

Искусственный интеллект на страже безопасности. Решение ViPNet для предотвращения угроз и вторжений

Светлана Старовойт

Проблемы

- Рост количества событий ИБ
- Нехватка специалистов по ИБ
- Устаревшие инструменты



©2017, ОАО «ИнфоТеКС».


События ИБ

Определения

- **Событие информационной безопасности** - Идентифицированное появление определенного состояния системы, сервиса или сети, указывающее *на возможное* нарушение политики ИБ или отказ защитных мер, или возникновение ранее неизвестной ситуации, которая *может иметь отношение* к безопасности



- **Инцидент информационной безопасности** - появление *одного или нескольких* нежелательных или неожиданных событий ИБ, с которыми связана *значительная вероятность* компрометации бизнес-операций и создания угрозы ИБ.

ГОСТ Р ИСО/МЭК ТО 18044—2007

©2017, ОАО «ИнфоТеКС».

Отчет ПМ за 1 полугодие 2017

Нарушение политик	Подбор паролей	DDoS атака	Вредоносный трафик	Эксплуатация уязвимостей



- **15 500 узлов мониторинга**
- **392 326 588 событий ИБ**
- **242 инцидента**

Cisco внешний SOC

- **200 млрд. событий**
- **7 млн. угроз**
- **7 тысяч инцидентов**

Два клиента Cisco SOC (I квартал) :



©2017, ОАО «ИнфоТеКС».

4 из 10 не расследованы



©2017, ОАО «ИнфоТеКС».



Ресурсы

Работа аналитика SOC



©2017, ОАО «ИнфоТеКС».

Статистика

Мировой рынок:

Спрос специалистов ИБ вырастет до 6 млн вакансий уже к 2019 году,

прогнозируемый дефицит — 1,5 миллиона специалистов»

45% российских компаний говорят о дефиците специалистов по информационной безопасности

Зарплата 1 специалиста по ИБ в год:

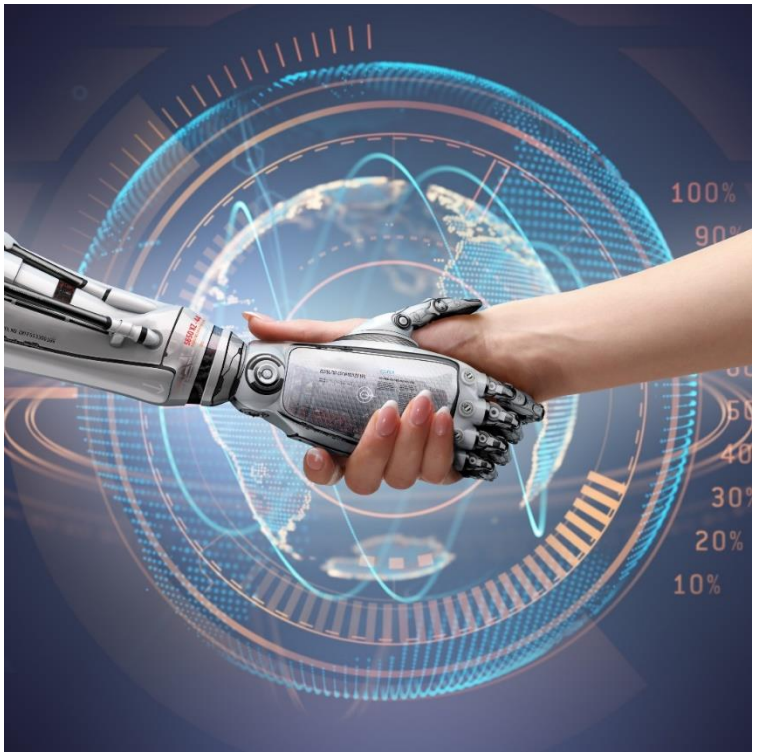
60x12x40%=1 200 000 рублей

Регион	Диапазон I (без опыта работы специалистом по информационной безопасности)	Диапазон II (с опытом работы от 1 года)	Диапазон III (с опытом работы от 2 лет)	Диапазон IV (с опытом работы от 3 лет)	Медиана (средняя заработная плата)
Москва	35 000–50 000	50 000–70 000	70 000–100 000	100 000–150 000	80 000
Санкт-Петербург	28 000–40 000	40 000–55 000	55 000–80 000	80 000–120 000	64 000
Волгоград	18 000–25 000	25 000–35 000	35 000–48 000	48 000–70 000	38 000
Воронеж	18 000–25 000	25 000–35 000	35 000–50 000	50 000–75 000	40 000
Екатеринбург	20 000–32 000	32 000–45 000	45 000–65 000	65 000–95 000	51 000
Казань	18 000–25 000	25 000–35 000	35 000–50 000	50 000–75 000	40 000
Красноярск	20 000–30 000	30 000–40 000	40 000–55 000	55 000–85 000	46 000
Нижний Новгород	18 000–28 000	28 000–40 000	40 000–55 000	55 000–85 000	44 000
Новосибирск	20 000–32 000	32 000–45 000	45 000–65 000	65 000–95 000	50 000
Омск	18 000–25 000	25 000–35 000	35 000–50 000	50 000–75 000	40 000
Пермь	20 000–28 000	28 000–40 000	40 000–55 000	55 000–85 000	46 000
Ростов-на-Дону	20 000–30 000	30 000–40 000	40 000–57 000	57 000–85 000	45 000
Самара	20 000–30 000	30 000–40 000	40 000–55 000	55 000–85 000	46 000
Уфа	18 000–25 000	25 000–35 000	35 000–50 000	50 000–75 000	40 000
Челябинск	20 000–30 000	30 000–42 000	42 000–58 000	58 000–85 000	46 000

©2017, ОАО «ИнфоТеКС».

Выводы:

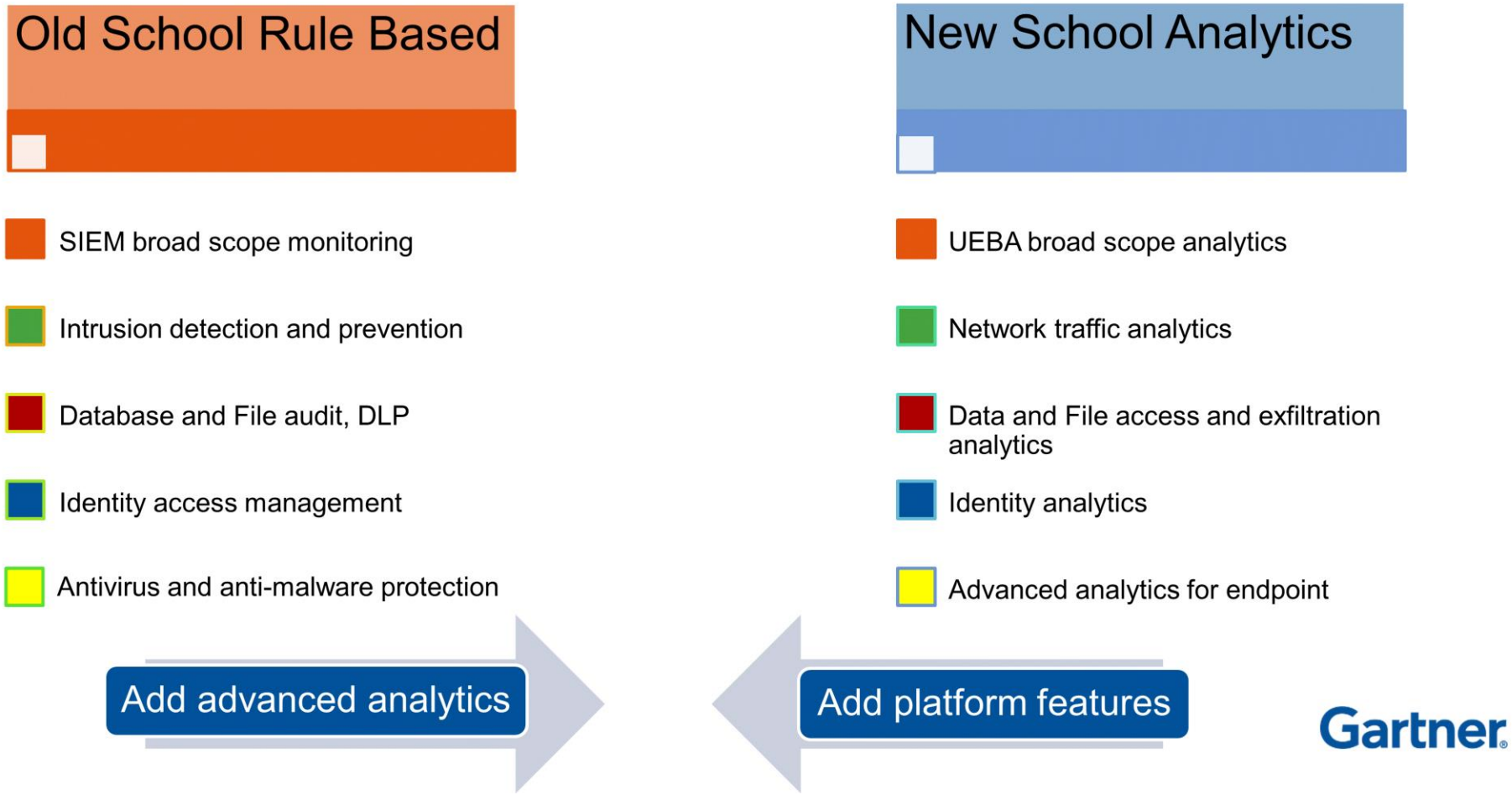
- Снижать количество ручной работы
- Использовать технологии машинного обучения



©2017, ОАО «ИнфоТеКС».


Инструменты

Old School Versus New School Security Products

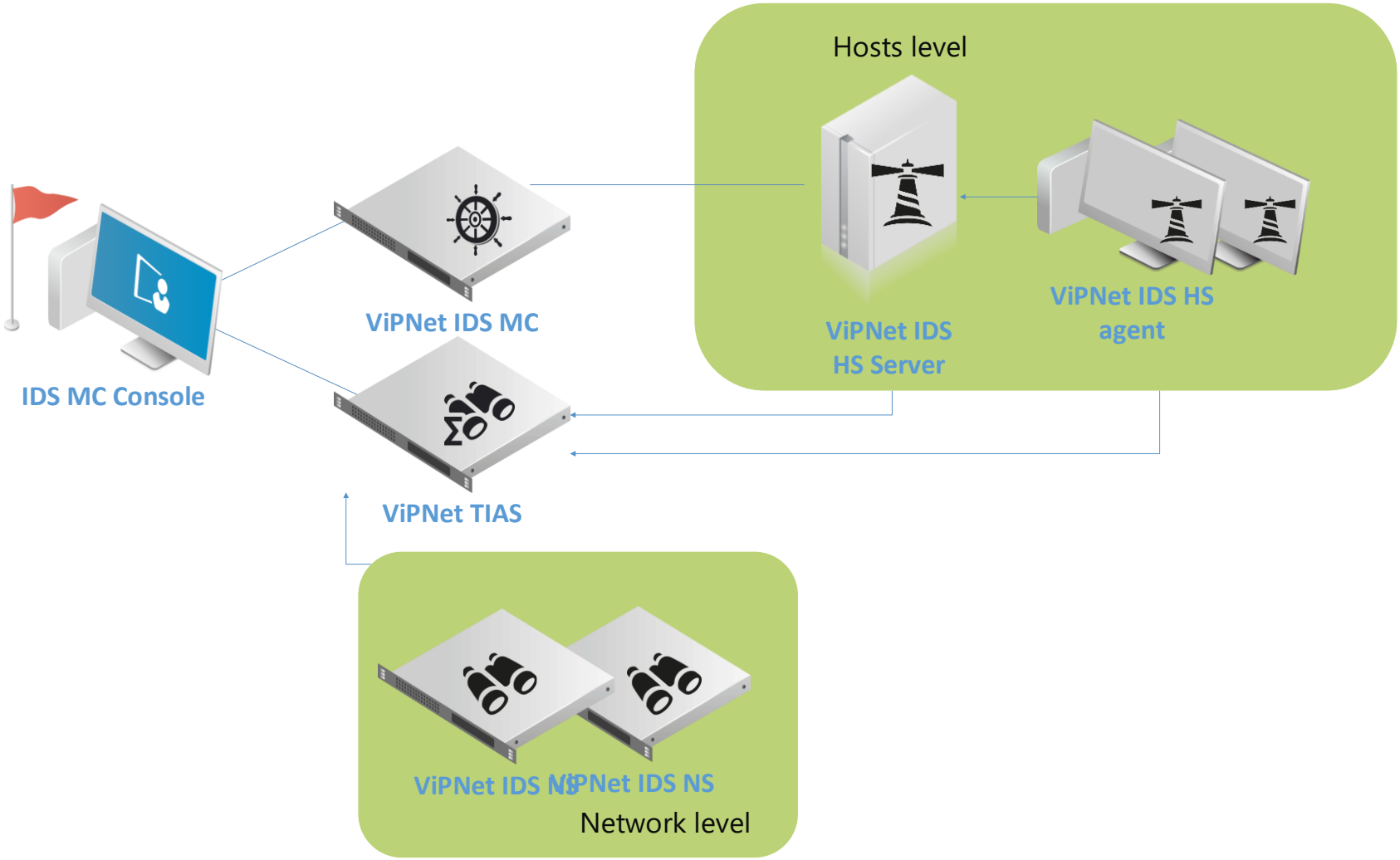


©2017, ОАО «ИнфоТеКС».



Решение

Решение ViPNet по обнаружению угроз и вторжений



©2017, ОАО «ИнфоТеКС».

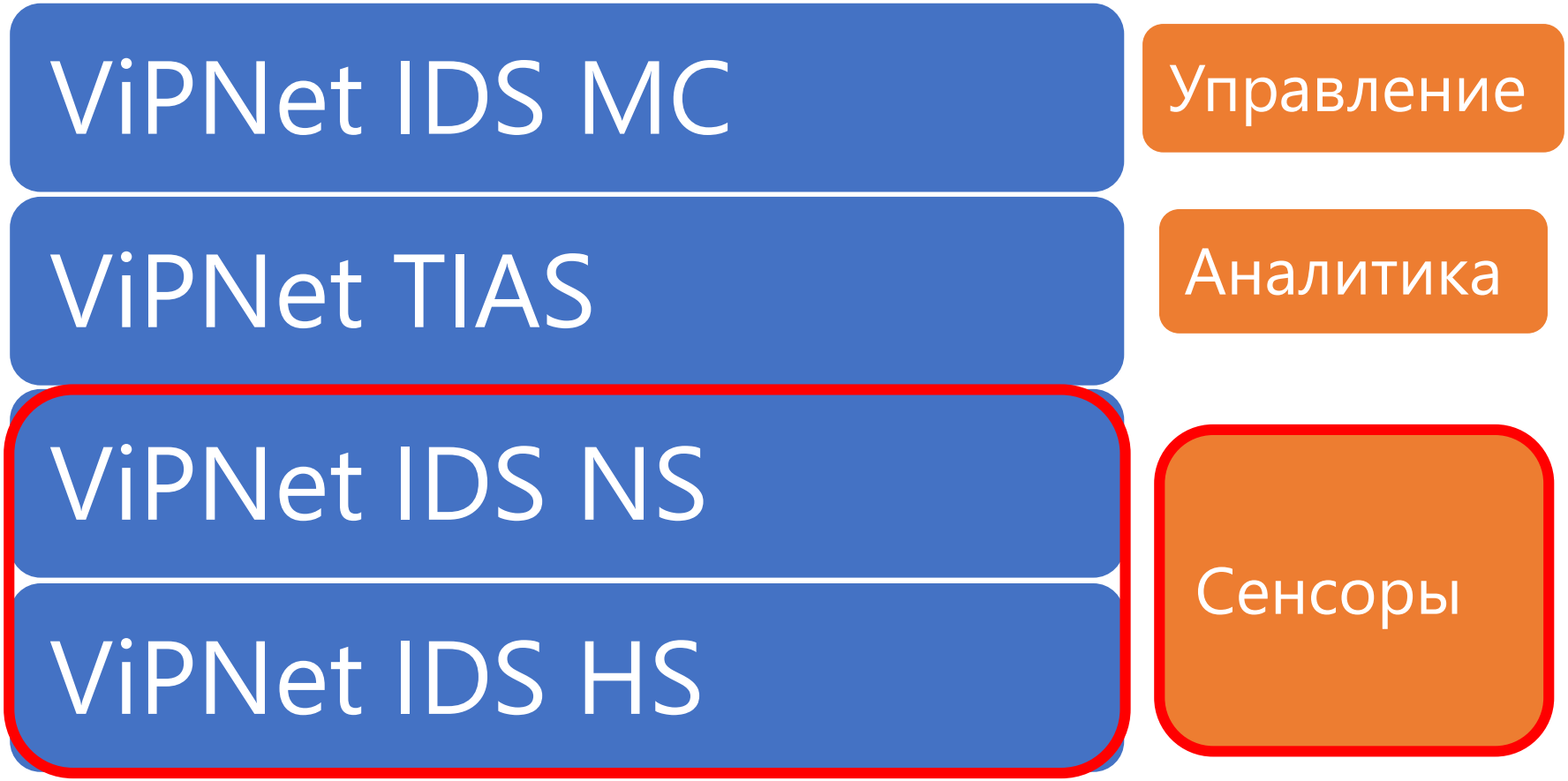
Решаемые задачи:

- непрерывный процесс анализа событий;
- адекватная реакция на произошедшие события;
- быстрое устранение последствий инцидента;
- извлечение полезных уроков



©2017, ОАО «ИнфоТеКС».

Назначение компонент решения



©2017, ОАО «ИнфоТеКС».

Сенсоры

IDS NS

- Network Sensor - захватывают и анализируют сетевые пакеты

IDS HS

- Host-based Intrusion Detection System - отслеживают активность хоста (аудит событий ОС, системных логов и анализ трафика)

©2017, ОАО «ИнфоТеКС».

Сетевой сенсор

ViPNet IDS MC

ViPNet TIAS

ViPNet IDS NS

ViPNet IDS HS

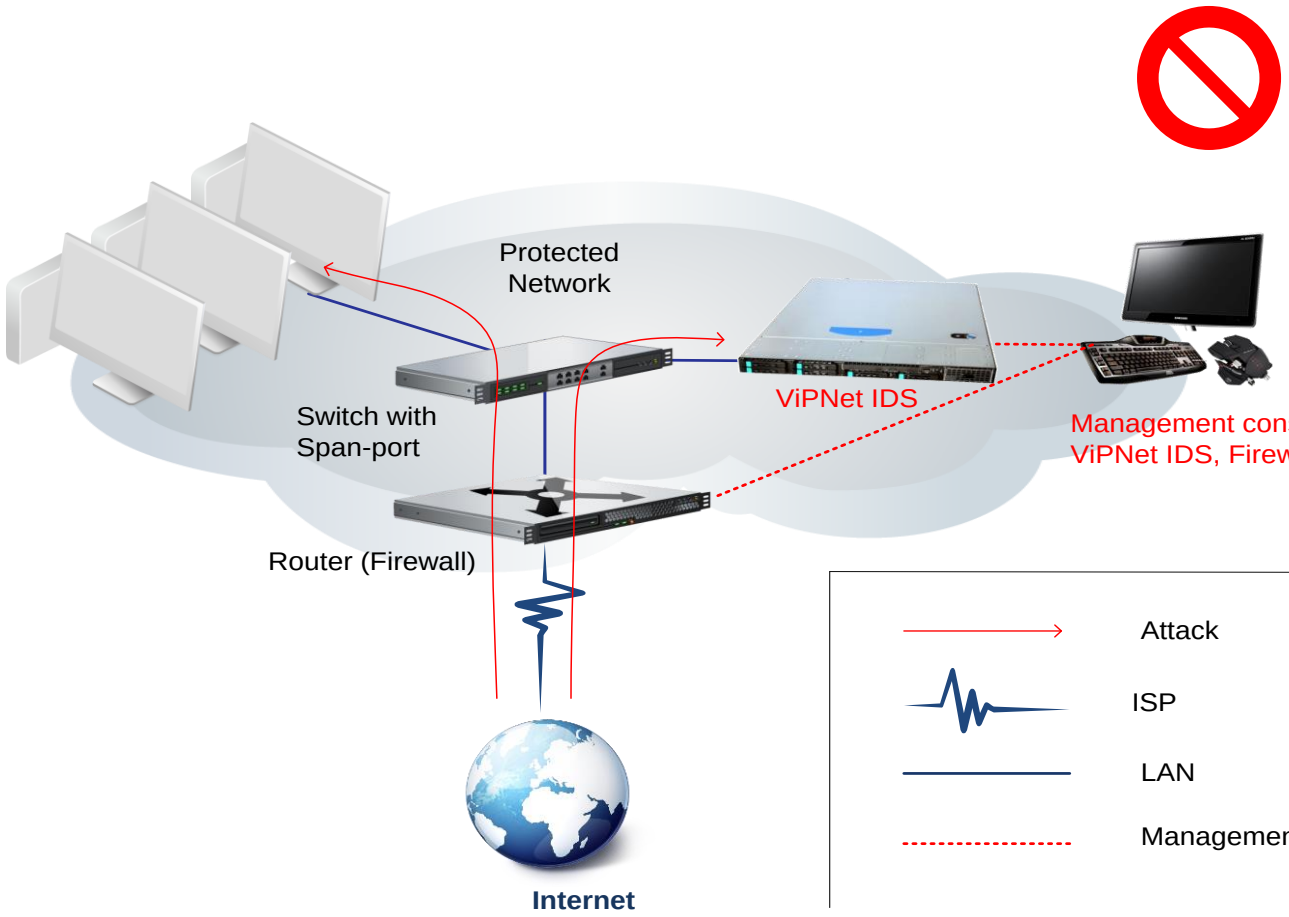
Управление

Аналитика

Сенсоры

©2017, ОАО «ИнфоТеКС».

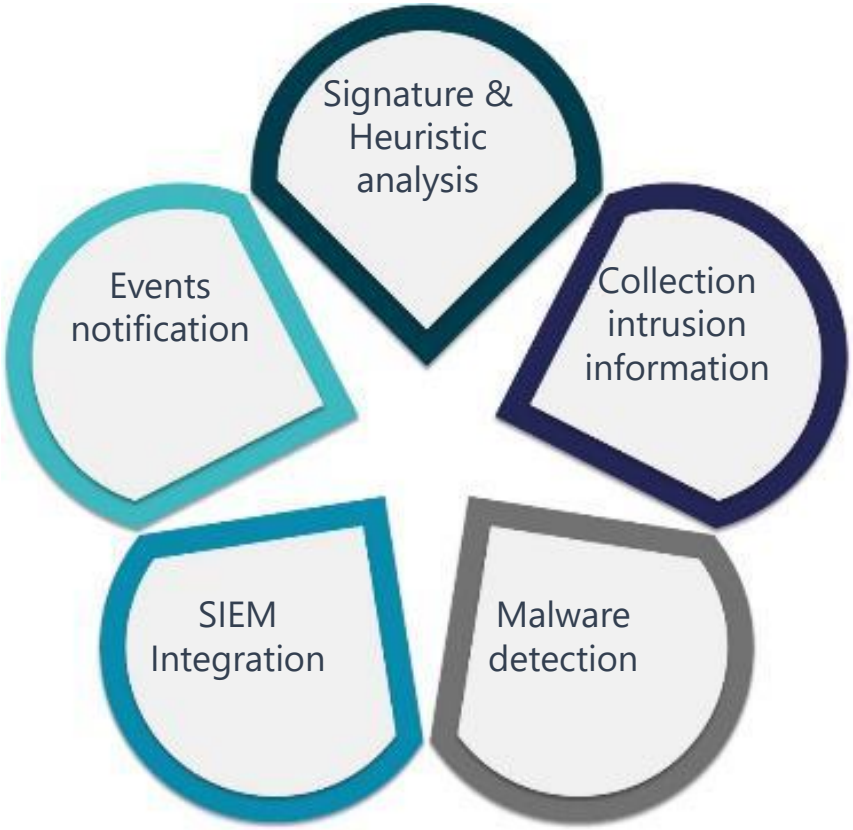
Выявление атак с помощью ViPNet IDS





©2017, ОАО «ИнфоТеКС».

ViPNet IDS NS



Варианты исполнения:

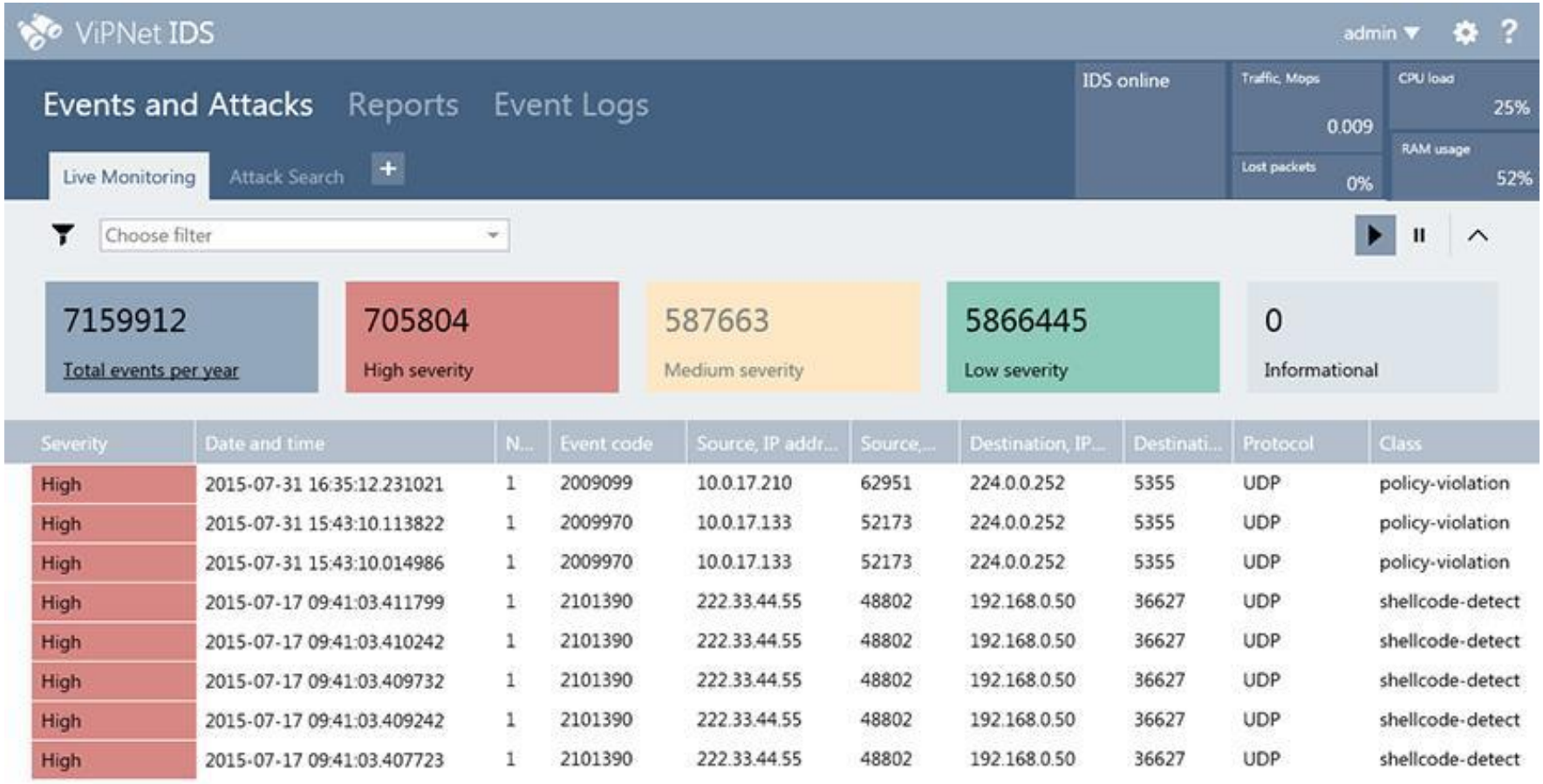
- ViPNet IDS NS 100
- ViPNet IDS NS1000
- ViPNet IDS NS 2000

Virtual appliance

- ViPNet IDS NS VA

©2017, ОАО «ИнфоТеКС».

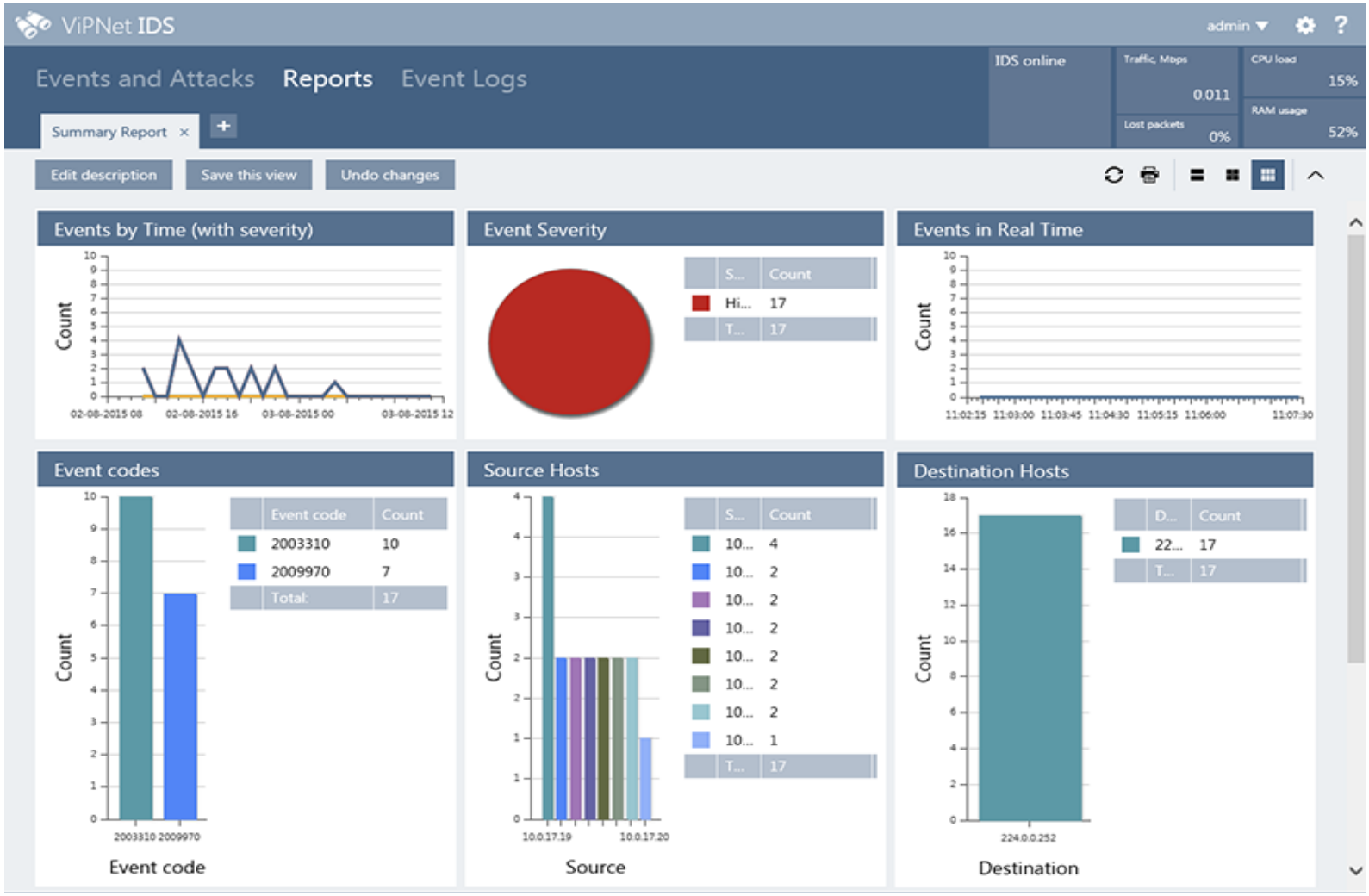
On-line мониторинг



Severity	Date and time	N...	Event code	Source, IP addr...	Source,...	Destination, IP...	Destinati...	Protocol	Class
High	2015-07-31 16:35:12.231021	1	2009099	10.0.17.210	62951	224.0.0.252	5355	UDP	policy-violation
High	2015-07-31 15:43:10.113822	1	2009970	10.0.17.133	52173	224.0.0.252	5355	UDP	policy-violation
High	2015-07-31 15:43:10.014986	1	2009970	10.0.17.133	52173	224.0.0.252	5355	UDP	policy-violation
High	2015-07-17 09:41:03.411799	1	2101390	222.33.44.55	48802	192.168.0.50	36627	UDP	shellcode-detect
High	2015-07-17 09:41:03.410242	1	2101390	222.33.44.55	48802	192.168.0.50	36627	UDP	shellcode-detect
High	2015-07-17 09:41:03.409732	1	2101390	222.33.44.55	48802	192.168.0.50	36627	UDP	shellcode-detect
High	2015-07-17 09:41:03.409242	1	2101390	222.33.44.55	48802	192.168.0.50	36627	UDP	shellcode-detect
High	2015-07-17 09:41:03.407723	1	2101390	222.33.44.55	48802	192.168.0.50	36627	UDP	shellcode-detect

©2017, ОАО «ИнфоТеКС».

Отчеты и статистика



©2017, ОАО «ИнфоТеКС».

Сенсор уровня узла

ViPNet IDS MC

ViPNet TIAS

ViPNet IDS NS

ViPNet IDS HS

Управление

Аналитика

Сенсоры

©2017, ОАО «ИнфоТеКС».

Для чего нужен IDS HS?

- Определять атаки, которые “не видит” сетевой сенсор;
- Обнаруживать атаки после расшифровки входящего трафика;
- Обнаруживать подозрительную активность внутри ОС (файловая активность, изменения в реестре и процессах).



©2017, ОАО «ИнфоТеКС».

ViPNet IDS HS

- мониторинг и обработка событий внутри хоста;
- сигнатурный и эвристический методы анализа атак;
- отечественные правила и сигнатуры
- syslog (формат CEF) и snmp
- интеграция с Active Directory и ViPNet-сетями

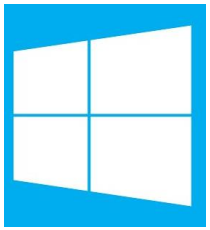


©2017, ОАО «ИнфоТеКС».

Поддерживаемые ОС

- Семейство операционных систем Windows





- AstraLinux 1.5 релиз «Смоленск» (агент)



- Debian 8 (агент)



©2017, ОАО «ИнфоТеКС».

Сертификация

Сертификат соответствия ФСТЭК России № 3802 на СОВ ViPNet IDS HS

Действителен до декабря 2020 г



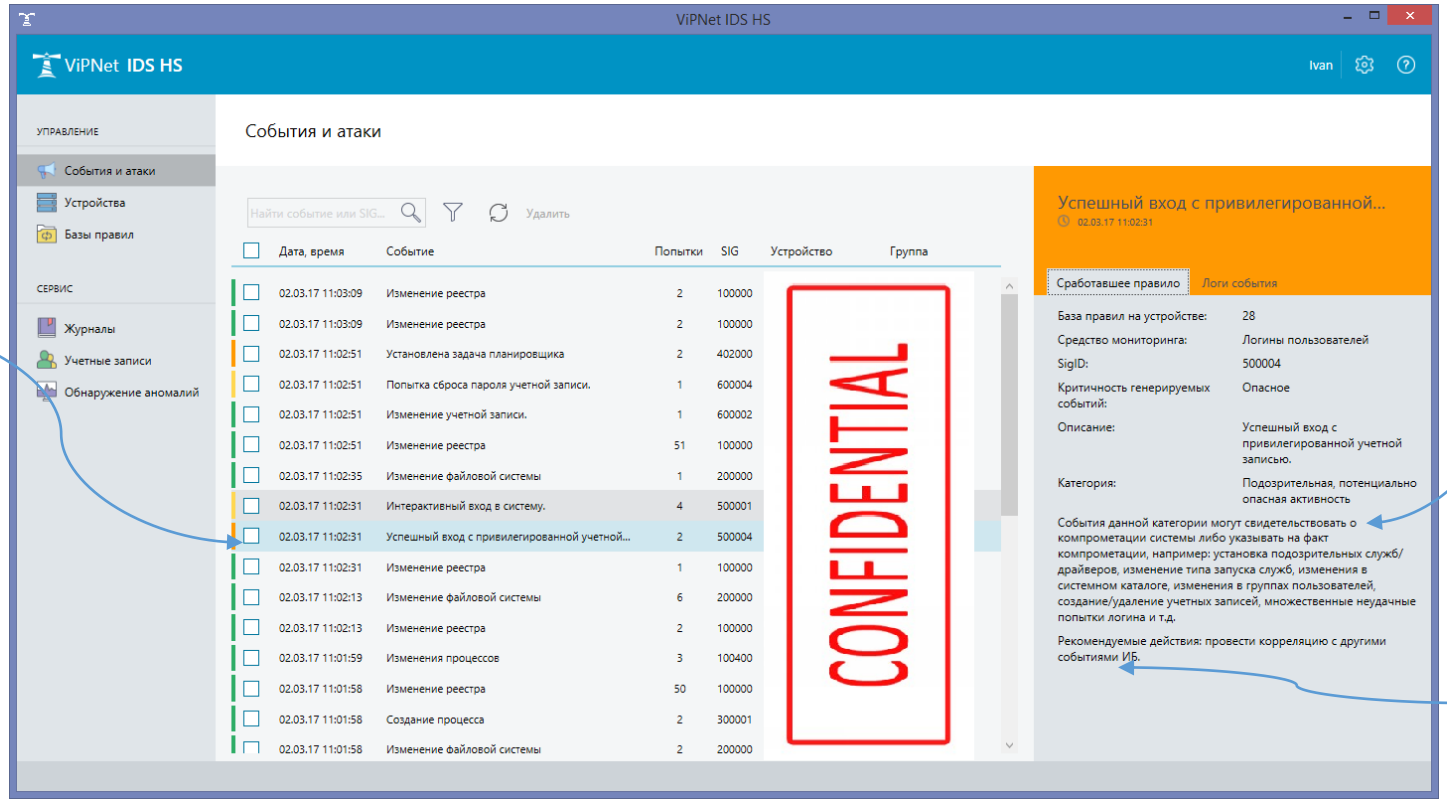
Меры защиты информации в информационных системах

(Приказы ФСТЭК №21 и №17)

ИАФ.1, ИАФ.5, УПД.4, РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7, СОВ.1, СОВ.2, АНЗ.3, ОЦЛ.1, ОЦЛ.3, ИНЦ.2, ИНЦ.3, ИНЦ.4

©2017, ОАО «ИнфоТеКС».

Внешний вид интерфейса



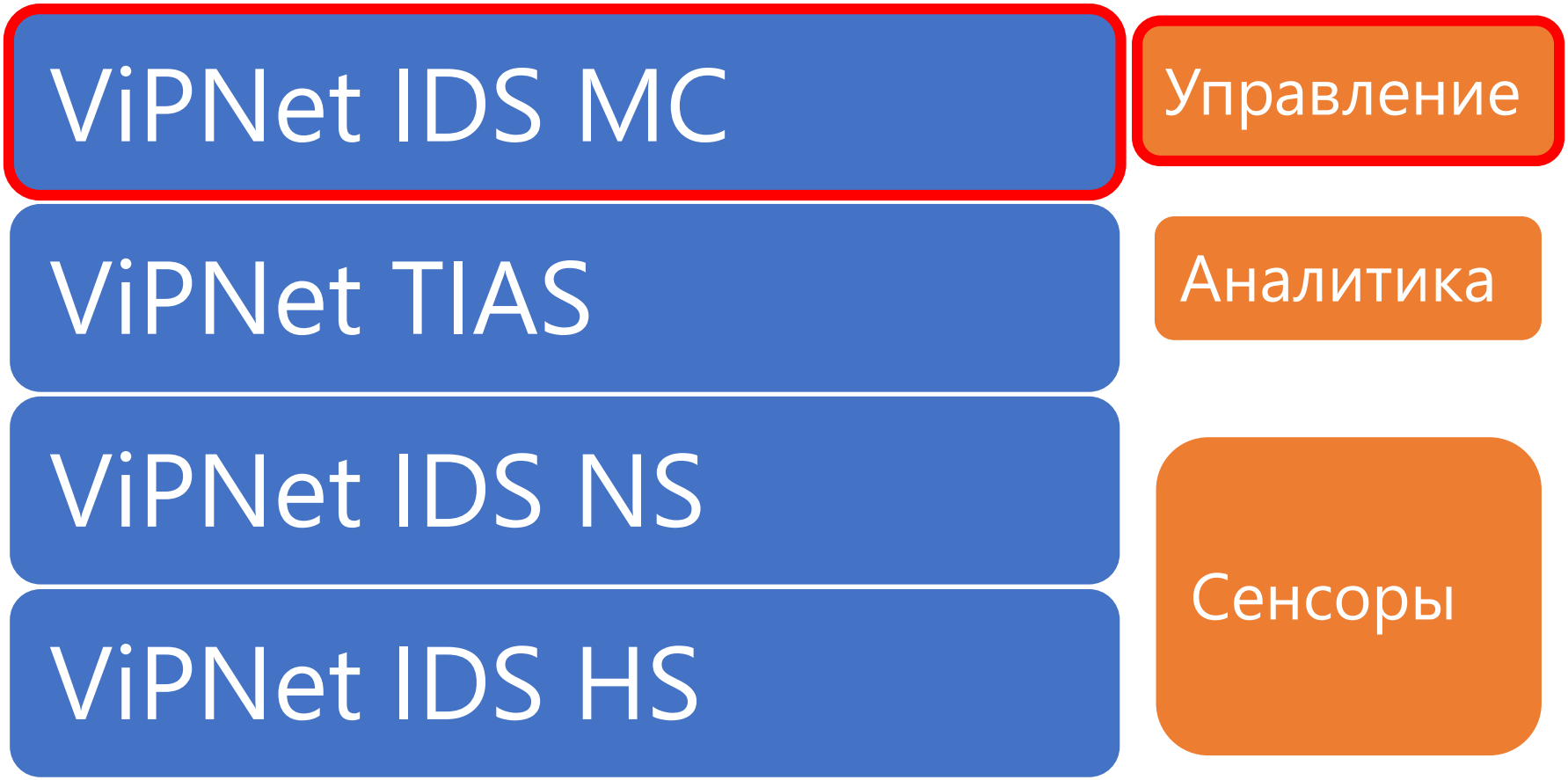
Опасное событие

Подробная информация о событии

Рекомендации по дальнейшим действиям

©2017, ОАО «ИнфоТеКС».

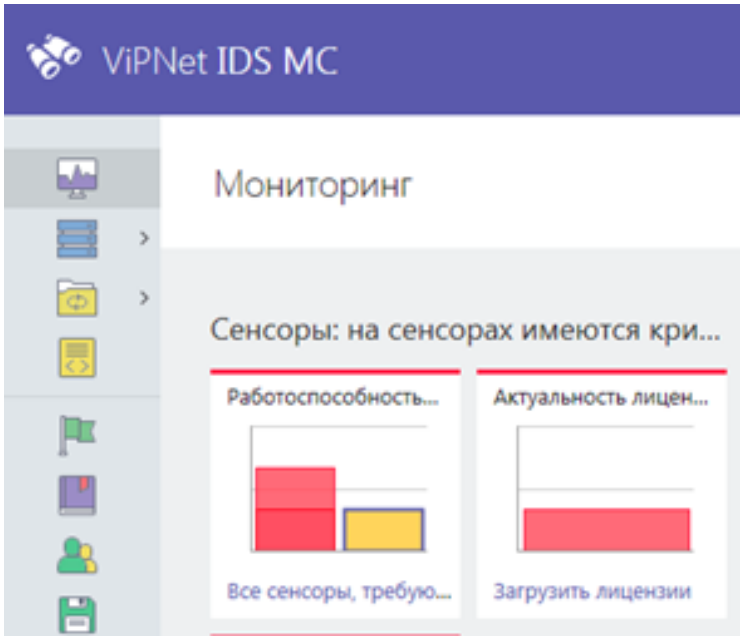
Центр управления



©2017, ОАО «ИнфоТеКС».

ViPNet IDS MC

- Единая графическая консоль управления
- Разграничение прав доступа;
- Управление обновлениями и настройками
- Мониторинг состояния сенсоров



©2017, ОАО «ИнфоТеКС».

Интеллектуальный анализ

ViPNet IDS MC

ViPNet TIAS

ViPNet IDS NS

ViPNet IDS HS

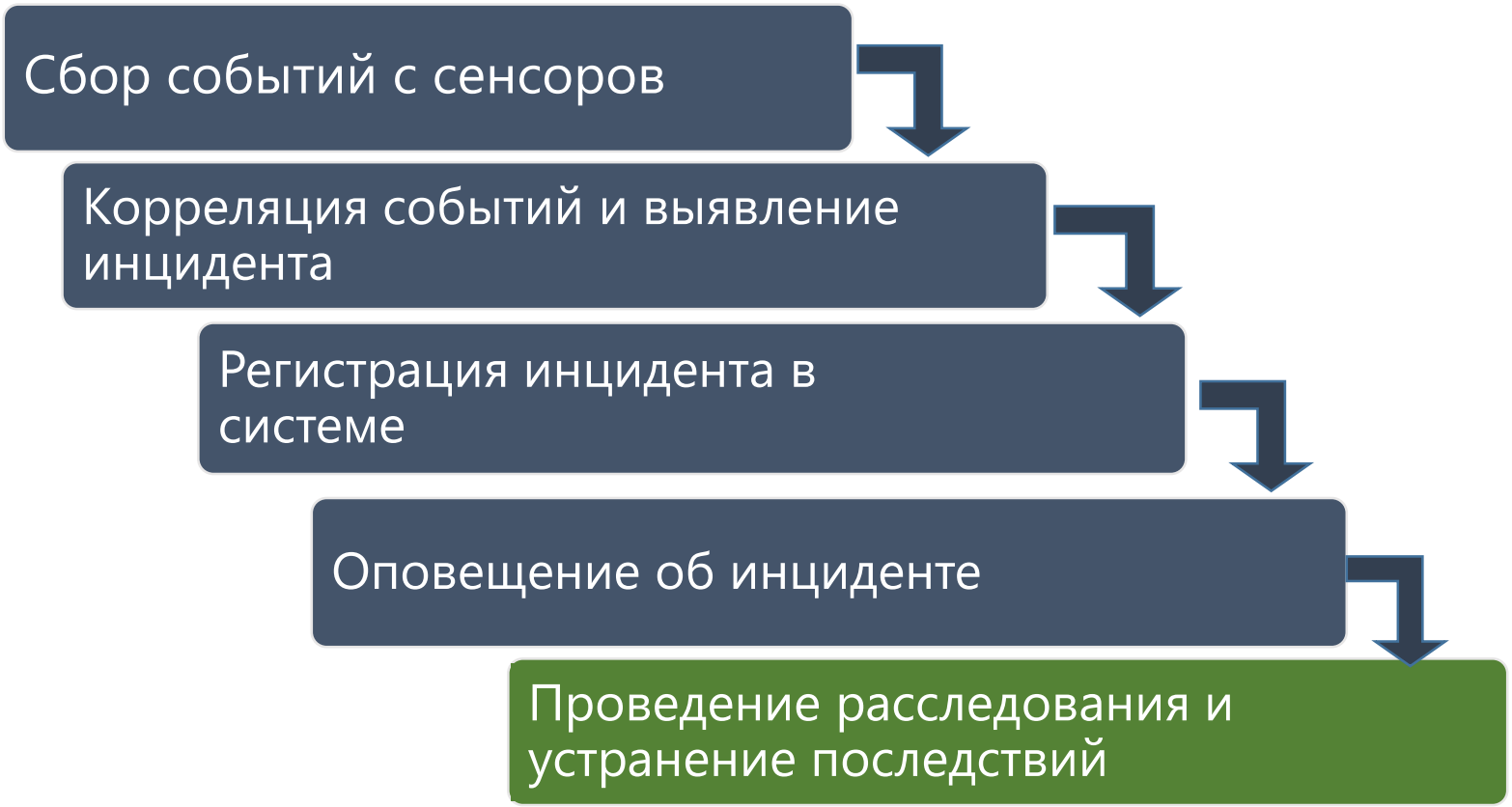
Управление

Аналитика

Сенсоры

©2017, ОАО «ИнфоТеКС».

Сценарий обработки событий



©2017, ОАО «ИнфоТеКС».

Как это работает?



©2017, ОАО «ИнфоТеКС».

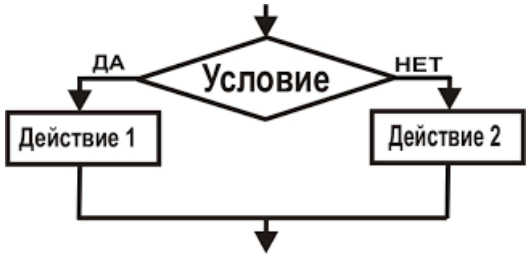
Отличительная особенность

Комбинирование двух методов:

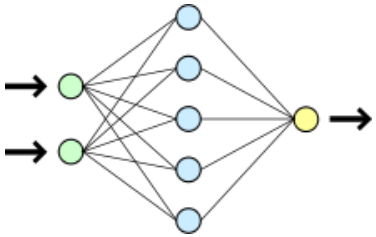
- метод, основанный на использовании базы решающих правил;
- метод машинного обучения математической модели принятия решений



Правила



Нейросеть



©2017, ОАО «ИнфоТеКС».

Основные функции

- сбор и анализ событий от сенсоров ViPNet IDS;
- автоматическое выявление инцидентов;
- оповещение об инцидентах;
- расследования по инцидентам
- отчеты по событиям и инцидентам;



©2017, ОАО «ИнфоТеКС».

Варианты исполнения

Desktop



ПАК ViPNet TIAS 100

Server 1U



ПАК ViPNet TIAS 1000

ПАК ViPNet TIAS 2000

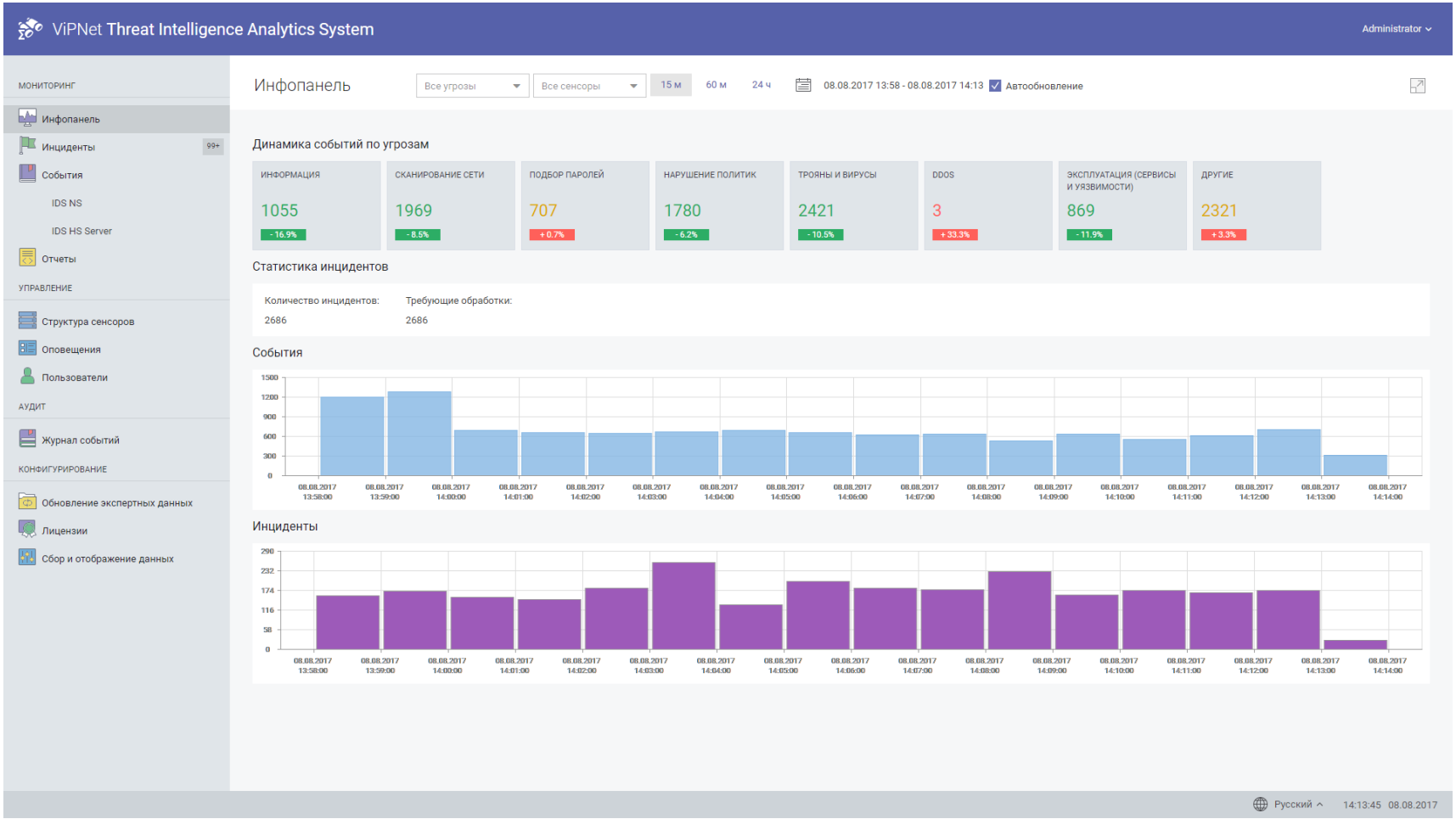
ПАК ViPNet TIAS 5000

Virtual Appliance

ViPNet TIAS VA

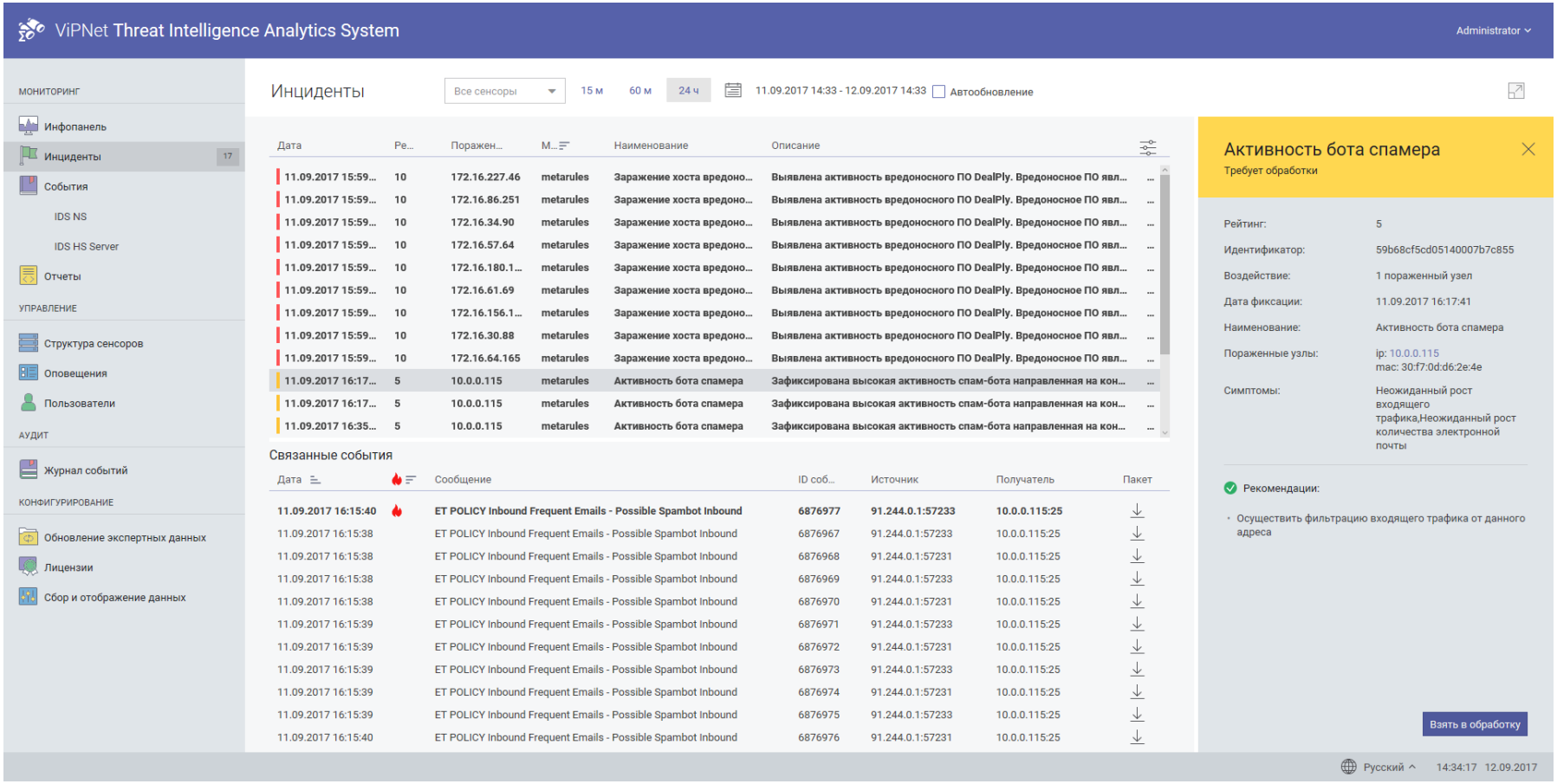
©2017, ОАО «ИнфоТеКС».

Информационная панель



©2017, ОАО «ИнфоТеКС».

Инциденты



©2017, ОАО «ИнфоТеКС».

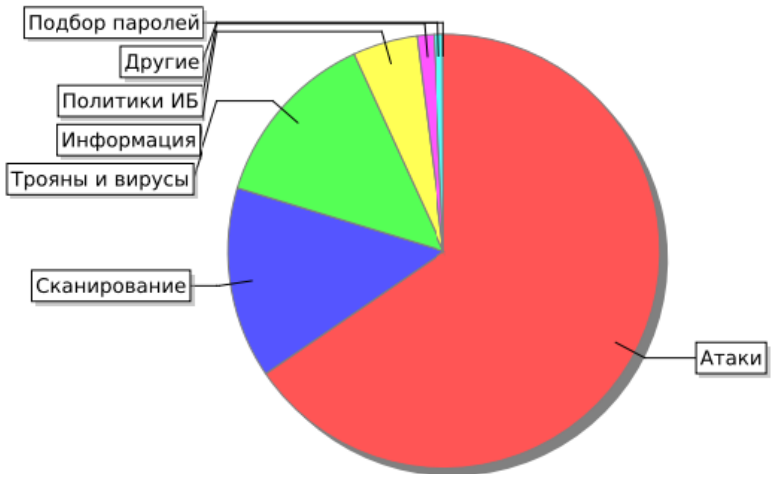
Отчеты

Статистика по событиям

Распределение событий по категориям

События с 9/15/16 4:50 PM по 9/16/16 3:57 PM

Наименование	Количество
Атаки	28008
Сканирование	6097
Трояны и вирусы	5745
Информация	2071
Политики ИБ	537
Другие	314
Подбор паролей	14



©2017, ОАО «ИнфоТеКС».

Меры защиты

XIV. Выявление инцидентов и реагирование на них (ИНЦ)		
ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них	Правила ПМ
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Управление пользователями и ролевая модель
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Есть
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Уведомление по e-mail
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Автоматический анализ Расследование по инцидентам
ИНЦ. 5	Принятие мер по устранению последствий инцидентов	Рекомендации в карточках инцидентов
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Отчеты

©2017, ОАО «ИнфоТеКС».

TIAS для оказания услуг

№	Наименование оборудования	Технические и (или) функциональные характеристики
24.	Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств.
25.	Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация. Должны иметь сертификаты соответствия ФСТЭК России
26.	Средства управления инцидентами информационной безопасности	Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств.

Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79

©2017, ОАО «ИнфоТеКС».

Сертификация

ФСТЭК

- отсутствие НДВ 4 Уровень по ТУ
- СОВ (в составе IDS 3)

ФСБ

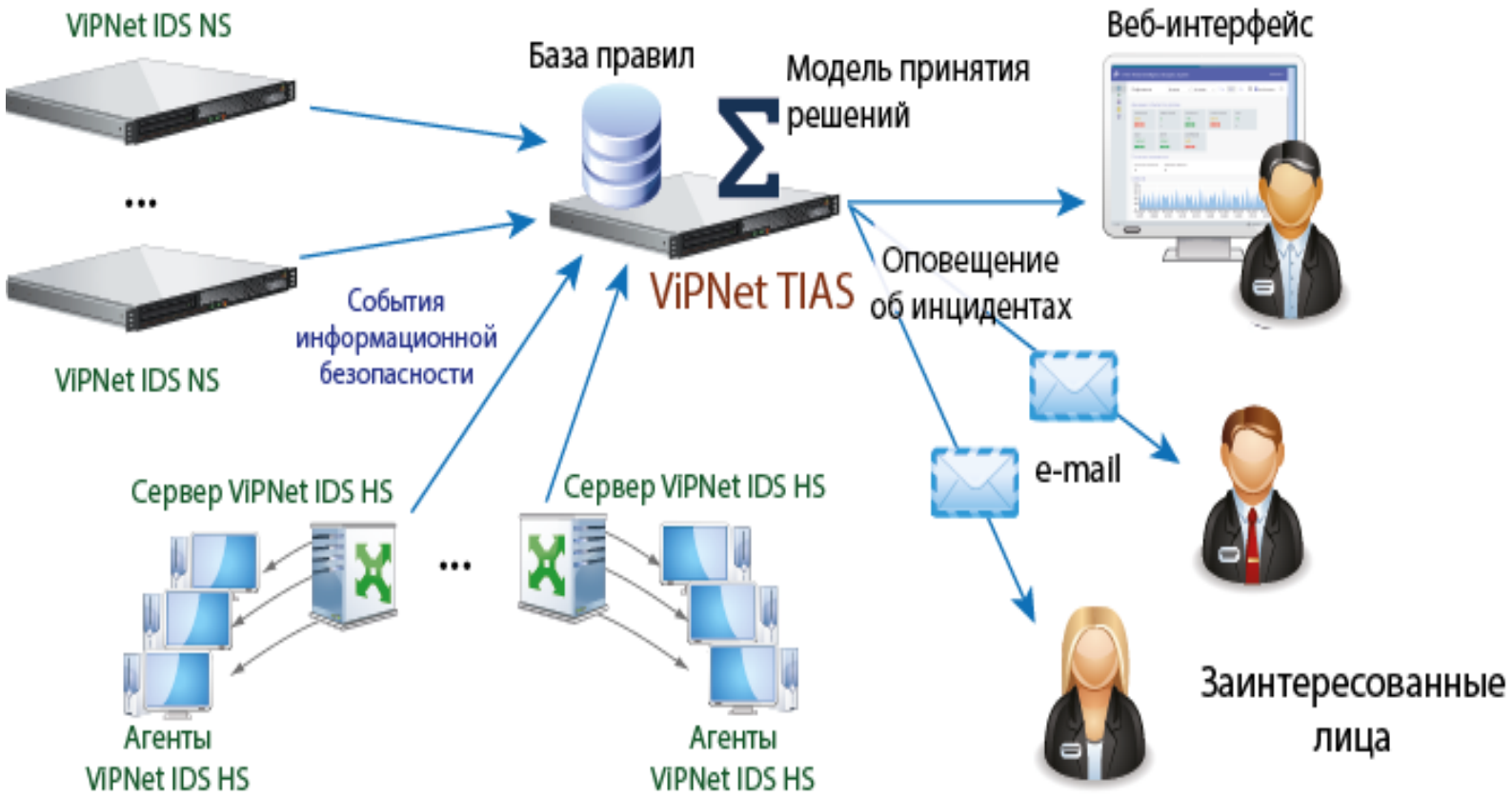
- СОА класс В (в составе IDS 3)

©2017, ОАО «ИнфоТеКС».



Решение ITDP

Основной сценарий работы



©2017, ОАО «ИнфоТеКС».

Преимущества решения



Инструмент и техподдержка от ИнфоТеКС



Экспертиза и сервисы от Перспективного мониторинга



Эффективное работающее решение

©2017, ОАО «ИнфоТеКС».


Спасибо!