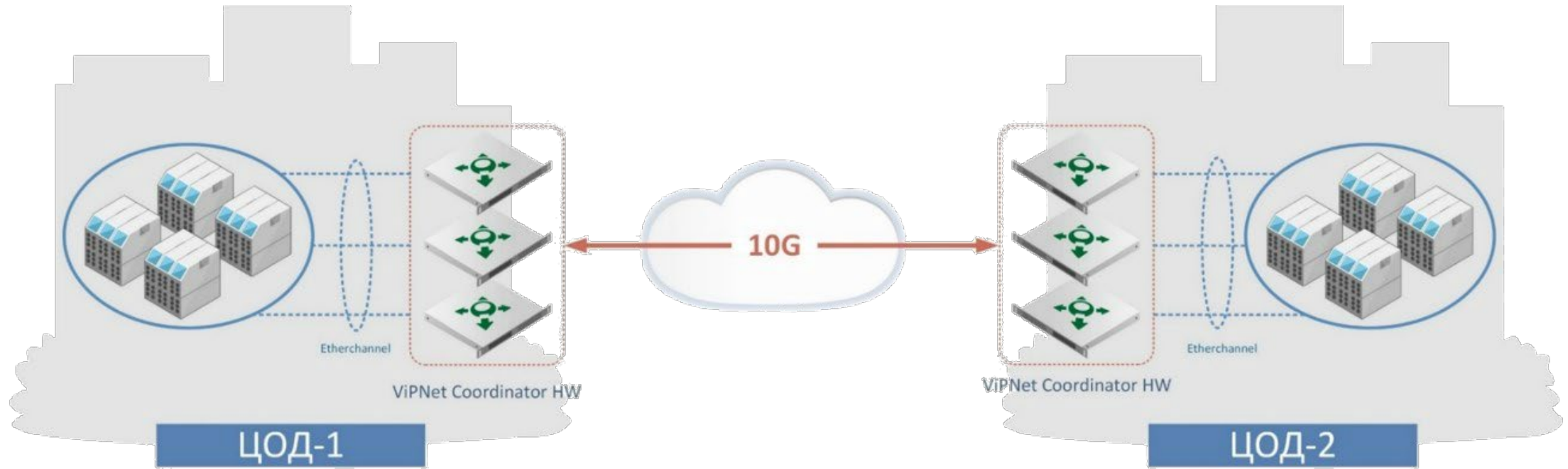


Защита каналов связи (L3 VPN) - король



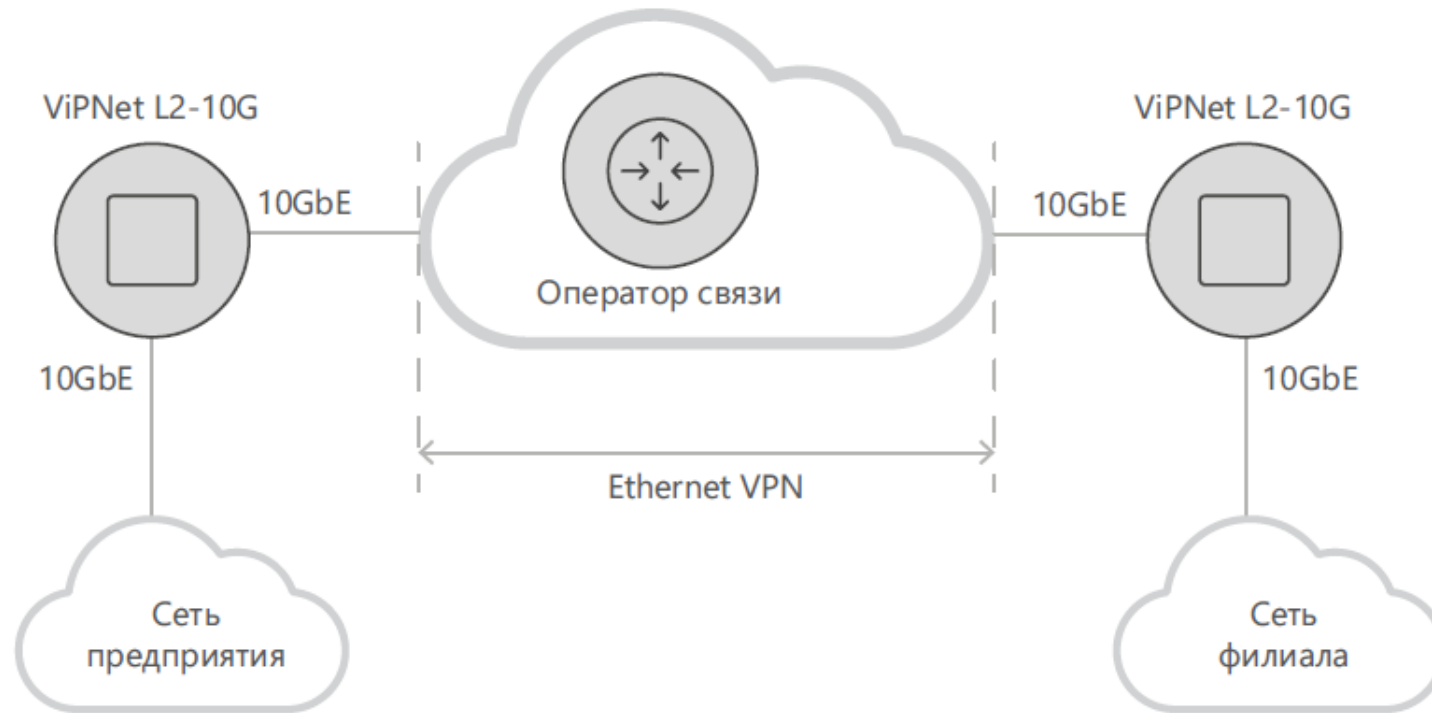
- ✓ Защита периметра сети
- ✓ Объединение распределенных сетей
- ✓ Предотвращение НСД к информации

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



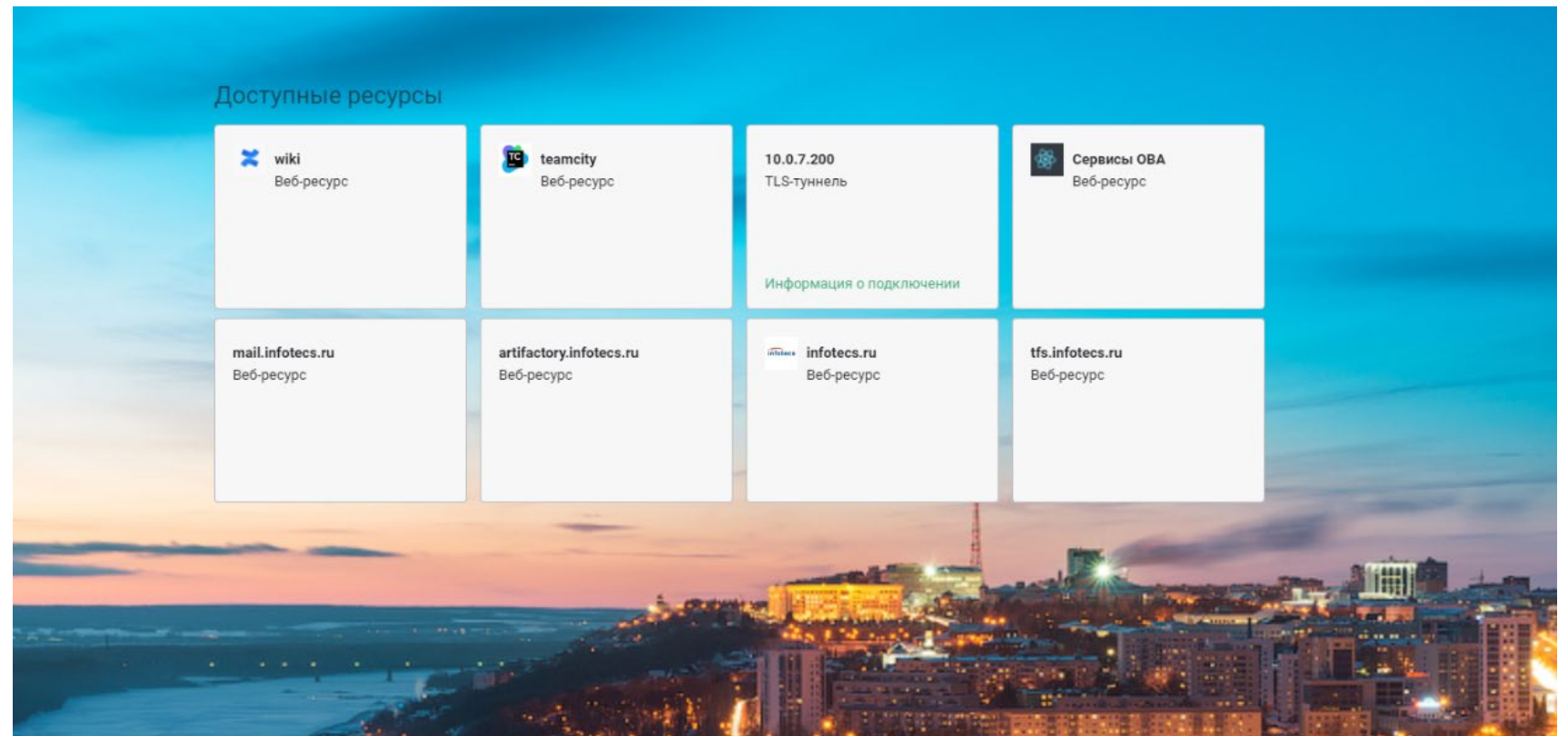
- Совместная работа с ViPNet PKI Client версии 1.3.
- Для протоколов RDP, SMTP, POP3, IMAP, WebDAV и др.
- Поддержка всех браузеров: Chrome, Firefox, Edge, IE

Подключение клиентов

Пользовательскую страницу можно выполнить в корпоративном стиле заказчика

Клиентское ПО:

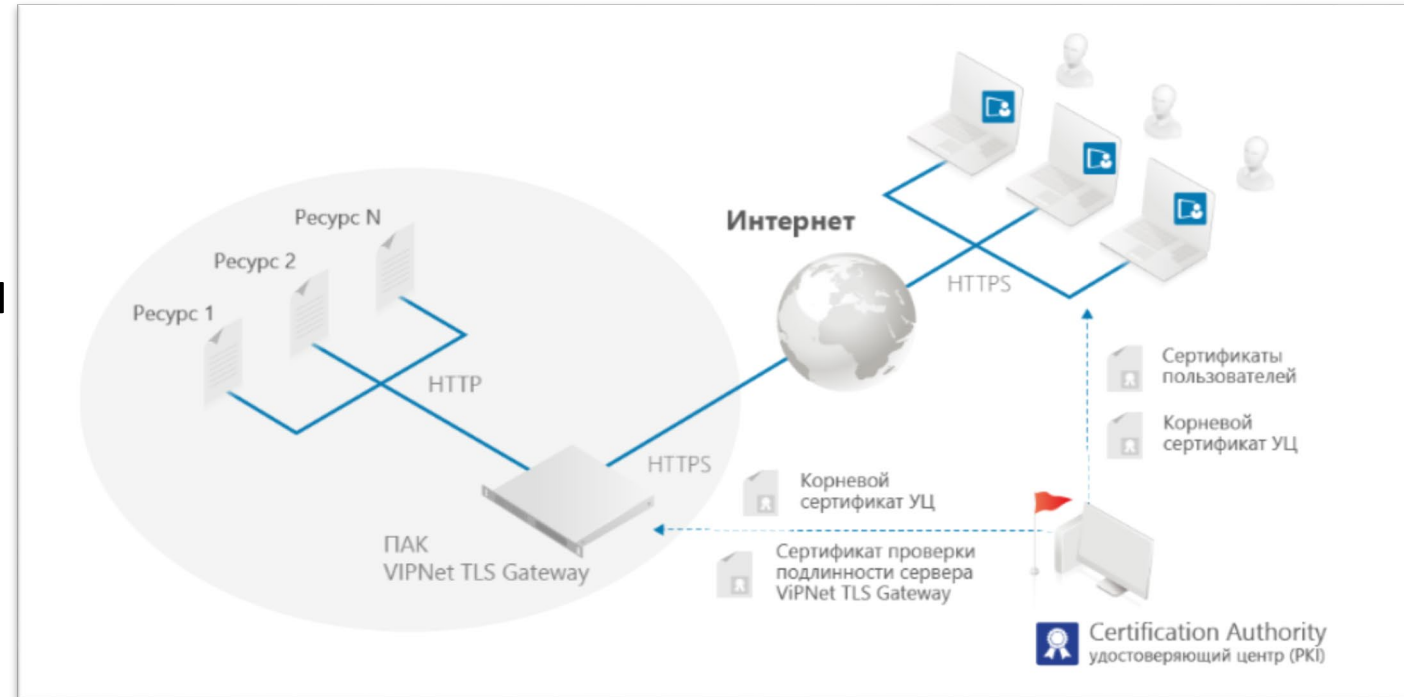
- ViPNet CSP
- ViPNet PKI Client
- СКЗИ (ГОСТ TLS)



ViPNet PKI Client: модули

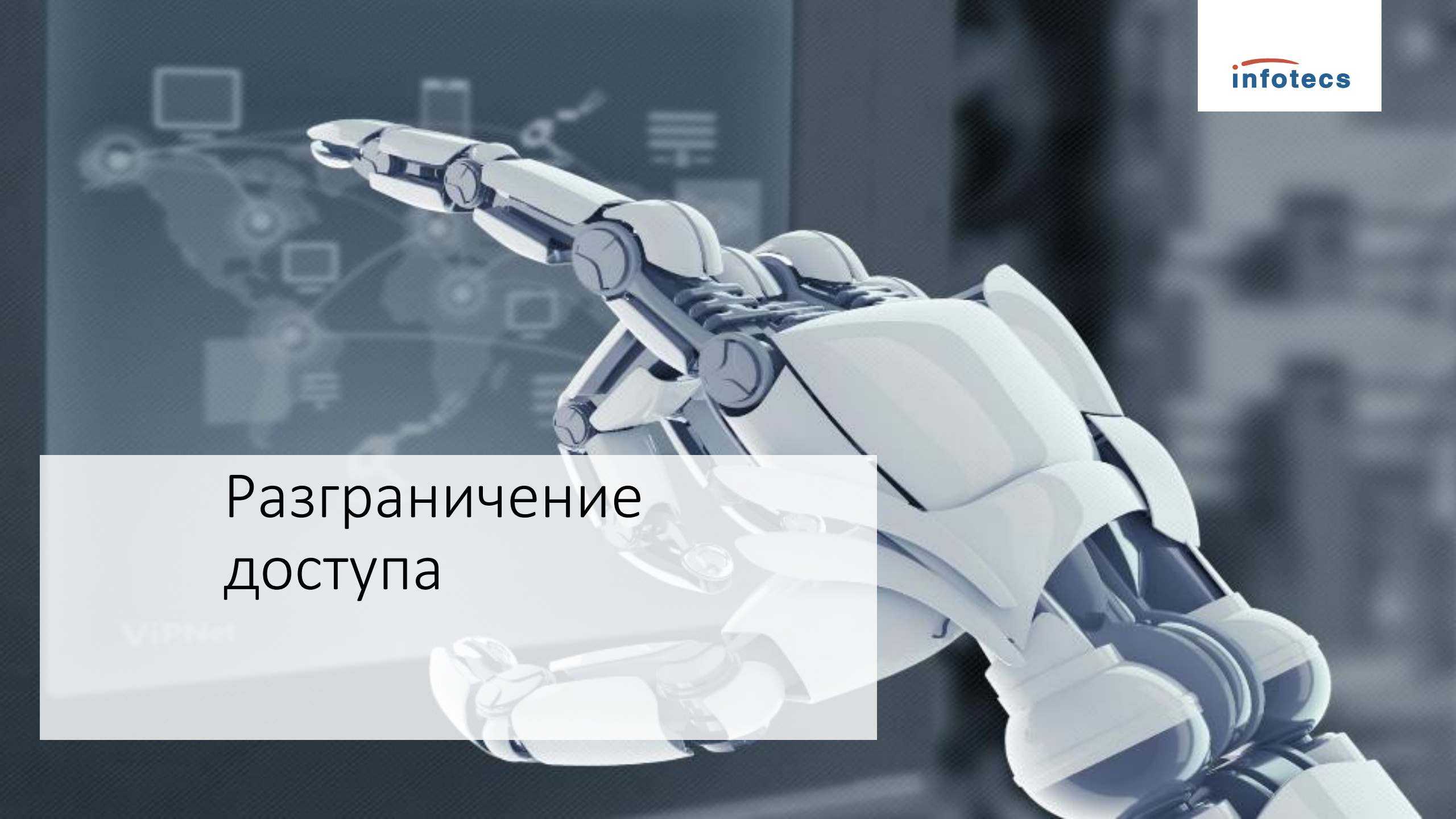
TLS Unit:

- Локальный TLS-проxy
- 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

A 3D rendered robotic hand, primarily white with blue accents, is shown in a dynamic pose, reaching towards the left. The background is a dark, blurred space with faint, glowing icons of various devices and network symbols. A semi-transparent white box is overlaid on the left side of the image, containing the title text.

Разграничение доступа

VIPNet

7 задач

Знать что охранять

Управлять доступом

Защитить от сетевых атак

Реализовать BYOD

Защитить от вирусов

Что делать с SSL

Защита от неизвестных угроз

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

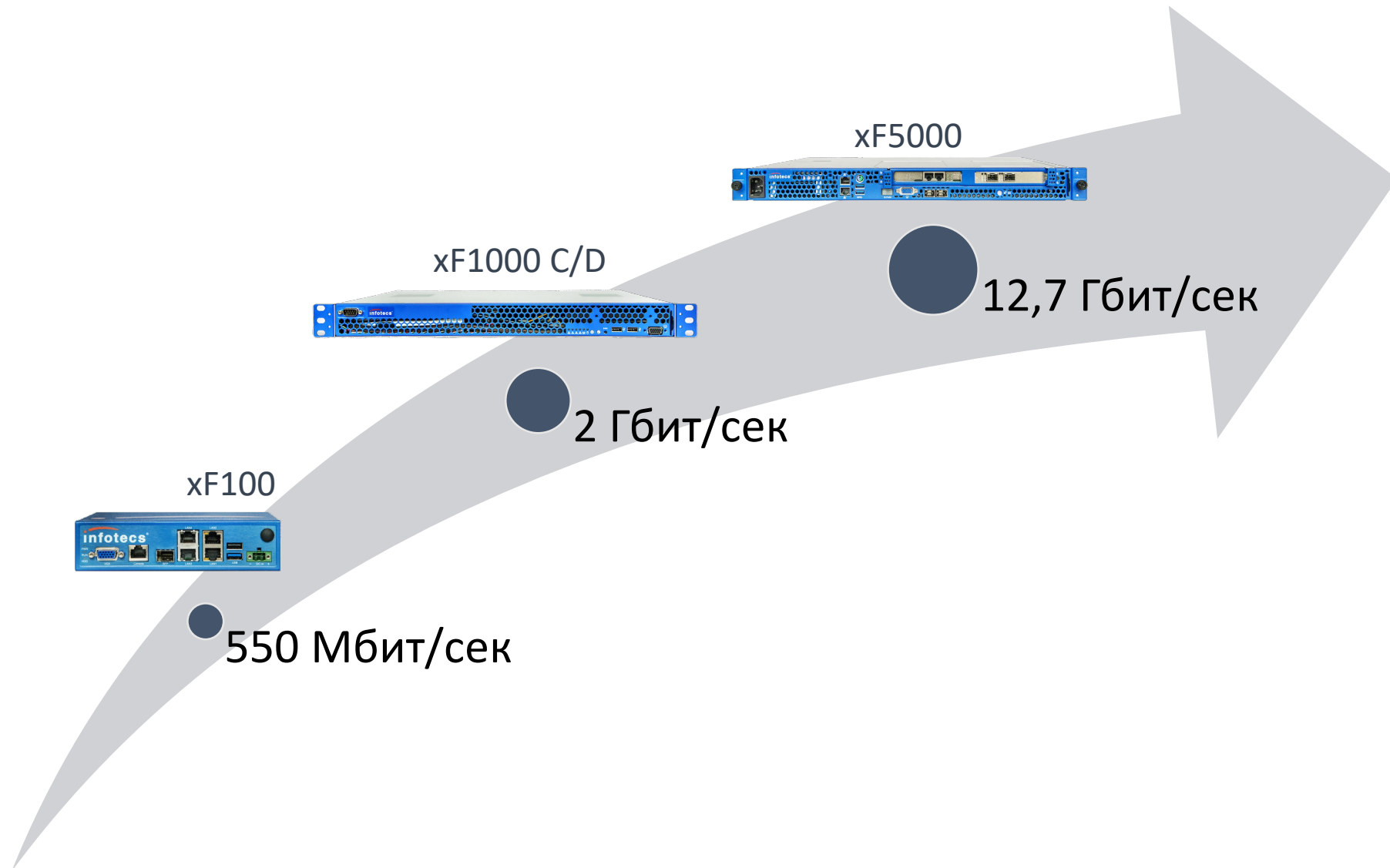
Сетевой экран
приложений -
DPI

Система
предотвращени
я 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



Top Ranking		Top Gainers	
Bejeweled Blitz PopCap	1 →	Hidden Runaway BULKYPDX	139 ▲ 262
Hanging With Friends Zynga Inc.	2 ▲ 1	Tom Clancy's ... Gameloft S.A.	228 ▲ 141
SCRABBLE Free Electronic Arts Inc.	3 ▼ 1	Minecraft Companio ... Jason Fieldman	267 ▲
Jewels of the Amaz ... SGN	4 →	Police Chase Smash ... Hesham Ahmed Kamal	145
James Cameron' ... Gameloft S.A.	5 ▲ 1	G.U.N BYSS mobile	111 ▲
Police Chase Smash Hesham Ahmed Kamal	6 ▲ 2	Wordfeud Bertheussen IT	65 ▲ 99
Police Chase (FREE ... Daniel Carbone	7 ▲ 5	Hidden Expedition: ... Big Fish Games, Inc	329 ▲ 72
Amazon™: Hidden Ex ... Big Fish Games, Inc	8 ▲ 8	Minecraft Help XAECCO LIMITED	293 ▲ 71
Police Chase Car R ... Sean Detmeyere	9 ▲ 2	Crimson: Steam Pir ... Bungie Aerospace Cor ...	277 ▲ 68
Diamond Dash wooga gmbh	10 ▼ 3	The ROBLOX Quiz John LaRouche	142 ▲ 64
Agent Dash Full Fat Productions ...	11 ▼ 2	Justin Bieber/Nick ... Steven Goodemote	220 ▲ 60
Motorcycle Bike Ra ... RoboNacho Systems, L ...	12 ▲ 3	I Dig It Expeditio ... InMotion Software, L ...	132 ▲ 56
iGun Pro™ LITE - T ... Crimson Moon Enterta ...	13 ▼ 3	Solitaire Finger Arts	194 ▲ 56
Air Patriots Lemon Games SL	14 ▼ 9	Choo Choo Steam Tr ... Chillingo Ltd	143 ▲ 53
Goaaa!™ Soccer TA ... Skyworks Interactive ...	15 ▼ 2	Solitaire + Chronological Ltd	258 ▲ 53

95 из категории
«Социальные сети»

45 – потоковое
видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

№2 - Управлять доступом



Интеграция с MS AD



A hand in a dark suit jacket points towards the center of the image. The background is a dark blue gradient with a grid of hexagonal icons. Some icons are padlocks (some locked, some unlocked) and some are magnifying glasses. The text 'INTRUSION DETECTION AND PREVENTION SYSTEM' is overlaid in large, white, outlined letters.

INTRUSION DETECTION AND PREVENTION SYSTEM

ViPNet xFirewall 5.0


infotecs®

Релиз весной 2019 года.

- Статистика и журналы ^
- Состояние системы
- Статистика
- Межсетевой экран ^
- Сетевые фильтры
- NAT
- Группы объектов
- Прокси-сервер
- Пользователи сети
- Предотвращение вторжений
- Сетевые настройки ^

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:	Любой
Приложение:	Любое
Прикладной протокол:	Любой
Транспортный протокол:	Все протоколы
Сетевой интерфейс:	Все сетевые интерфейсы
Тип трафика:	Весь трафик
Тип IP-адреса:	Любой
Трансляция IP-пакетов:	Все
Событие:	Блокированные IP-пакеты
Группа правил IPS:	Любая
Правило IPS:	Любое

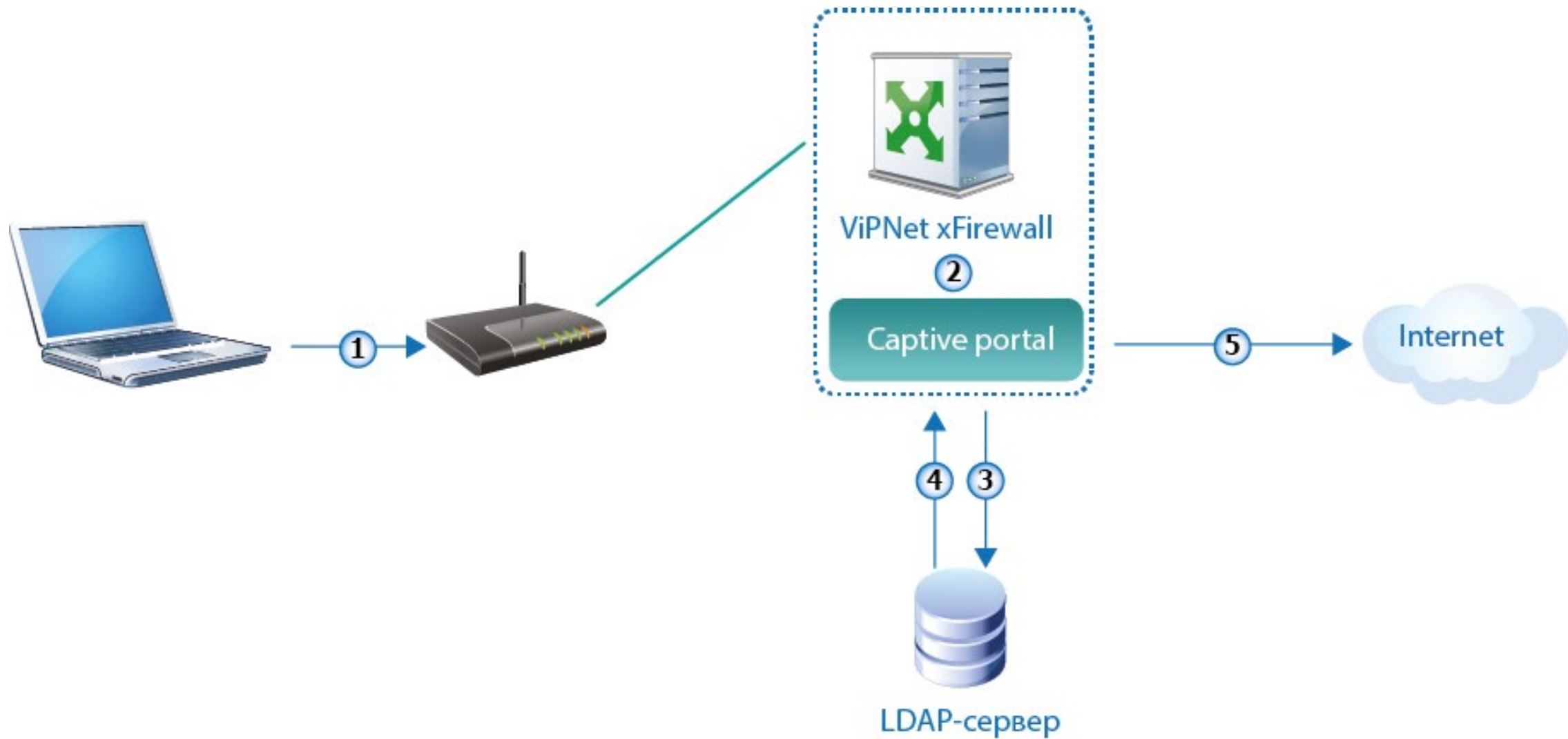
Найти

Восстановить значения по умолчанию

No4 - 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

The background of the slide is a network diagram. It consists of several white circular icons, each containing a stylized person in a suit and tie. These icons are connected by thin white lines, forming a network. In the center of the network is a large, semi-transparent white padlock icon with a keyhole, symbolizing security or a breach. The entire graphic is overlaid on a blurred background of a person's hand holding a smartphone.

Выявление атак

Методы обнаружения

Обн
злоуп



ужение
маний

Обнаружение следующего поколения



Old School Versus

Modern Products

Old School Rule Based

New School Analytics



SIEM broad scope monitoring

UEBA broad scope analytics

Intrusion detection and prevention

Network traffic analytics

Database and File audit, DLP

Data and File access and exfiltration analytics

Identity access management

Identity analytics

Antivirus and anti-malware protection

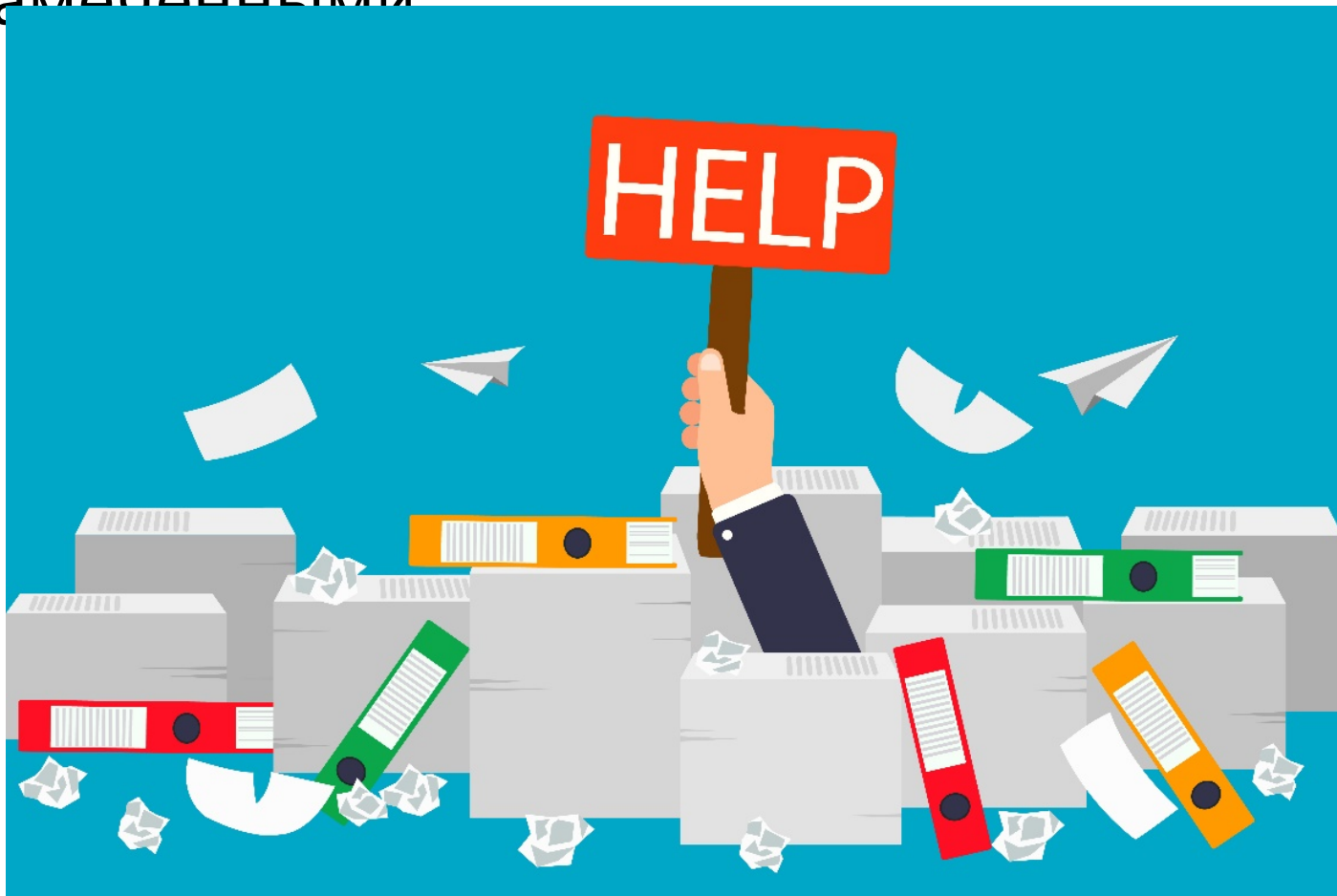
Advanced analytics for endpoint

Add advanced analytics

Add platform features

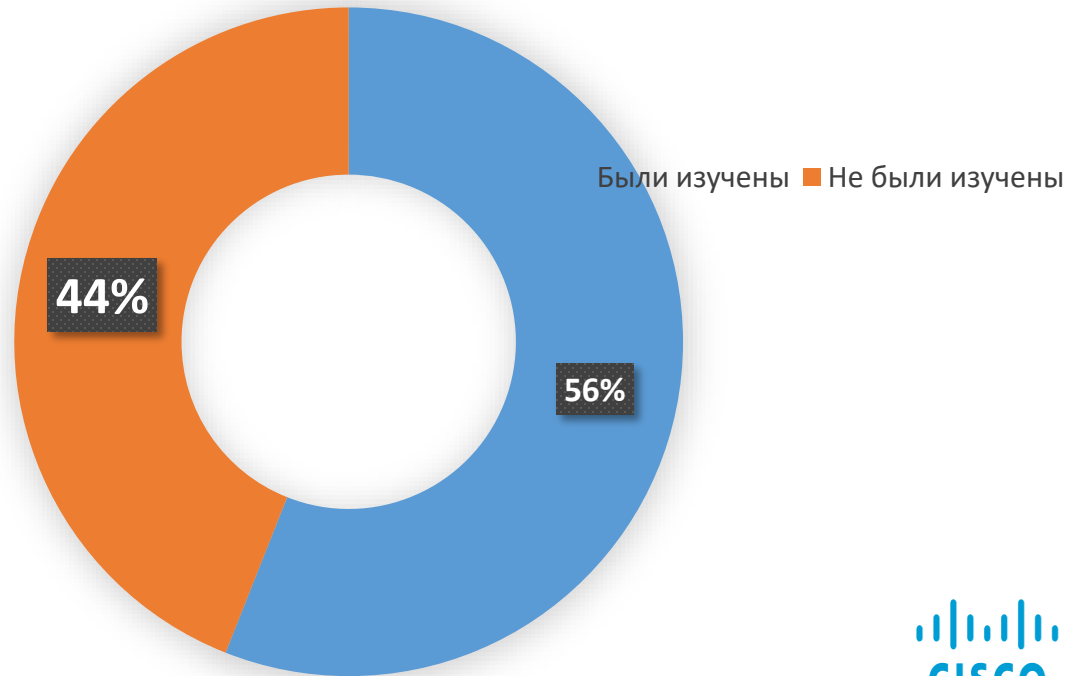


Важные события остаются не
замеченными

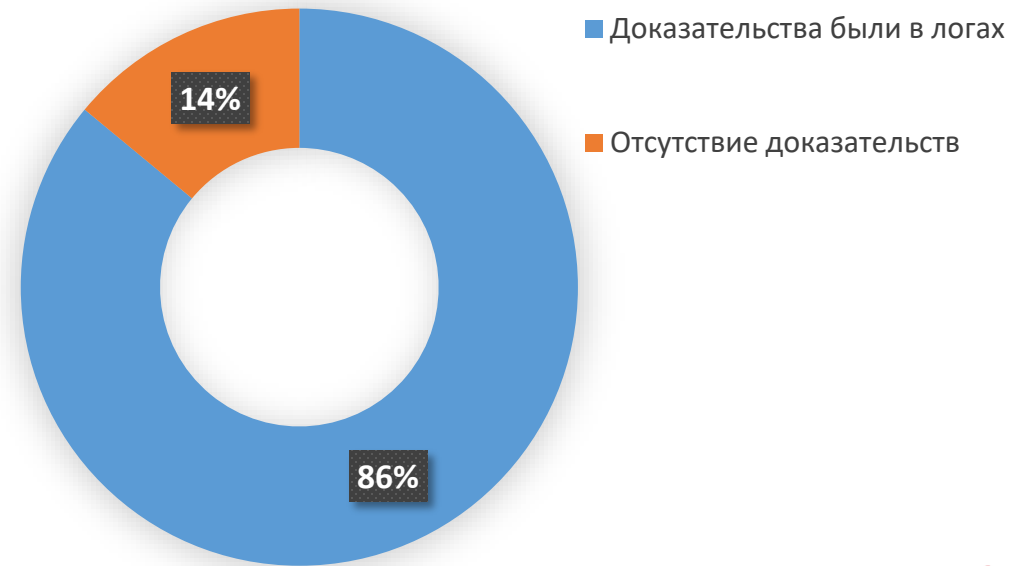


Средства ИБ
создают
«информационный
шум»!

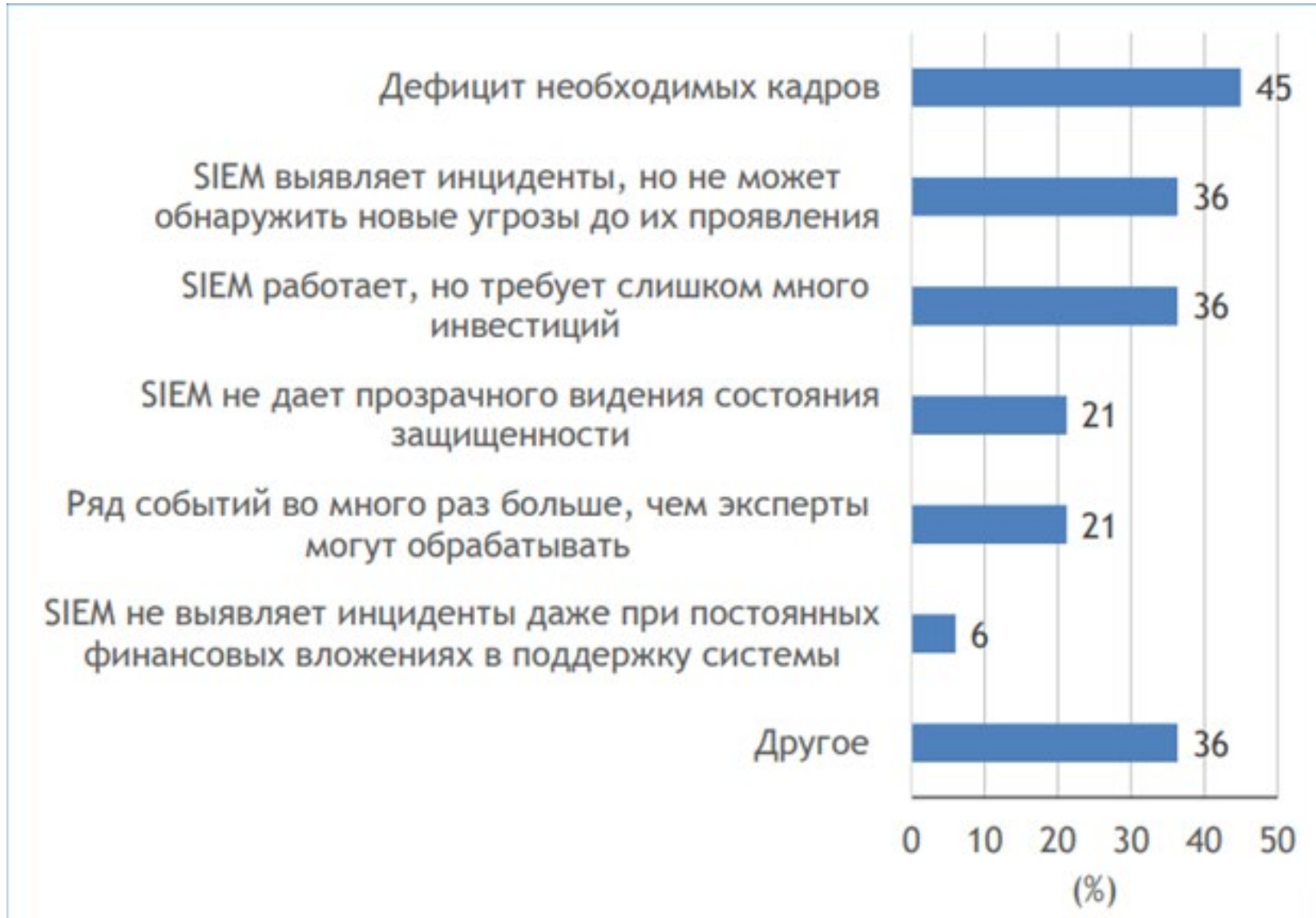
Предупреждения от средств ИБ



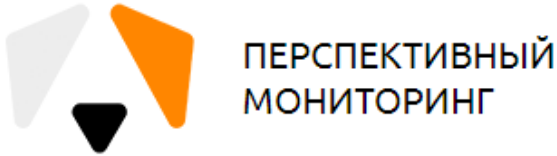
Причины утечек



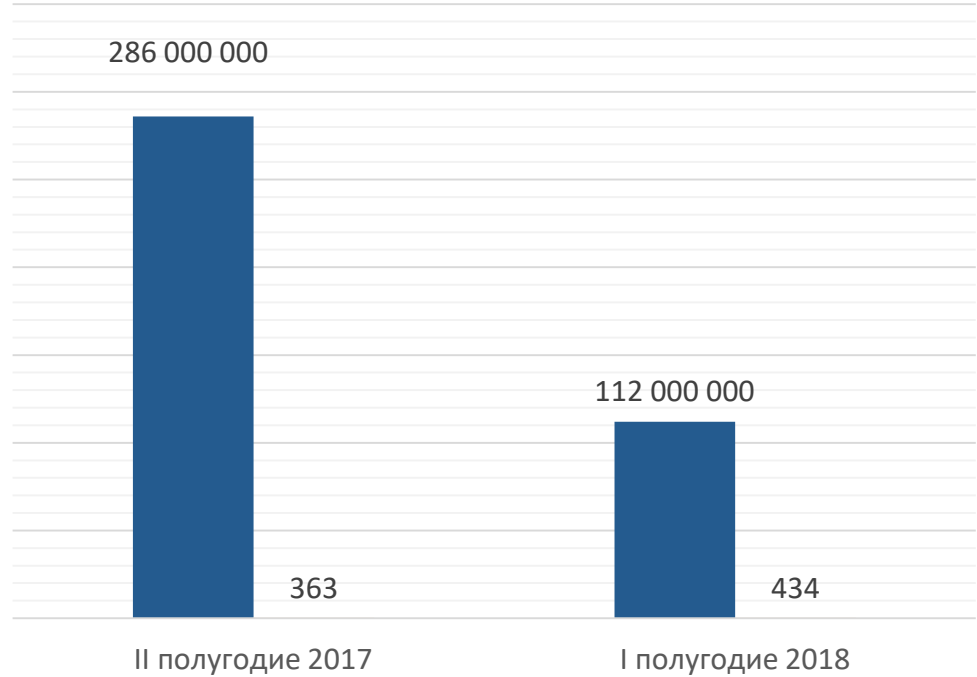
Причины неудовлетворенности системой SIEM



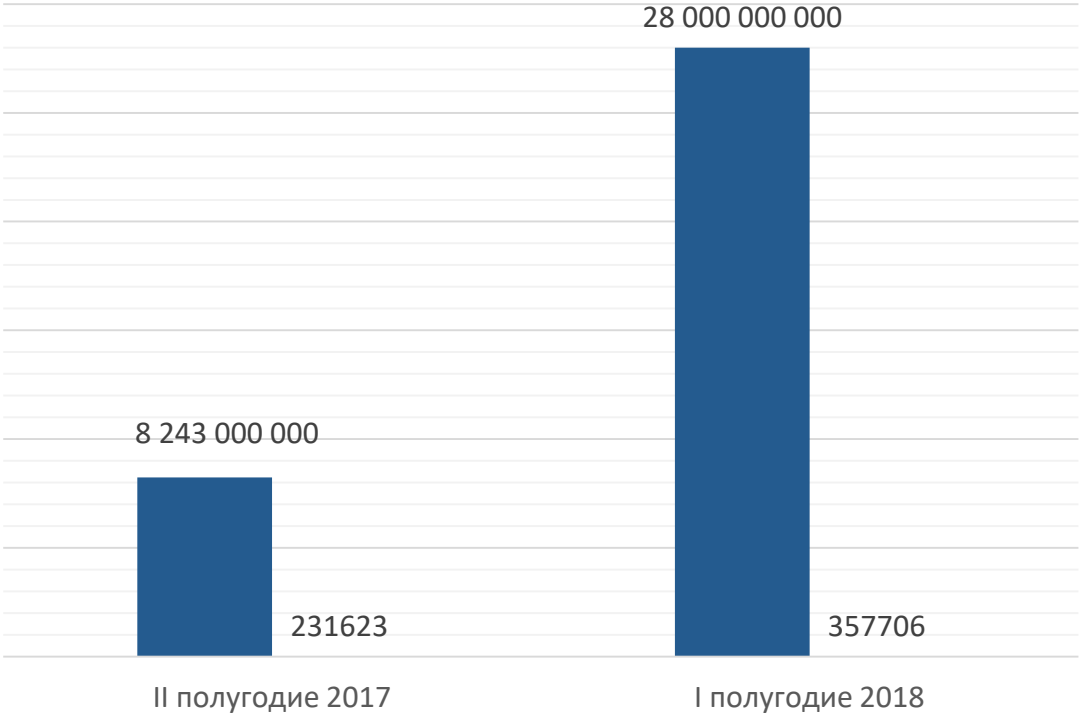
Сколько событий обрабатывает SOC?



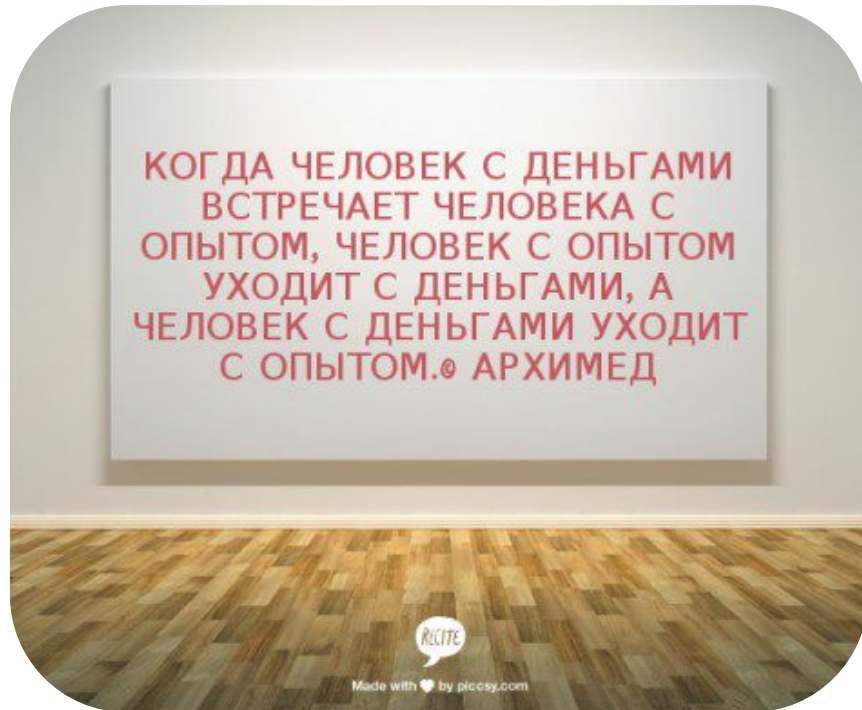
■ События ■ Инциденты



■ События ■ Инциденты




Что нужно



Экспертиза - опыт



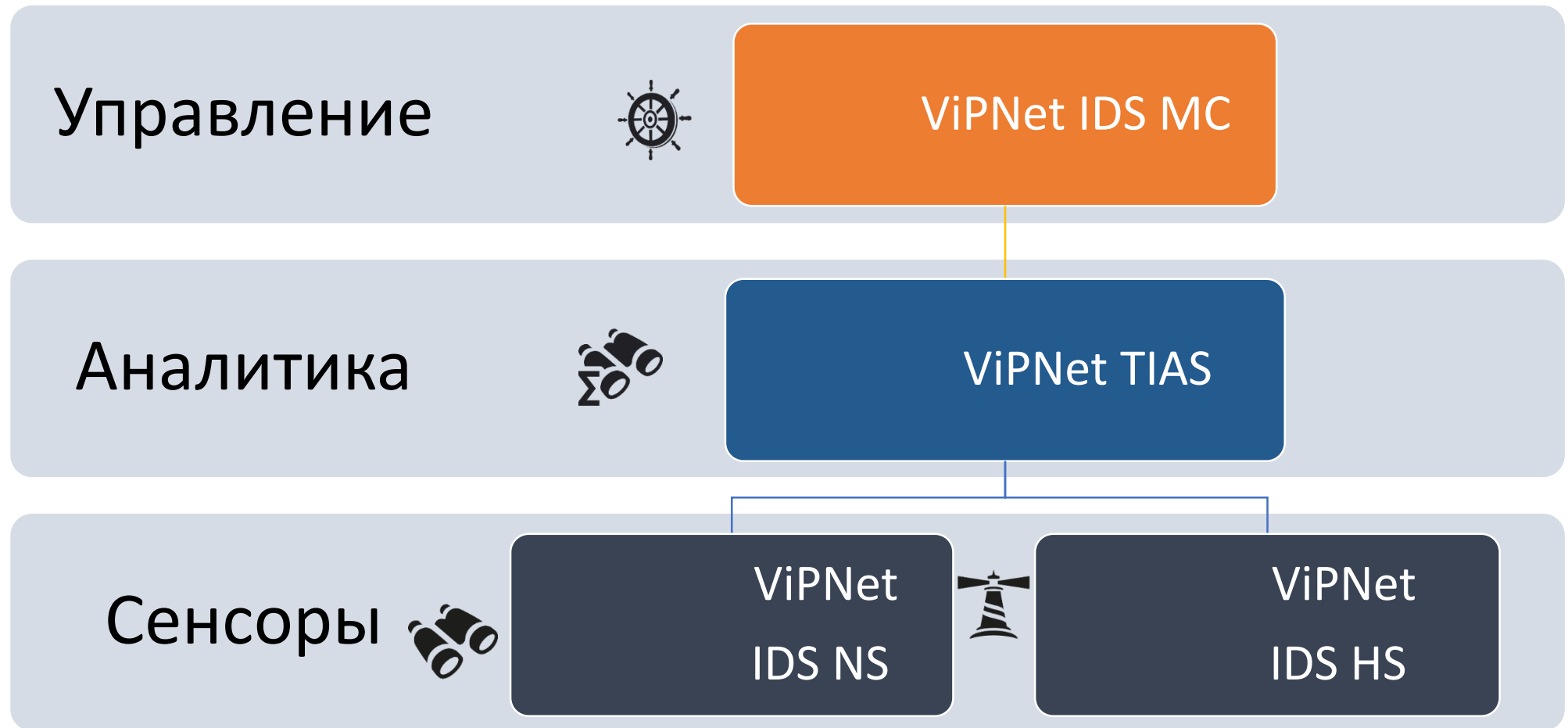
Автоматизация

A detailed 3D rendering of a white and blue robotic hand, shown from a side profile with the index finger pointing towards the left. The hand is highly articulated with visible joints and segments. The background is a dark, blurred space with faint, light-colored icons of various devices and network connections.

Решение от
ИнфотеКС

VIPNet

Решение по обнаружению угроз и вторжений



Решаемые задачи

Непрерывный
процесс анализа
событий

Адекватная
реакция на
произошедшие
события

Быстрое
устранение
последствий
инцидента

Извлечение
полезных уроков





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



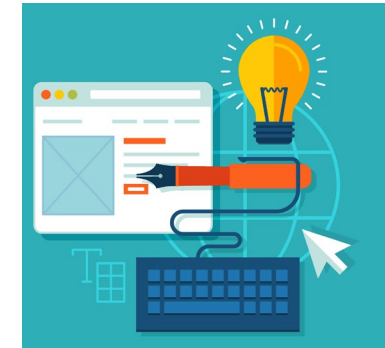
Как это работает?



События ИБ



Модуль анализа
ViPNet TIAS



Инциденты ИБ



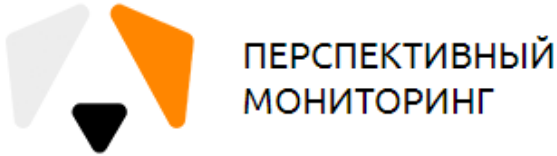
Статистика и
отчеты

Комбинирование двух методов

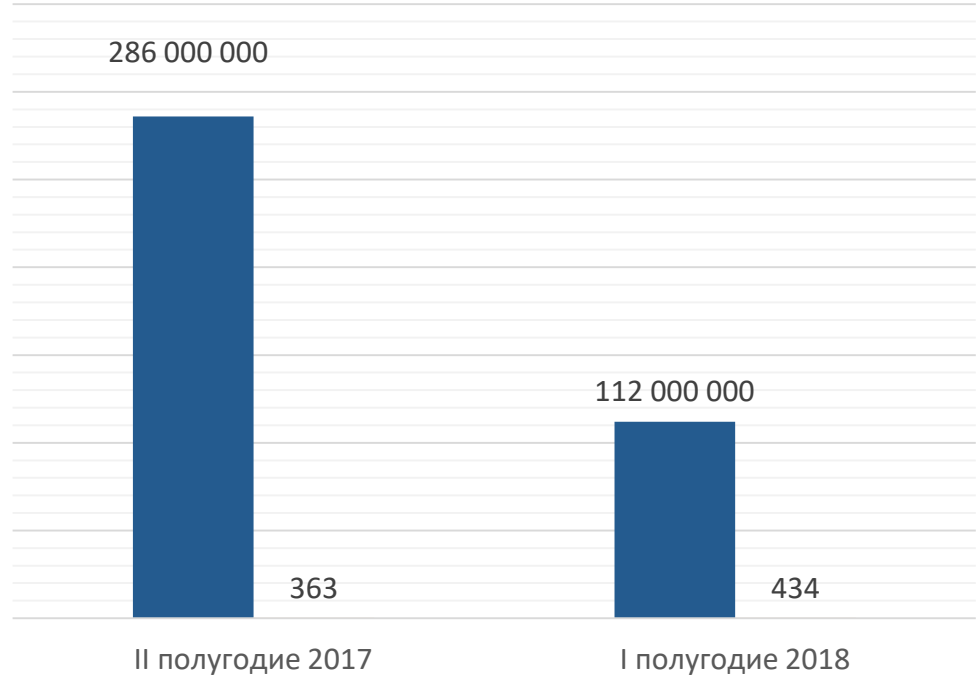
- ✓ **Сигнатурный метод** – на основе метаправил выявления инцидентов
- ✓ **Эвристический метод** – на основе машинного обучения математической модели принятия решений



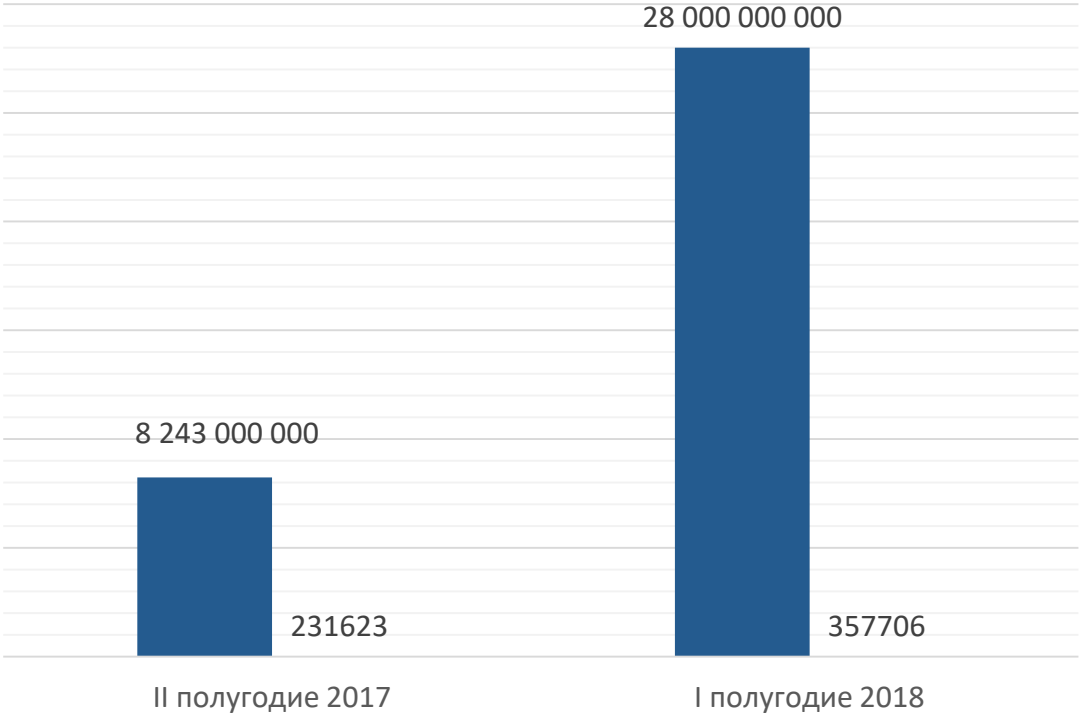
Сколько событий обрабатывает SOC?



■ События ■ Инциденты



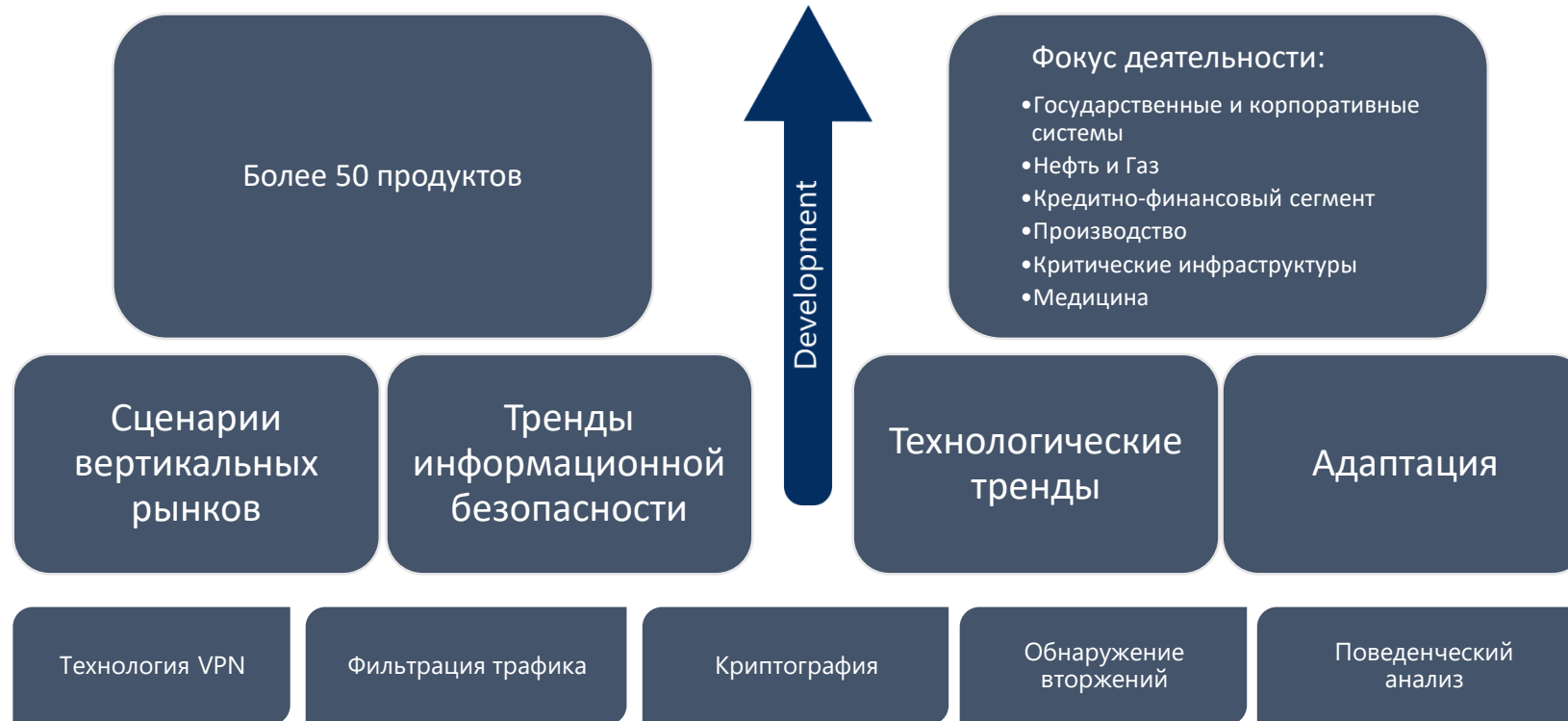
■ События ■ Инциденты



The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, a large high-voltage power line tower stands prominently. The sun is low on the horizon, creating a strong glow and casting long shadows. The overall scene conveys a sense of clean energy and infrastructure.

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 COB

Покрывает
все классы
атак

Покрывает
все уровни

Адаптивна к
неизвестным
атакам

Масштабируе
тся

Является
открытой

Имеет
встроенные
механизмы
реагирования

Является
защищённой
от атак на
компоненты
COB

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

