Актуальные сценарии и опыт защиты КИИ

Дурягин Сергей

США вводят санкции против 12 российских компаний

ВАШИНГТОН, 25 сентября 2018г. /ТАСС/. Министерство торговли США приняло решение ввести ограничения против 12 российских компаний, которые, с точки зрения Вашингтона, действуют вразрез с интересами национальной безопасности Соединенных Штатов.
В списки минторга США попали: … «ИнфоТеКС» …

Актуальные угрозы

Портал Правительства Оренбургской области

D:RUSSIA.RU Новости Темы и рубрики ПРОФ-IT О центре RSS

В регионах | Кибербезопасность | Электронное правительство

Хакер похитил с сайта правительства Оренбургской области обращения граждан и их персональные данные

Редакция - 25.05.2016

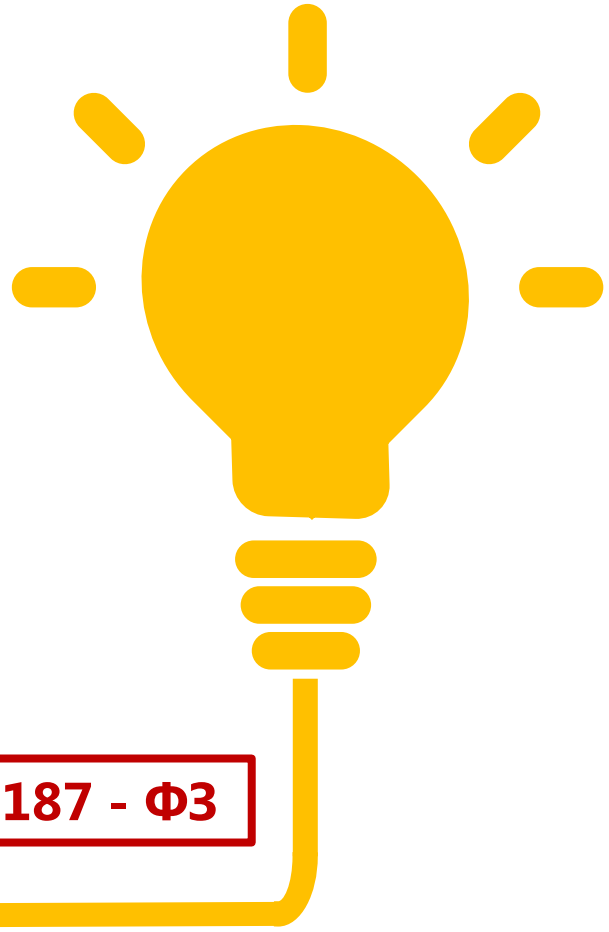
Сайт правительства Оренбургской области был взломан 23 мая. Ответственность за произошедшее взял на себя хакер под ником Ruh8, который разместил в открытом доступе тексты обращений граждан, отправлявшиеся через сайт, с именами и контактами

Что надо сделать?

01 **Категорирование объектов КИИ**
Присвоение категории в соответствии со значимостью объекта

02 **Обеспечение безопасности объекта КИИ**
Мероприятия по обеспечению безопасности КИИ и размещение на территории объекта КИИ ТЗКИ

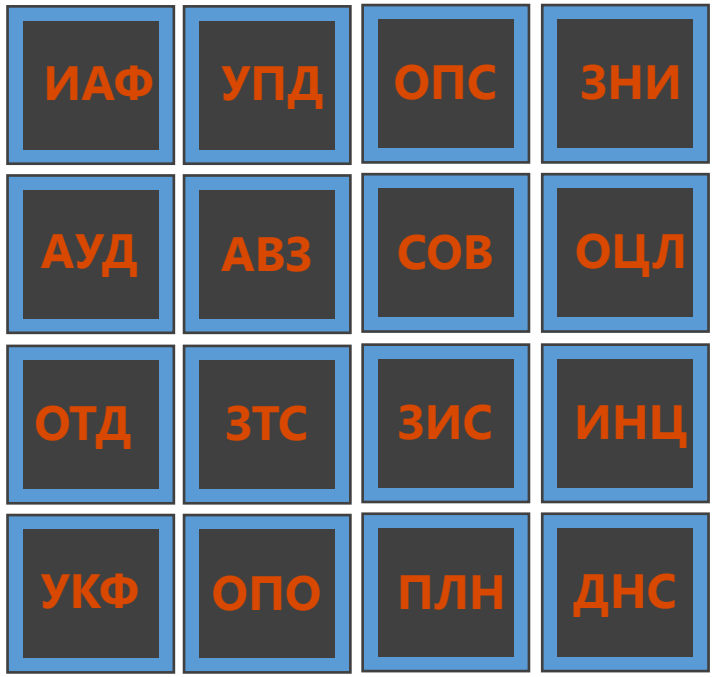
03 **Противодействие компьютерным атакам**
Взаимосвязь с ГосСОПКА, размещение на территории объекта КИИ ТЗИ ГосСОПКА



* **Состав мер по обеспечению безопасности для значимого объекта КИИ определен Приказом ФСТЭК России №239 от 25.12.2017г.**

Состав мер

В соответствии с Приказом ФСТЭК России №239 от 25.12.2017 г.



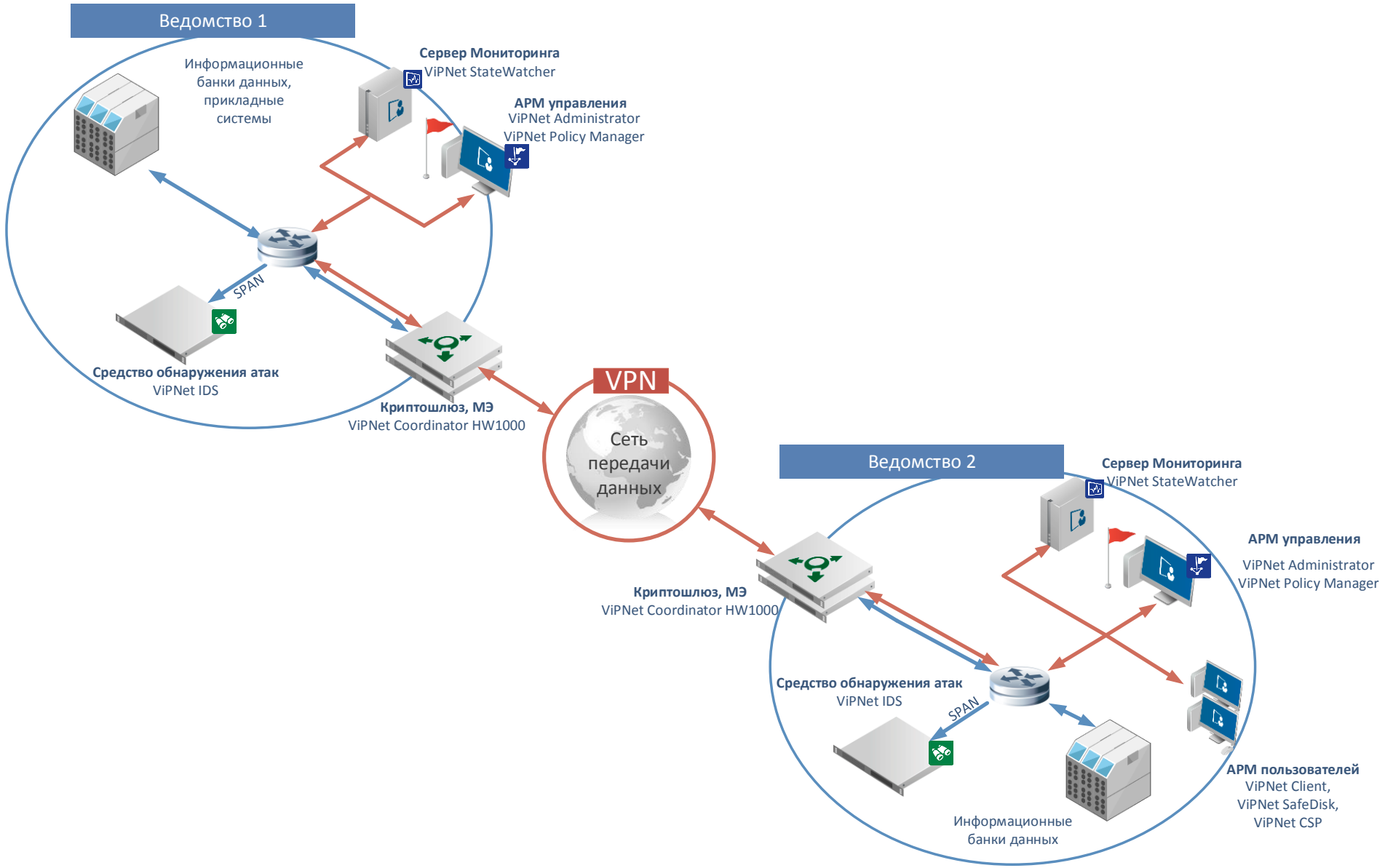
- идентификация и аутентификация (ИАФ)
- управление доступом (УПД)
- ограничение программной среды (ОПС)
- защита машинных носителей информации (ЗНИ)
- аудит безопасности (АУД)
- антивирусная защита (АВЗ)
- предотвращение вторжений (компьютерных атак) (СОВ)
- обеспечение целостности (ОЦЛ)
- обеспечение доступности (ОДТ)
- защита технических средств и систем (ЗТС)
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- планирование мероприятий по обеспечению безопасности (ПЛН)
- управление конфигурацией (УКФ)
- управление обновлениями программного обеспечения (ОПО)
- реагирование на инциденты информационной безопасности (ИНЦ)
- обеспечение действий в нештатных ситуациях (ДНС)
- информирование и обучение персонала (ИПО)

Основные решения и сценарии

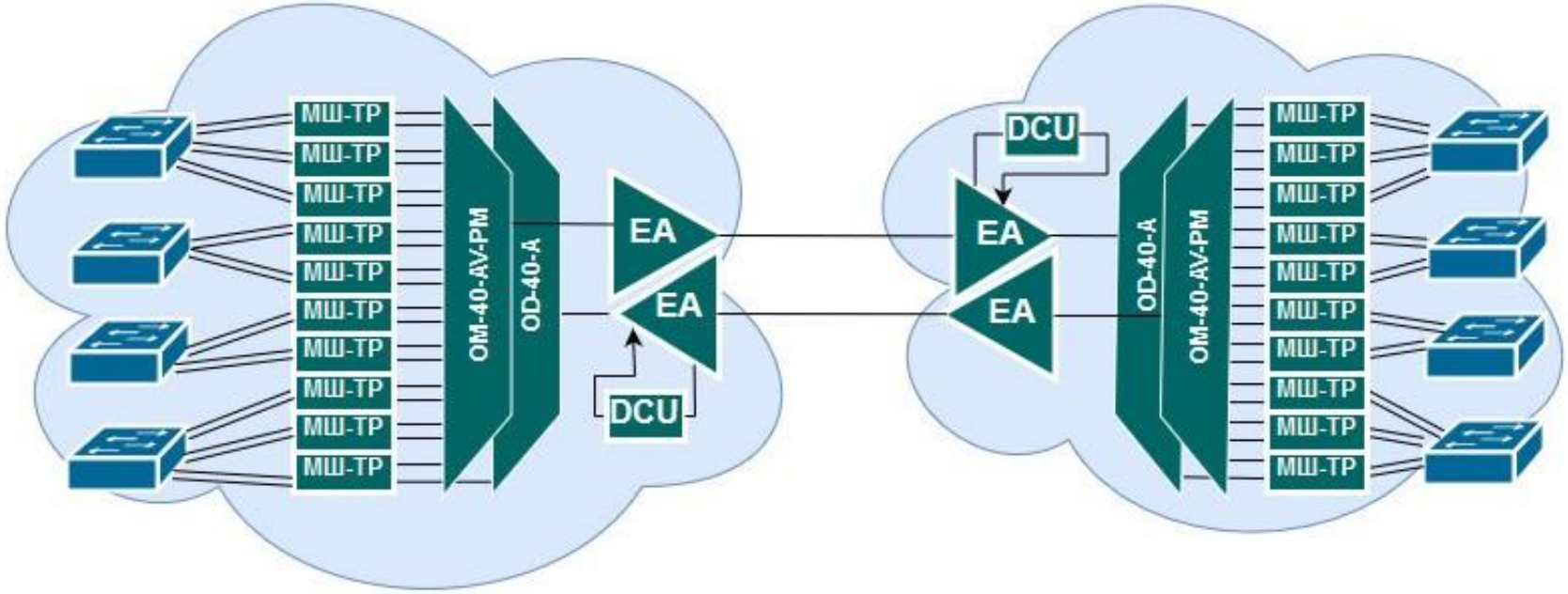
1. **Защита информации при передаче по каналам связи**
2. **Защита периметра, межсетевые экраны нового поколения**
3. **Защищенные мобильные решения**
4. **Защита аппаратных платформ, модули доверенной загрузки**
5. **Решения для АСУ ТП**
6. **Системы обнаружения и анализа компьютерных атак**

1. Защита информации при передаче по каналам связи

Классический VPN

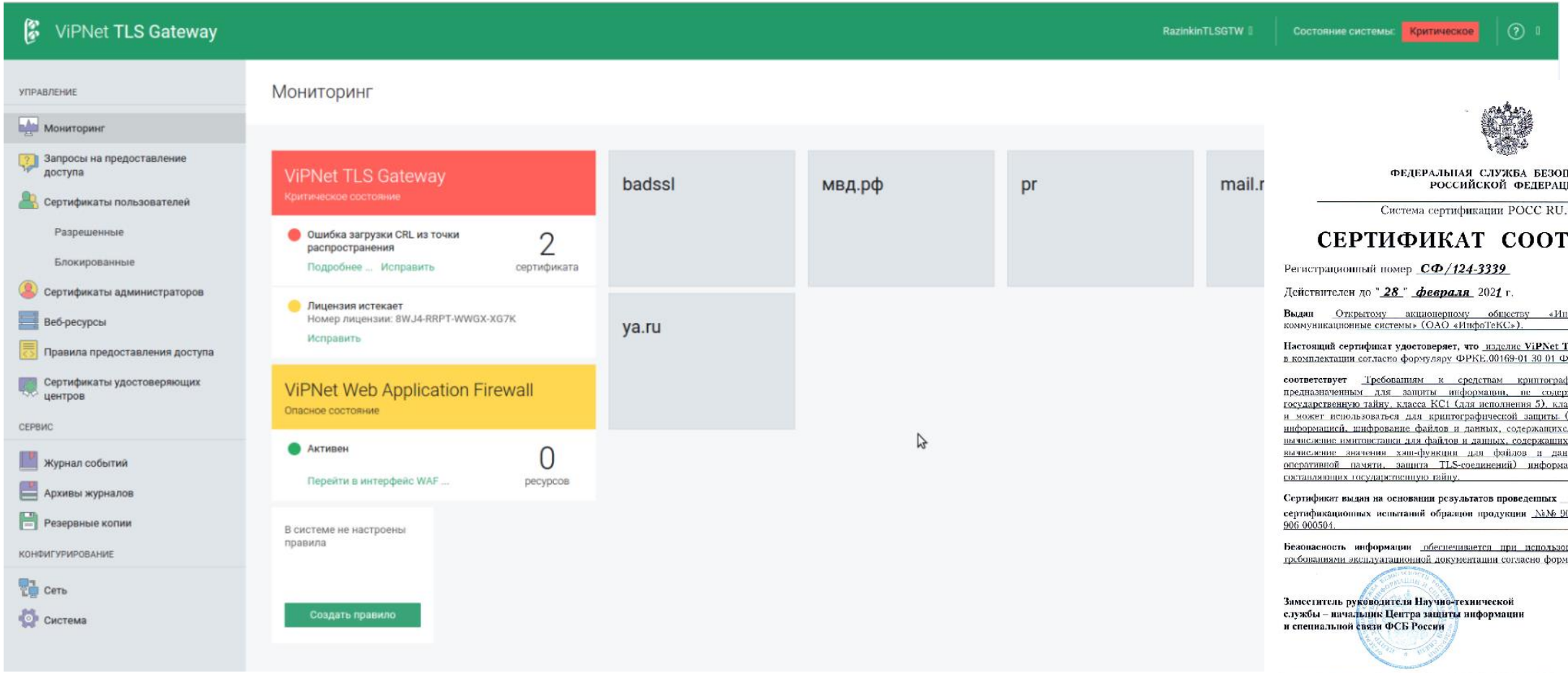


Решения уровня ЦОД-РЦОД:
ViPNet Квазар – защита OTN сетей



! Организация защиты канала до 100 Гбит/с

ViPNet TLS Gateway



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3339* от "*28*" *февраля* 2018 г.

Действителен до "*28*" *февраля* 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие **ViPNet TLS Gateway** (исполнения 1, 2, 3, 5) в комплектации согласно формуляру ФРКЕ.00169-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 5), класса КС3 (для исполнений 1, 2, 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» **сертификационных испытаний образцов продукции** №№ 906-000501, 906-000502, 906-000503, 906-000504.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00169-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России

Настоящий сертификат зарегистрирован в государственном реестре

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России

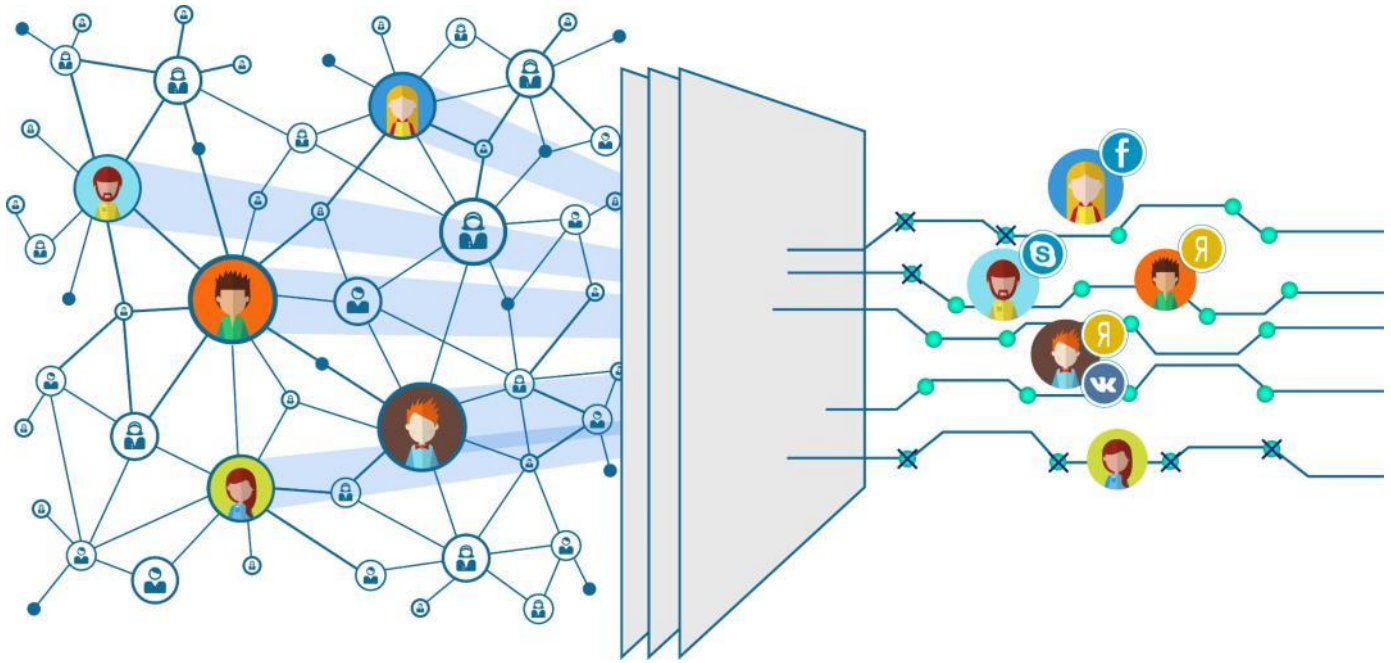
Легитимная работа с любым СКЗИ – TLS/SSL

Ключевые преимущества ViPNet TLS

- ✓ Работа с любым сертифицированным СКЗИ, поддерживающим TLS-соединение, на АРМ пользователя (КриптоПро CSP, ViPNet PKI Client и др.)
- ✓ Возможность применения бесплатного ViPNet CSP на стороне пользователя
- ✓ Одновременная работы с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012
- ✓ Класс СКЗИ до КС3
- ✓ Конструктор правил для группового разграничения прав доступа
- ✓ Автоматическая загрузка информации об аккредитованных УЦ с использованием Trusted Certificates List (TCL) Минкомсвязи РФ
- ✓ Наличие удобного клиента ViPNet PKI Client (кросс-браузерность, работа с CRL, туннелирование TCP, шифрование, ЭП)

2. Защита периметра, межсетевые экраны нового поколения

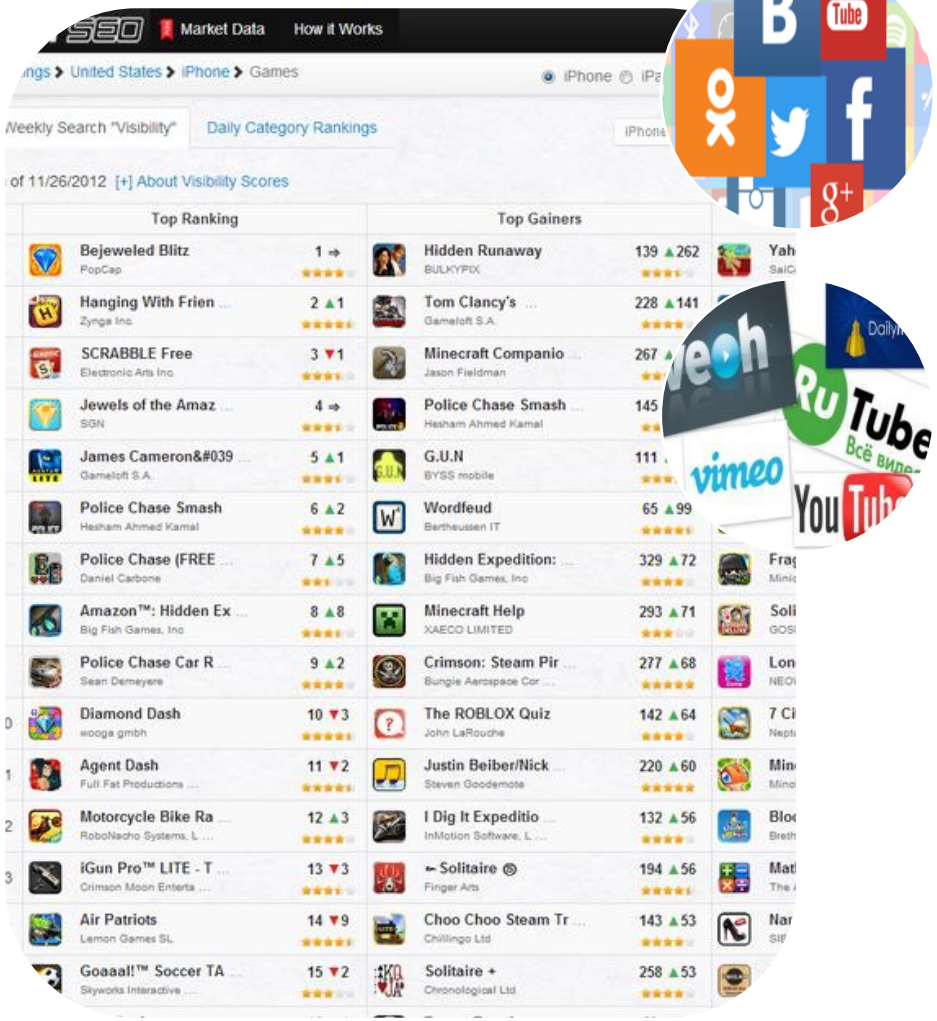
ViPNet xFirewall



Положительные свойства DPI

- Максимальная видимость трафика на 7 уровне (OSI)
- Защита от сетевых атак – блокировка аномалий, запретных команд
- URL-фильтрация – выявление трафика приложений web 2.0

2065 – уникальных приложений/протоколов приложений



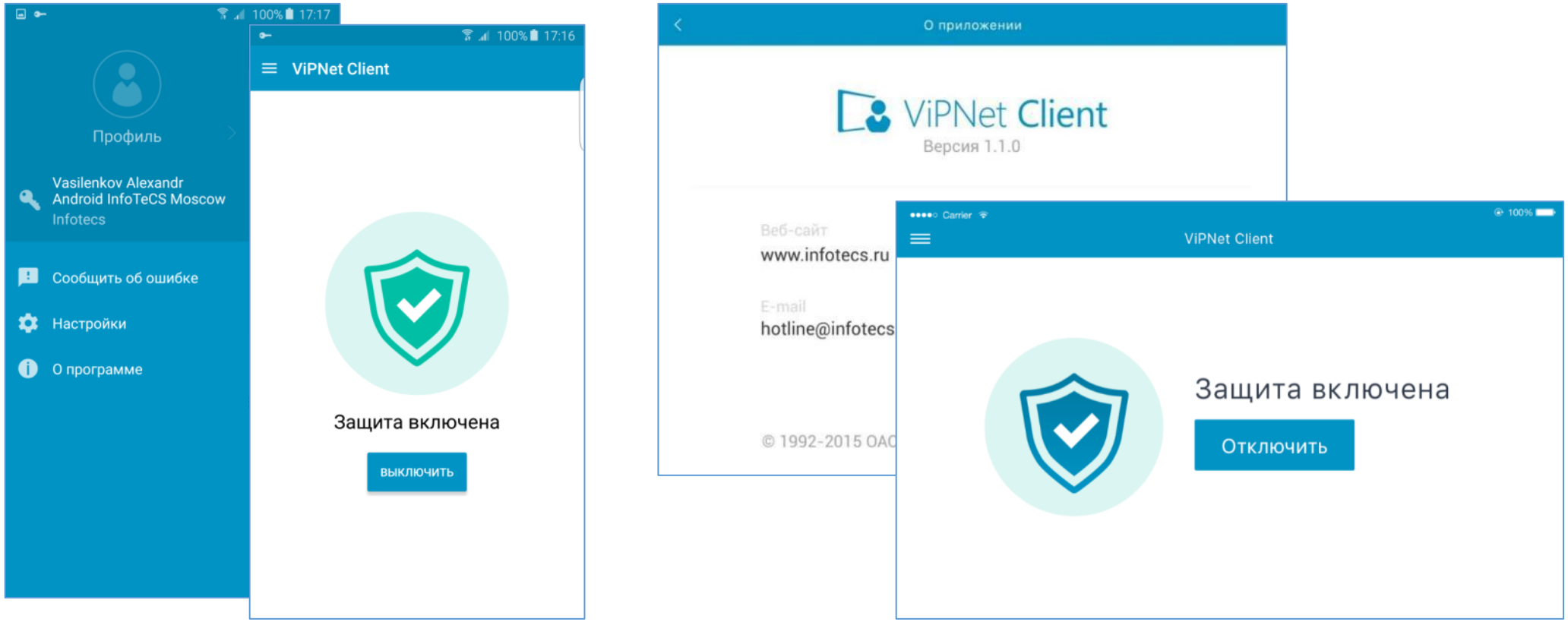
95 из категории «Социальные сети»

45 – потоковое видеовещание

3. Защищенные мобильные решения

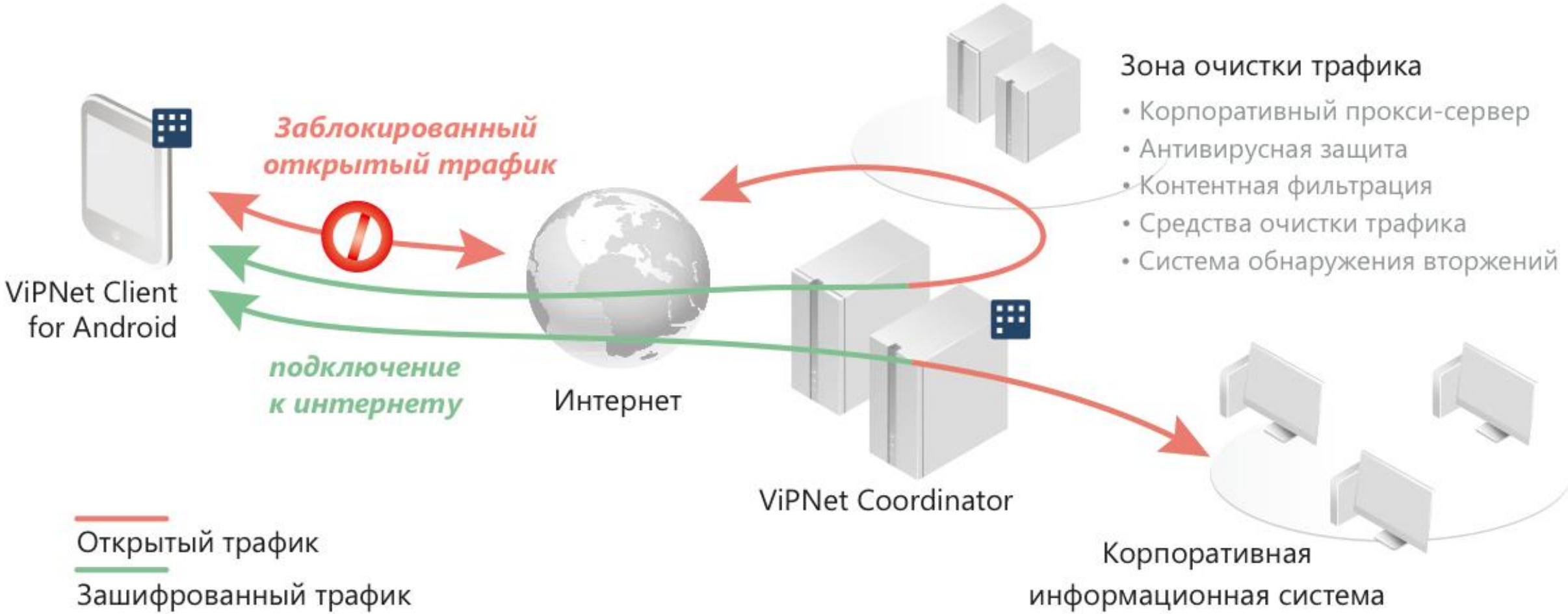
ViPNet Client для мобильных устройств

ViPNet Client for iOS, Android и Sailfish



- VPN (ГОСТ), Сертификат ФСБ

Доверенный интернет на мобильном устройстве



4. Защита аппаратных платформ, модули доверенной загрузки

ViPNet SafeBoot

Программный модуль доверенной загрузки

Устанавливается в UEFI BIOS различных производителей

Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS

Сертифицирован как средство доверенной загрузки уровня базовой системы ввода-вывода **второго** класса С возможностью использования в ИСПДн до УЗ1 включительно и в ГИС до 1-го класса защищенности

Ключевые особенности

- Поддержка UEFI BIOS на различных платформах
- Возможность программного обновления замка
- Возможность установки в элементы виртуальной инфраструктуры
- Возможность создания шаблонов настройки для удобства ввода в строй парка АРМ
- Отсутствие «железной составляющей»:
  - ✓ Меньше цена продукта
  - ✓ Экономия на логистике

Сравнение по ценам:

ПО ViPNet SafeBoot	ПАК "Соболь". Версия 3.0, PCI. Inc. TS Basic lvl	(СДЗ) Dallas Lock
5 000 руб.	**10 350 руб.**	**10 400 руб.**

5. Решения для АСУ ТП

Решения ViPNet для индустриальной безопасности

ViPNet Coordinator IG10.

Индустриальный шлюз безопасности полевого уровня (10 Мбит/с)

- **Поддержка промышленных протоколов: EtherNet/IP, Modbus TCP, PROFINET, DNP, IEC 60870-5-104, MMS, OPC, LonWorks, bacnet**
- **ARM-платформа**
- **Безвентиляторный дизайн**
- **Рабочая температура: -20^{0}C … +60^{0}C**
- **IP30**
- **Напряжение питания: 10…30 V DC**
- **Крепление на din-рейку**
- **50x120x120 мм, 0.6 кг**
- **ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24**

ViPNet SIES Server.

Высокопроизводительный криптосервер

- **Высокая производительность по выполнению криптографических операций (до 58 000 операций в секунду)**
- **Защищенное хранение ключей информации для нескольких устройств автоматизации**
- **TSP-сервер (подпись меток времени), OCSP-сервер (подпись OCSP-ответов), SSL-шлюз**
- **Работа прикладных сервисов АСУ ТП в защищенной среде**
- **SIES API**

ViPNet SIES Core & ViPNet SIES Pack.

Индустриальный криптомодуль

ViPNet SIES Core

SOM, 64x36 мм

ViPNet SIES Pack

Блочное исполнение с разъемами типа M12

- **Реализация криптоалгоритмов ГОСТ (шифрование, имитозащита, ЭП)**
- **Управление ключами защиты**
- **Доступ к криптографическим функциям (SIES API)**
- **Поддержка промышленных интерфейсов**
- **Индустриальное исполнение (-40… +60C, IP66, индустриальный диапазон питания)**

Защита АСУ ТП: ViPNet IG-10 & ViPNet SIES

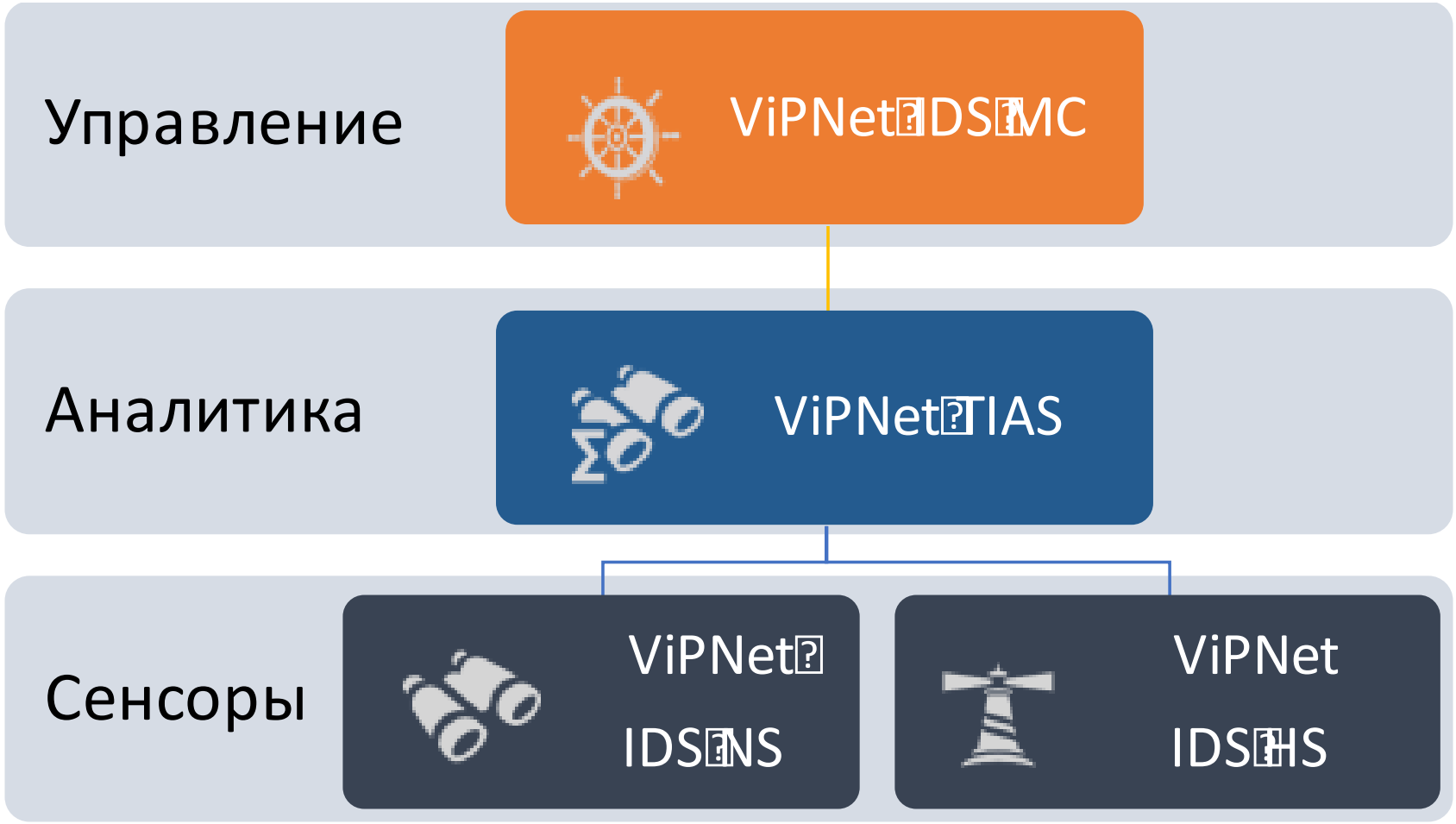
Задачи:

- Защита каналов связи в промышленных системах
- Аутентификация команд оператора при передаче по каналам связи
- Аутентификация данных на контроллере при передаче по каналу связи
- Логирование действий оператора и обеспечение неотрекаемости

6. Системы обнаружения и анализа компьютерных атак

Решения ViPNet

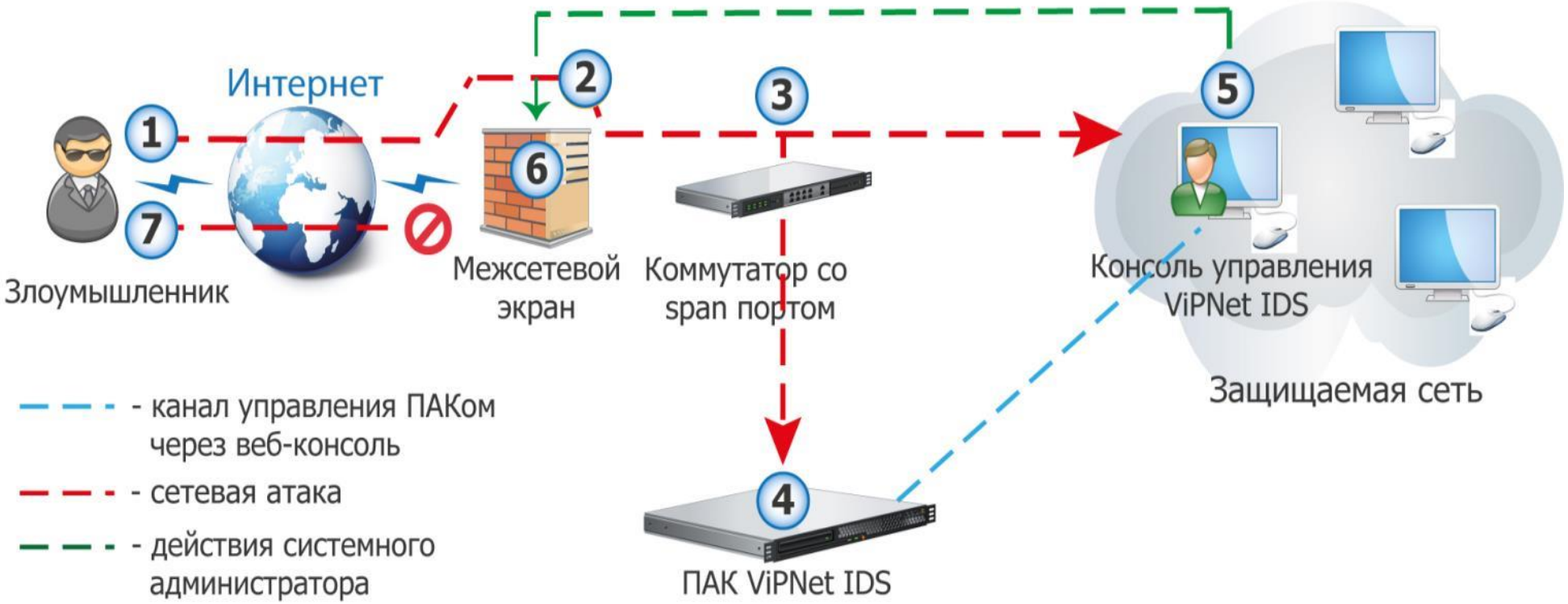
для обнаружения и анализа вторжений в информационные системы



Решения ViPNet

для обнаружения и анализа вторжений в информационные системы

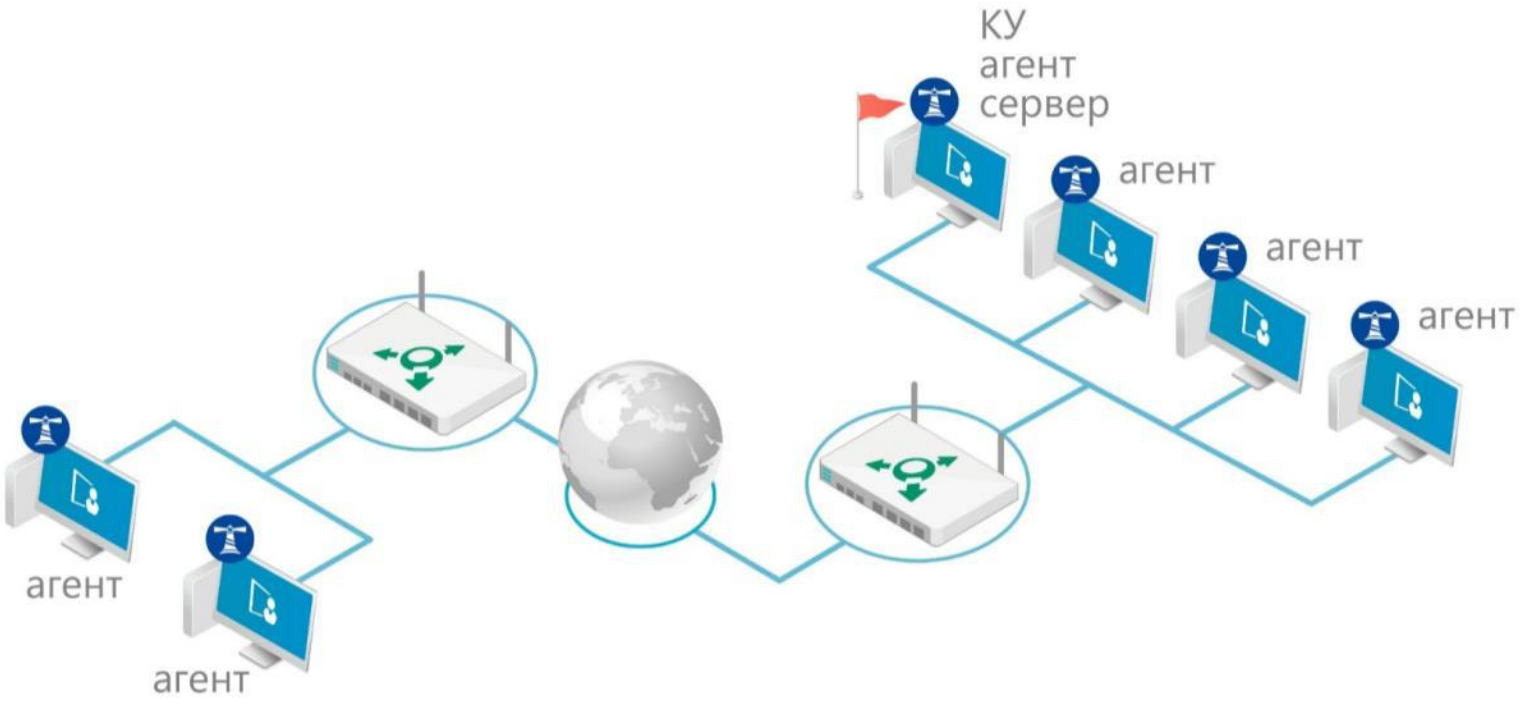
ViPNet IDS NS – система обнаружения компьютерных атак сетевого (канального) уровня, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры



Решения ViPNet

для обнаружения и анализа вторжений в информационные системы

ViPNet IDS HS - мониторинг и обработка событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры

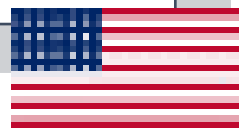


ИнфоТеКС – ключевой участник рынка поставщиков сигнатур атак

Cisco

(VRT, Talos)

- 32665
- 250-300 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США



ET

(Emerging Threats Pro)

- 30034
- 300-400 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США

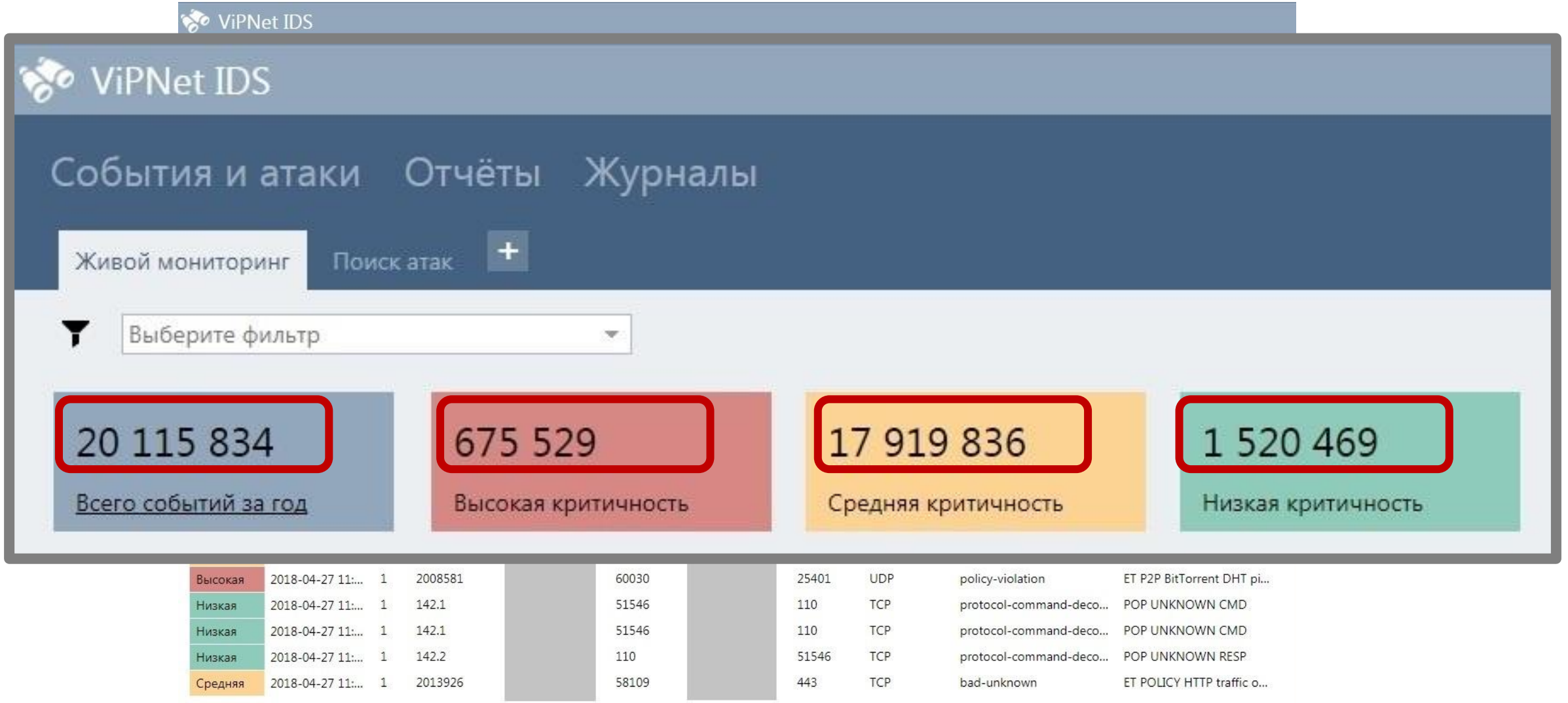
~~StoneSoft~~

ИнфоТеКС

(AM Rules)

- 24866
- 300-400 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: Россия

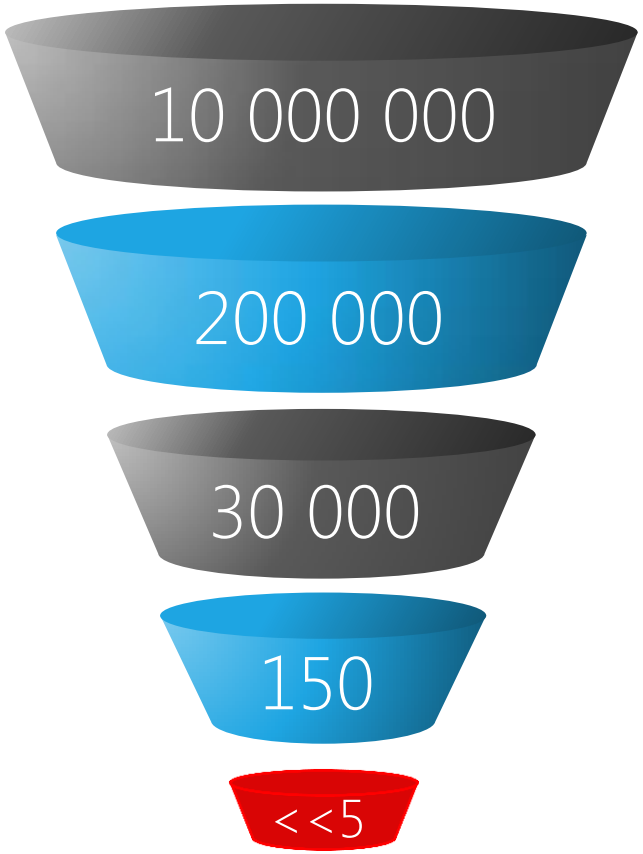
Система обнаружения вторжений



Высокая	2018-04-27 11:...	1	2008581		60030		25401	UDP	policy-violation	ET P2P BitTorrent DHT pi...
Низкая	2018-04-27 11:...	1	142.1		51546		110	TCP	protocol-command-deco...	POP UNKNOWN CMD
Низкая	2018-04-27 11:...	1	142.1		51546		110	TCP	protocol-command-deco...	POP UNKNOWN CMD
Низкая	2018-04-27 11:...	1	142.2		110		51546	TCP	protocol-command-deco...	POP UNKNOWN RESP
Средняя	2018-04-27 11:...	1	2013926		58109		443	TCP	bad-unknown	ET POLICY HTTP traffic o...

Обнаружение и анализ атак

Месячная статистика для организации ~500 АРМ, 10 Серверов



События информационной системы

События сенсоров ИБ

Важные ИБ-события

Критичные события ИБ

Инциденты ИБ

Настройка ViPNet IDS NS, IDS HS

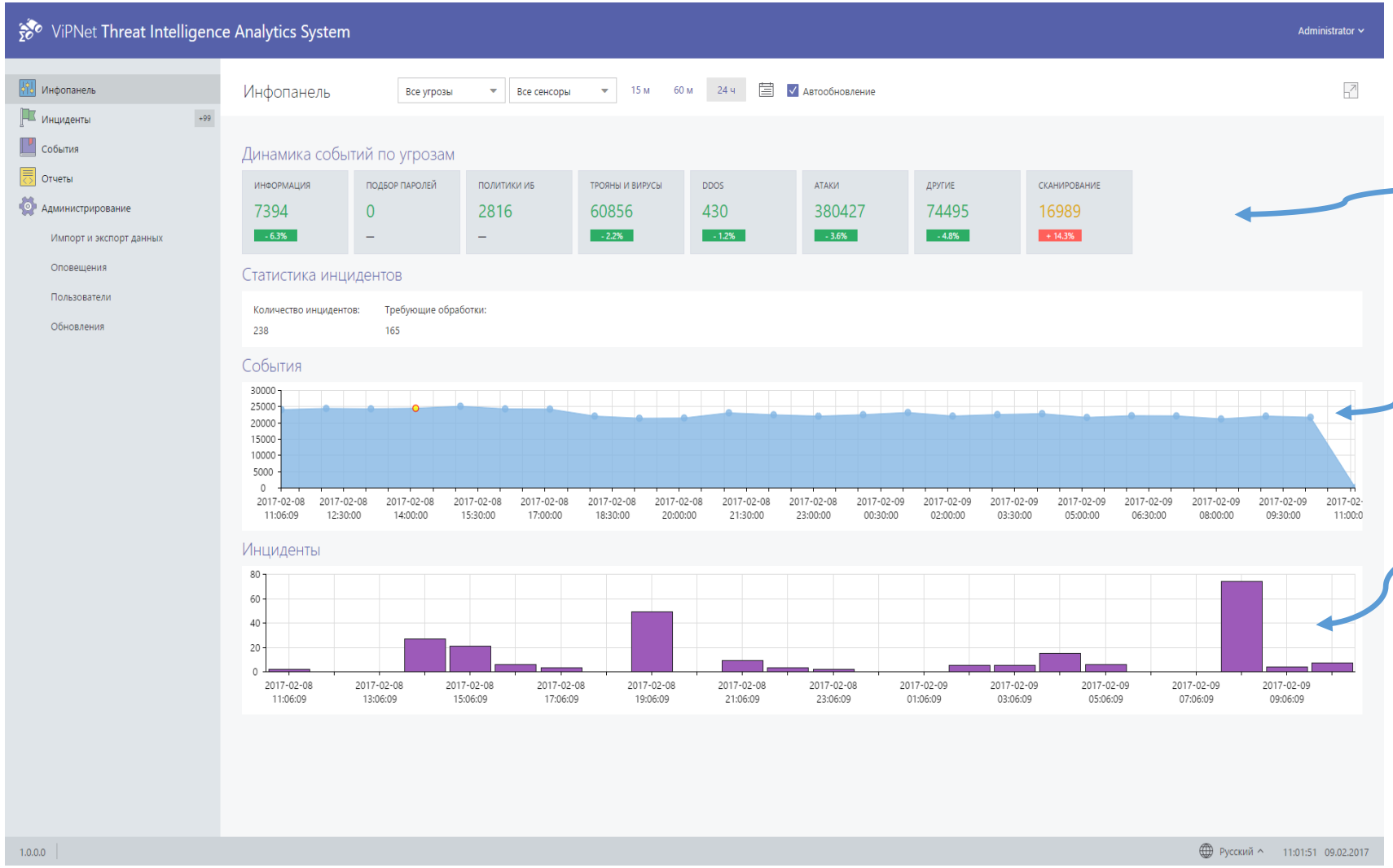
ViPNet TIAS

- Обработка поступающих событий
- Выявление критичных событий

- Аналитическая работа специалистов ЗАО «Перспективный мониторинг»

ViPNet TIAS

Понятное представление информации об угрозах и инцидентах



Динамика

События

Инциденты

Регистрация инцидентов

Понятное представление информации об угрозах и инцидентах

Инцидент

10 **#576bcf7b1d41c8000ca91be3**

Воздействие

Внутренний сегмент
1 пораженный узел

Дата фиксации

2016-06-23 15:00:59

Использование RPC portmap для amplification-атаки

Зафиксирована атака Portmap DDoS Amplification с использованием контролируемого ресурса. Атака проводится с использованием 111 порта (RPC) и заключается

Пораженные активы

Выявлено 1 пораженный узел:

msk-03-dd

User: User
ip: 91.244.183.8
mac: 00:15:5d:04:dd:18

Методы воздействия

Нарушение доступности
Нарушение неотказуемости

Симптомы

Аномальный рост исходящего трафика

Реагирование на инциденты

Устранение причин инцидентов

Пораженные активы

Выявлено 1 пораженный узел:

Методы воздействия

Нарушение доступности
Нарушение неотказуемости

Симптомы

Аномальный рост исходящего трафика

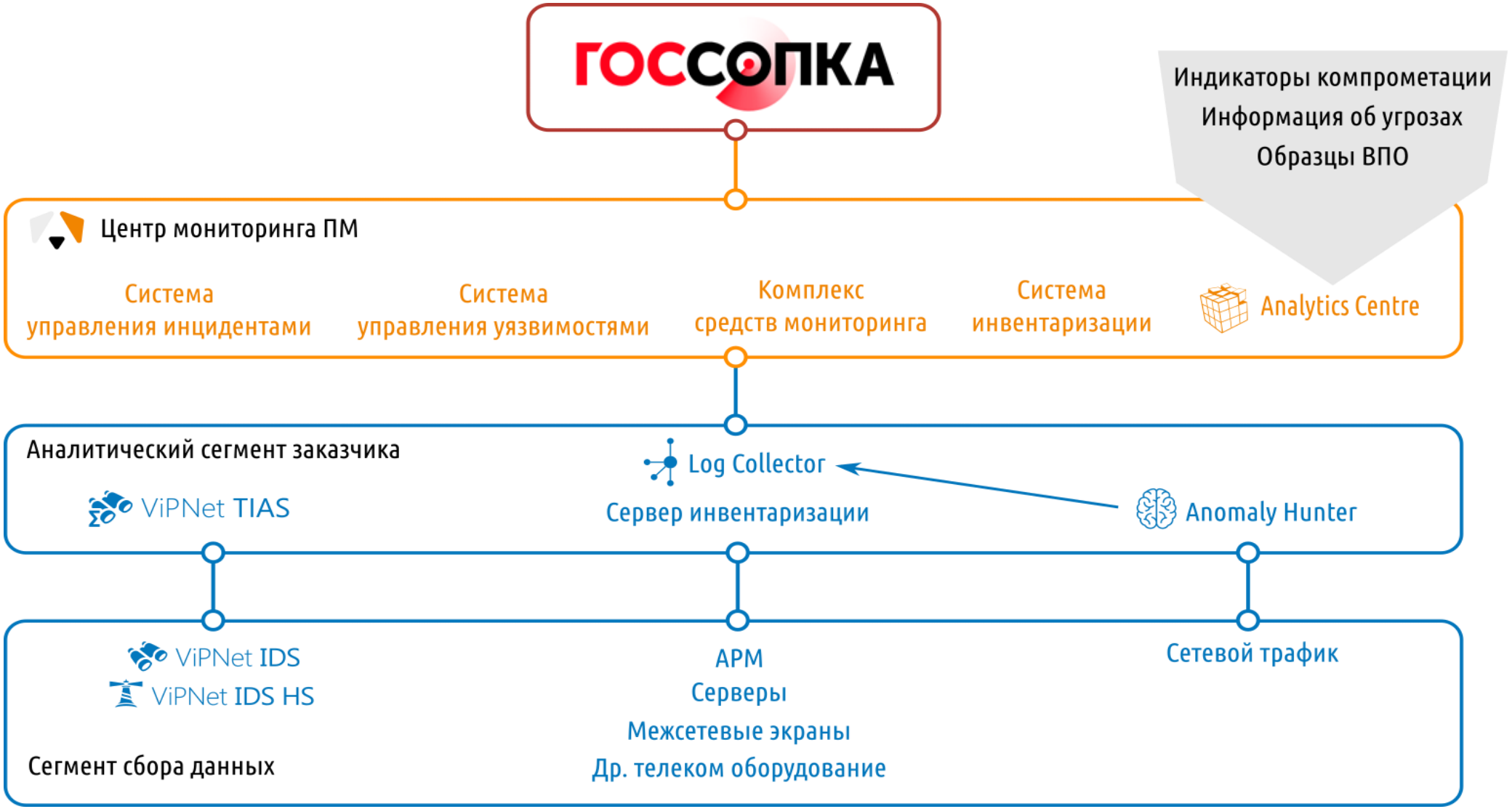
msk-03-dd

User: User
ip: 91.244.183.8
mac: 00:15:5d:04:dd:18

Рекомендации

- Закрыть доступ к portmapper из внешней сети
- Настроить portmapper на фильтрацию запросов от недоверенных источников
- Отключить зараженный компьютер от сети

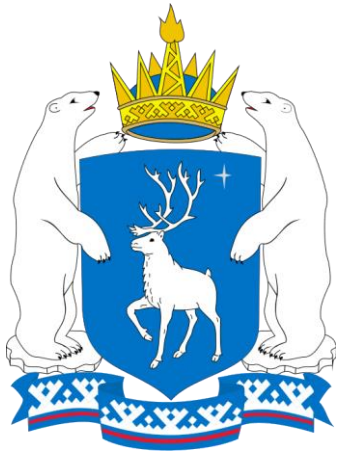
ЗАО «Перспективный мониторинг»



Услуги центра мониторинга
ООО "Перспективный мониторинг" (ГК ИнфоТеКС)

№	Линия	Перечень работ	Мониторинг	ГосСОПКА
1	**Первая линия**	Настройка и эксплуатация технических средств и систем Центра мониторинга	+	+
		Анализ данных о событиях информационной безопасности	+	+
		Регистрация инцидентов	+	+
		Приём обращений о возможных инцидентах от персонала и пользователей информационных ресурсов Заказчика	+	+
		Реагирование на инциденты и ликвидация их последствий	+	+
2	**Вторая линия**	Инвентаризация информационных ресурсов (узлов)	-	+
		Установление причин инцидентов	+	+
		Выявление уязвимостей информационных ресурсов	-/+	+
		Анализ угроз информационной безопасности	-	+
		Обнаружение компьютерных атак	-	+
		Взаимодействие с НКЦКИ	-	+
		Отчёт по инцидентам	+	+
3	**Третья линия**	Log Collector	-	+
		Выявление ранее неизвестных компьютерных атак	+	+
		Анализ вредоносных файлов, трафика, реверс-инжиниринг в ходе обработки инцидента	+	+
		Анализ исходного кода	-	+
		Подготовка методической базы	-	+
		Форензика	+	+

Услуги центра мониторинга
ООО "Перспективный мониторинг" (ГК ИнфоТеКС)



ЯНАО

Краснодарский край

Оренбургская область

Саха - Якутия

Смоленская область

Варианты подключения к технической инфраструктуре НКЦКИ

Вариант 1

Сеть ViPNet - 10976

Варианты подключения к технической инфраструктуре НКЦКИ

Вариант 2

При такой схеме подключения возможно будет организовать взаимодействие с использованием средств автоматизации (API)

Сеть ViPNet - 10976

Варианты подключения к технической инфраструктуре НКЦКИ

Вариант 3

Посредством использования уже действующей (собственной) сети ViPNet

Направить запрос на e-mail: gov-cert@gov-cert.ru и rea@gov-cert.ru в котором указать необходимую информацию для подготовки файла межсетевой информации

Доступ к странице авторизации личного кабинета осуществляется по адресу: https://portal.cert.local

Сеть ViPNet - 10976

Сергей Дурягин
DSA@infotecs.ru
+7 (964) 796-37-29