

ViPNet IDS. 5 причин купить сегодня

Алексей Данилов

Менеджер по развитию продуктов

danilov@infotecs.ru

Обнаружение атак в
режиме времени
близком к
реальному

Сигнатурный и
эвристический
модули

Оповещение об
атаках в Web-
интерфейсе и по e-
mail

Фиксация: время, IP
адрес, порт,
протокол,
критичность атаки,
IP-пакет

Интеграция с SIEM

Совершенная система обнаружения атак



Глазами потребителя

Удобство
пользования

Производительн
ость

100% выявление
атак

Отсутствие
ложных
срабатываний

Сертификация

Удобство пользования



The screenshot displays the VIPNet IDS web interface. A modal window titled "Событие 2015-07-30 19:17:53.015846" is open, providing details about a specific security event.

Источник	Событие	Получатель
10.0.14.175:52105 C8:60:00:C9:AD:A6 Частный IP-адрес	2015-07-30 19:17:53.015846 ET CHAT Skype VOIP Checking Version (Startup)	10.0.4.245:3128 00:08:E3:FF:FC:28 Частный IP-адрес

Событие

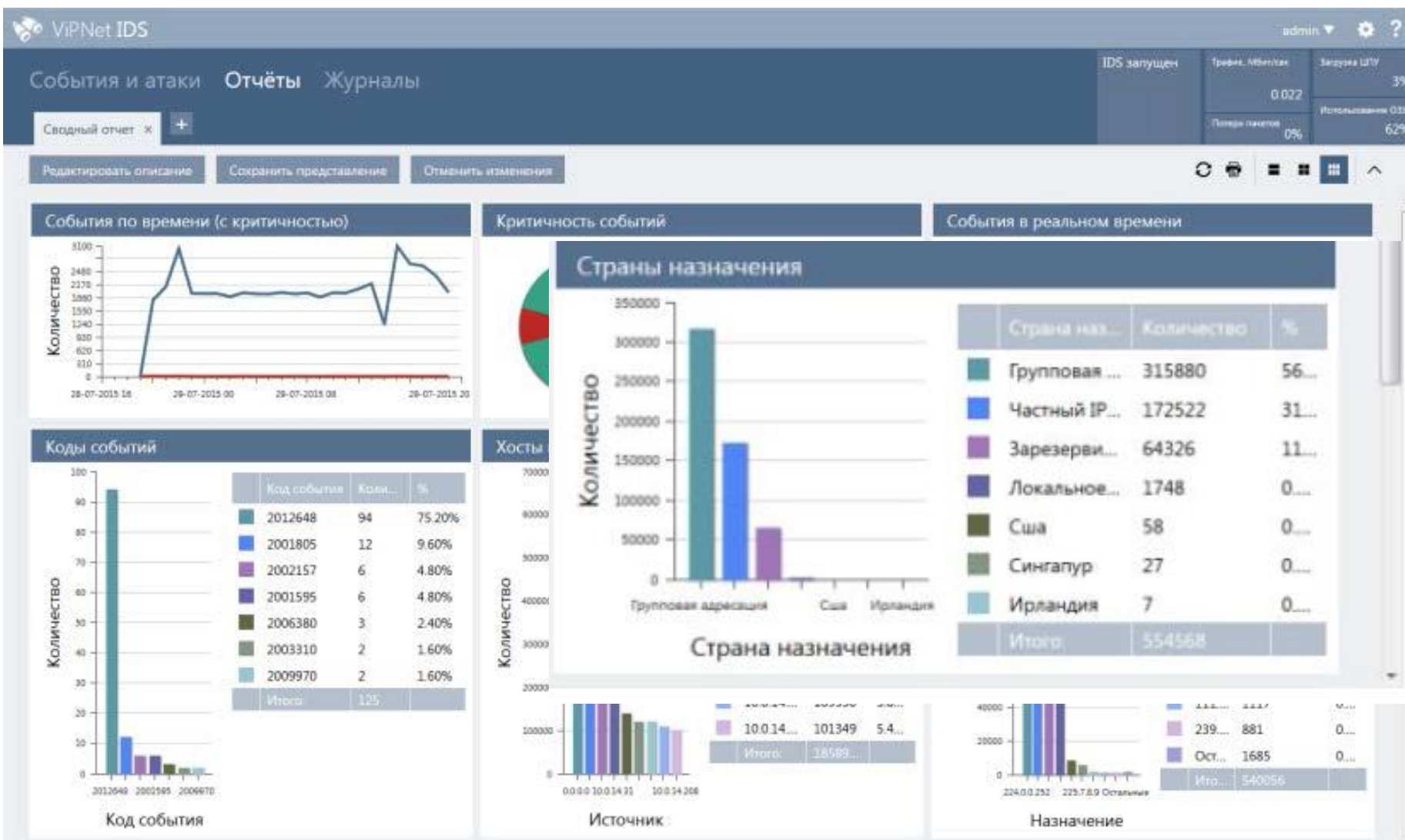
Дата, время получения:	2015-07-30 19:17:53.015846
Тип события:	Сигнальное событие
Протокол:	TCP
Код события:	2001595
Класс события:	policy-violation
Критичность события:	Высокая
Группа правил:	emerging-chat
Сработало правило:	ET CHAT Skype VOIP Checking Version (Startup)
Текст правила:	alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET CHAT Skype VOIP Checking Version (Startup)",flow,to_server,established,content:".ui"/http_uri,nocase,content:"getlatestversion?ver=".http_u r;/nocase,reference.url,www1.cs.columbia.edu/~library/TR-repository/re ports/reports-2004/cucs-039-04.pdf;reference.url,doc.emergingthreats.net/2001595;classtype:policy-violation,sid:2001595;rev:10)
Описание уязвимостей:	url: www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf url: doc.emergingthreats.net/2001595

Пакет

Смещение	Шестнадцатеричные данные	Описание
0000	00 08 E3 FF FC 28 C8 60 00 C9 AD A6 08 00 45 00	..âüç(È`·É!..E.
0010	00 E4 50 F6 40 00 7F 06 7D 99 0A 00 0E AF 0A 00	..âPø...)™....

In the background, a table lists recent events, all categorized as "Высокая" (High) severity and "policy-violation". The main dashboard shows system statistics like traffic volume (0.016 Mbit/sec) and CPU usage (5%).

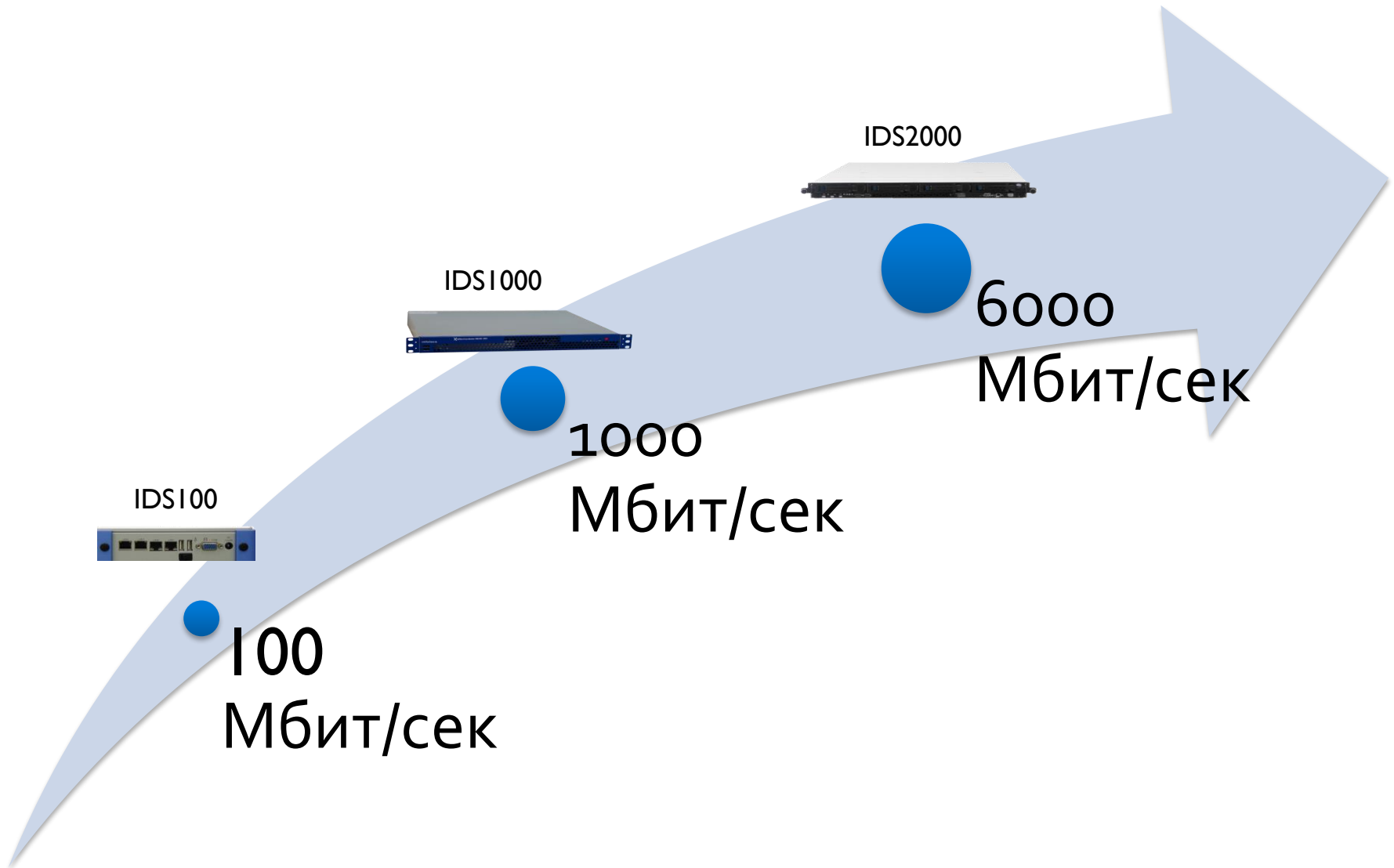
WEB-интерфейс: Статистика





Производительность

Варианты исполнения ViPNet IDS





Не все йогурты одинаково полезны



Поставщики сигнатур в мире и России

Cisco, SourceFire

- VRT, Cisco TALOS

CheckPoint, Код безопасности

- Emerging Threats (Pro версия)

StoneSoft

- StoneSoft



ИнфоТеКС

- Перспективный мониторинг

Актуальность

Отсутствие ложных срабатываний

Гибкая доработка под нужды заказчиков

Соответствие требованиям регуляторов

Сравнение поставщиков сигнатур атак

Cisco

32665

250-300 новых
сигнатур

ZeroDay сигнатуры

Страна
происхождения -
США 

ET

30034

300-400 новых
сигнатур

ZeroDay сигнатуры

Страна
происхождения -
США 

ИнфоТе КС

24866

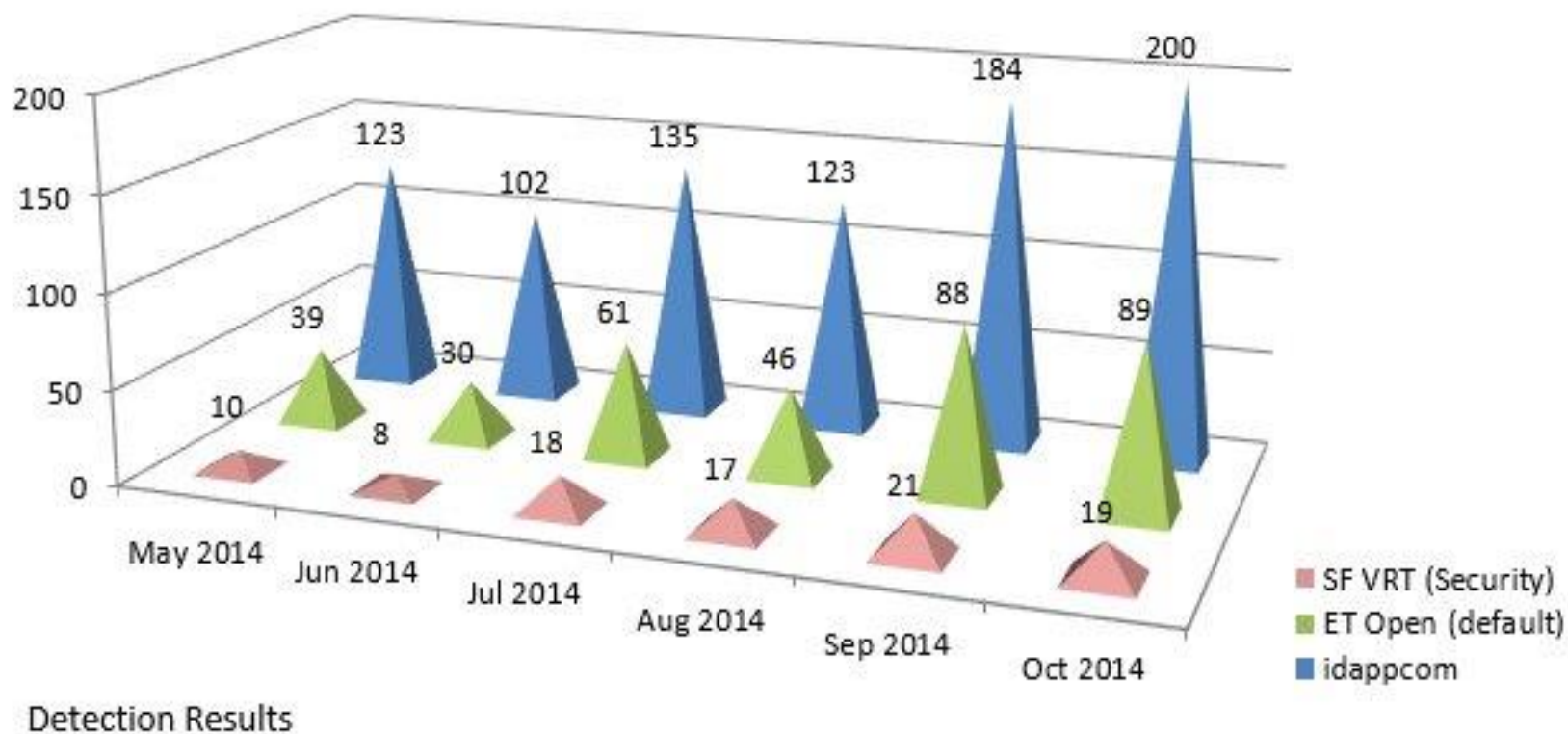
300-400 новых
сигнатур

ZeroDay сигнатуры

Страна
происхождения -
Россия 

Важно не количество, а качество сигнатур

Отчет компании idappcom о качестве сигнатур



План развития IDS

Релиз 2.4 (12.08.2015)

- GeoIP
- Статистика в формате Netflow
- IDS как виртуальное устройство
- Система обновления ПО

Релиз 2.5 (30.06.2016)

- Система выявления вредоносного ПО
- Performance optimization
- Система автоматического обновления БРП

ViPNet IDS
Management
Center (2 кв. 2016)

Система выявления вредоносного ПО -

ViPNet Malware Detection

Выявление в трафике файлов, включая PDF, Microsoft Office документы.



Анализ полученных файлов на наличие в них вирусов



Уведомление Администратора о выявленном вредоносном ПО



Сохранение файла в базе данных

ViPNet IDS Центр Управления версия 1.0

Графическая
консоль

Ролевая модель
доступа

Управление
лицензиями

Централизованн
ое управление
настройками

Обновление
сигнатур атак

УПРАВЛЕНИЕ

Мониторинг

Зарегистрированные сенсоры

Зарегистрированные сенсоры

StarK

Искать сенсор...

Наименование

☐ Все сенсоры☐ TLS☒ Hawaii☒ Marseille☐ Tokyo

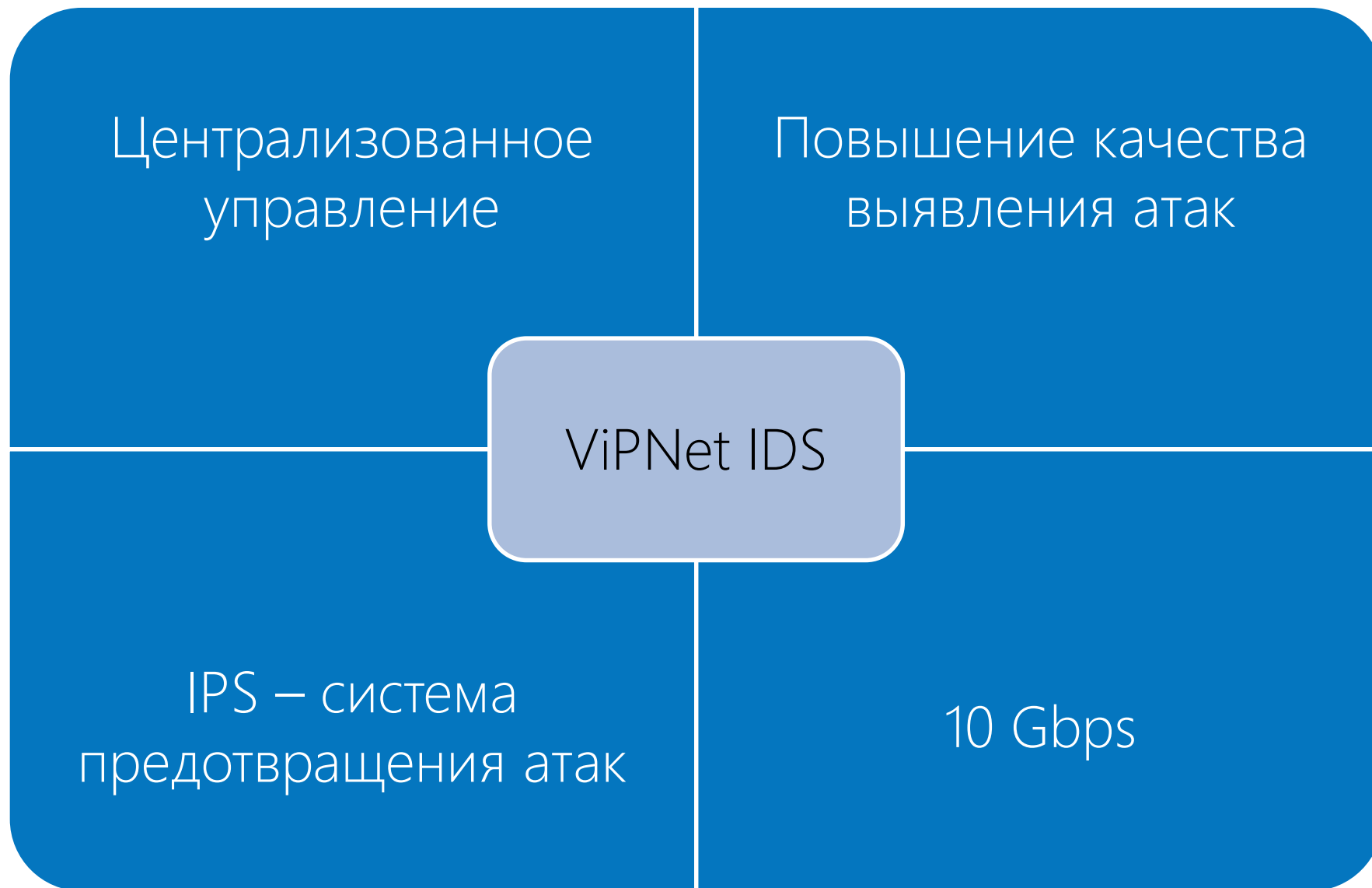
Рассылка обновления базы правил на сенсоры

Выбор базы правил

Искать обновление...

Дата создания	Источник	Загружено
07.08.2015 15:56:20		08.12.2015 19:25:06
11.09.2015 18:51:29		08.12.2015 19:25:29
☒ 17.11.2015 16:23:33		08.12.2015 19:25:47

ViPNet IDS: направления развития



Спасибо за внимание!
Вопросы?

Алексей Данилов
danilov@infotecs.ru
+7 (495) 737-61-92 (5113)