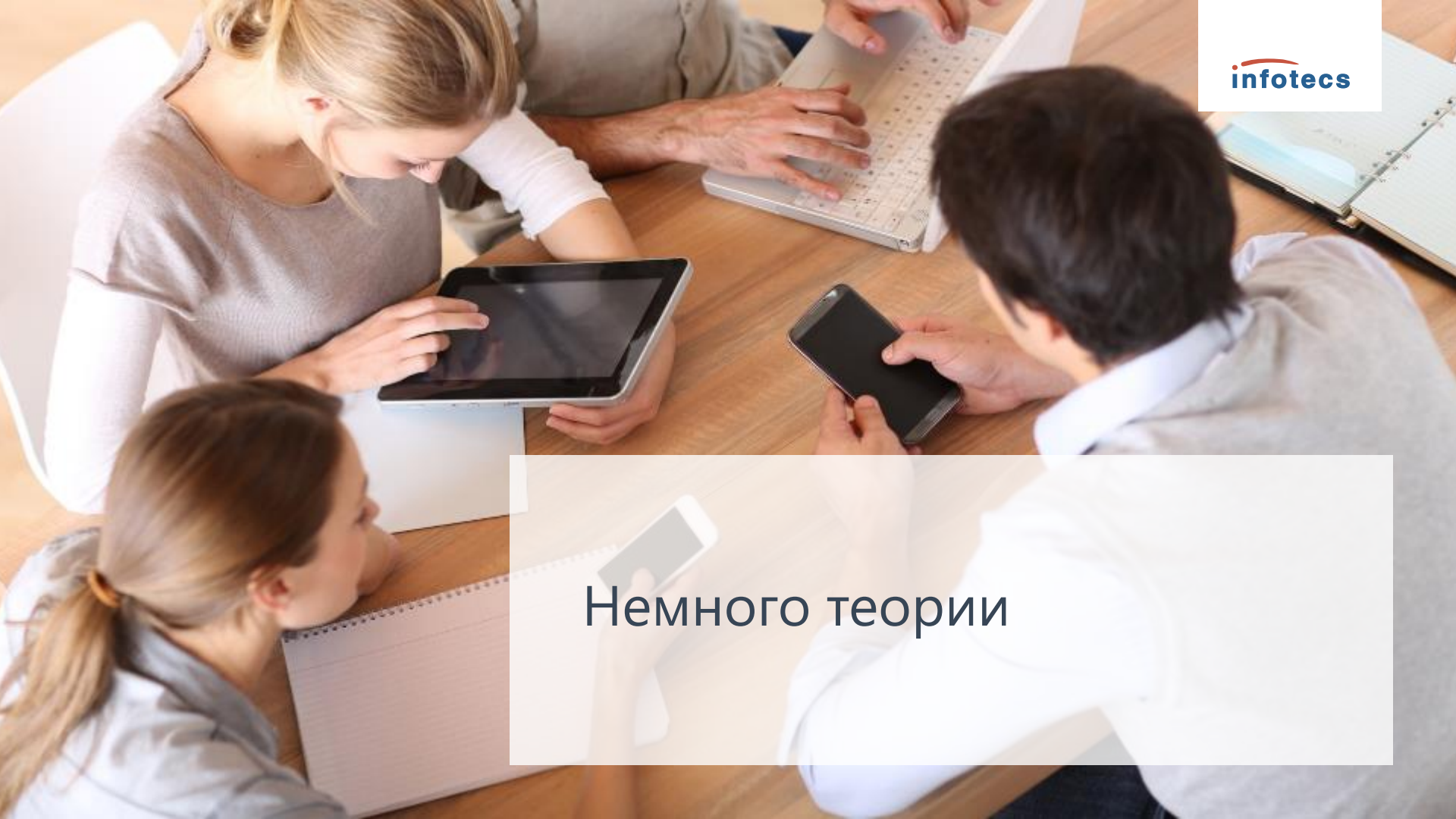
Системы обнаружения вторжений

Светлана Старовойт,
Руководитель направления, ОАО ИнфоТеКС
StarovoytSG@infotecs.ru



Немного теории

Система обнаружения вторжений

Система обнаружения вторжений (СОВ) — программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

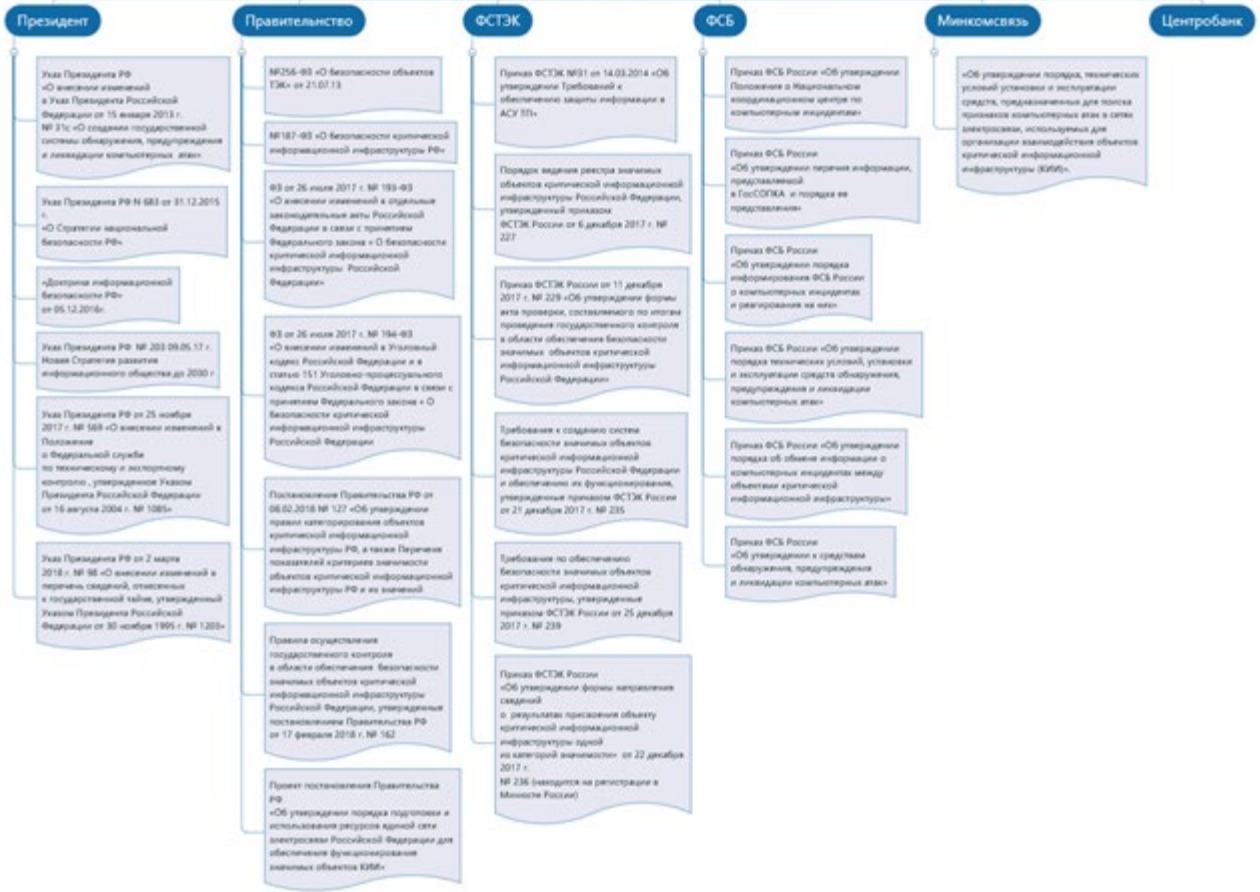
Тип системы обнаружения вторжений	6	5	4	3	2	1
Система обнаружения вторжений уровня сети	ИТ.СОВ. С6.ПЗ	ИТ.СОВ. С5.ПЗ	ИТ.СОВ. С4.ПЗ	ИТ.СОВ. С3.ПЗ	ИТ.СОВ. С2.ПЗ	ИТ.СОВ. С1.ПЗ
Система обнаружения вторжений уровня узла	ИТ.СОВ. У6.ПЗ	ИТ.СОВ. У5.ПЗ	ИТ.СОВ. У4.ПЗ	ИТ.СОВ. У3.ПЗ	ИТ.СОВ. У2.ПЗ	ИТ.СОВ. У1.ПЗ

Система обнаружения атак

Система обнаружения компьютерных атак (СОА) – программное, программно-аппаратное или аппаратное средство, целевая функция которого заключается в автоматическом выявлении воздействий на контролируемую данным средством АИС, которые могут быть классифицированы, как компьютерные атаки.

№	Предъявляемые требования	Класс Г	Класс В	Класс Б	Класс А
1.	Обнаружение атак	*	=	+	
2.	Реакция на обнаруженную атаку	*	+	+	
3.	Контролируемые ресурсы АИС	-	*	+	
4.	Контролируемые протоколы	*	=	+	
5.	Управление СОА	*	=	+	
6.	Маскирование	-	*	+	
7.	Наличие механизмов собственной защиты	*	+	+	
8.	Оптимизация/модернизация СОА	*	+	=	
9.	Ведение системного журнала	*	=	+	
10.	Наличие документации	*	+	+	

Нормативно-правовые акты КИИ



Нормативное регулирование деятельности центров ГосСОПКА

Основные требования

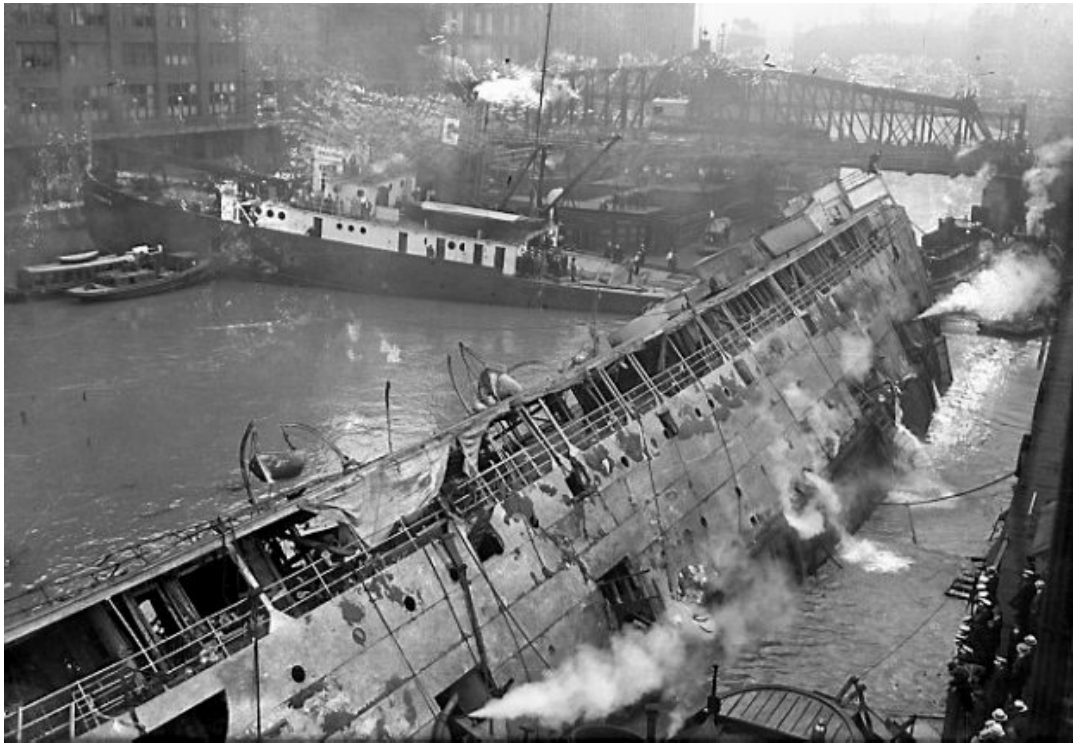
- Перечень информации, предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка предоставления информации в ГосСОПКА (Приказ № 367 от 24 июля 2018 года)
- Порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации… (Приказ ФСБ России от 24 июля 2018 г. N 368)
- **Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак** и реагирования на компьютерные инциденты (Проект приказа ФСБ)
- **Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры** Российской Федерации (Приказ ФСТЭК №239 от 25.12.2017 , приказ ФСТЭК № 138 от 9 августа 2018 г.).

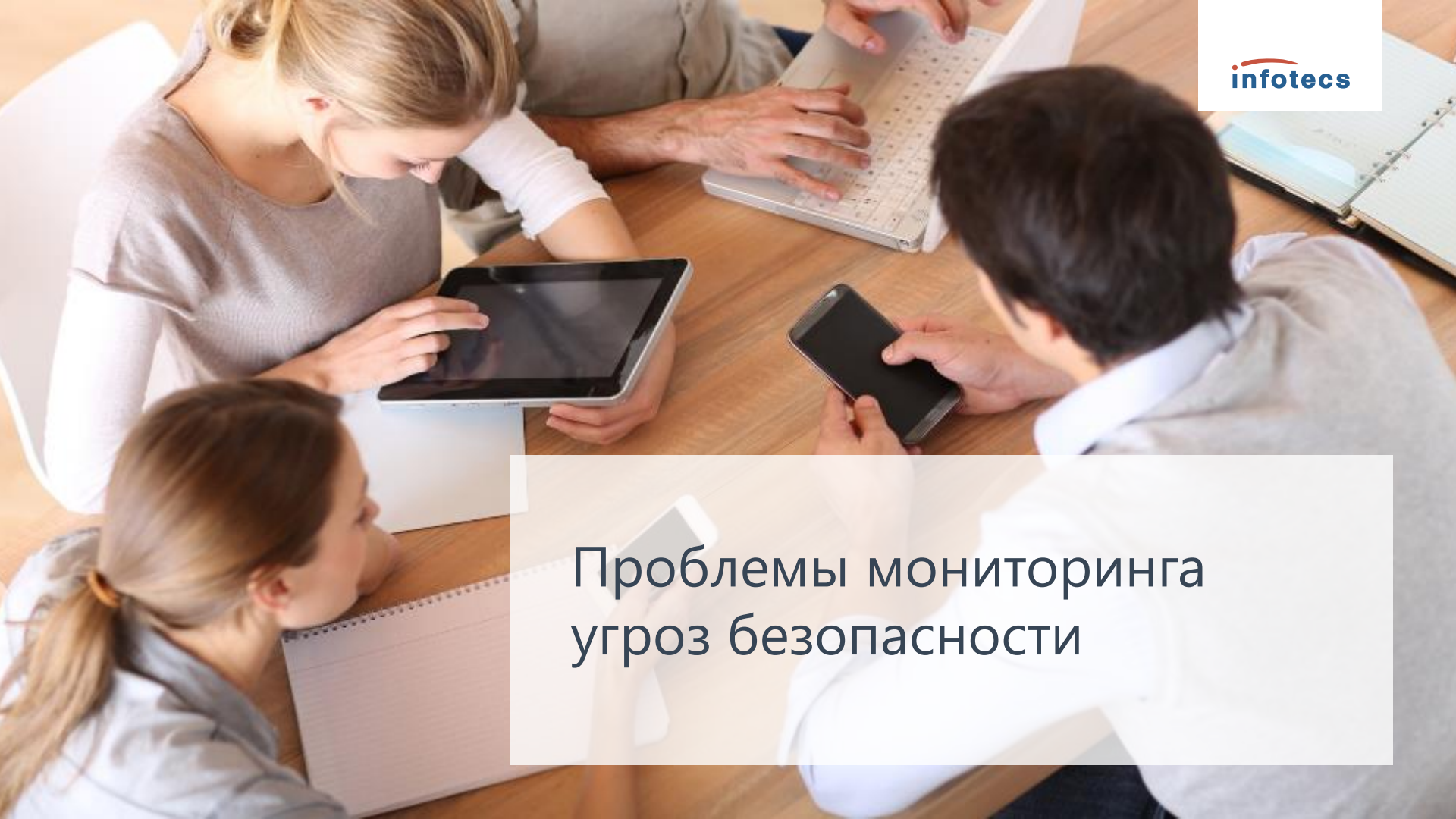
Обеспечение выполнения следующих задач:

- обнаружение компьютерных атак;
- предупреждение компьютерных атак;
- ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;
- поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ;
- криптографическая защита обмена информацией необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Обеспечение требований регуляторов





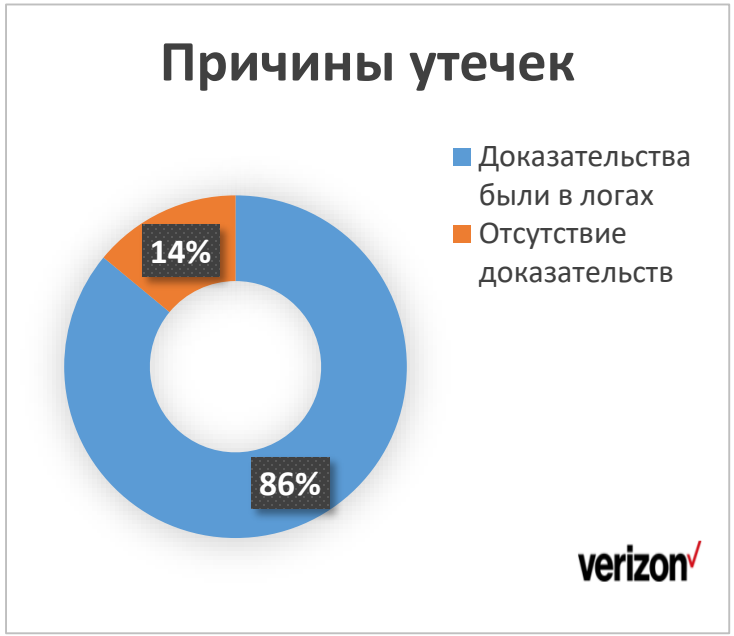
Проблемы мониторинга угроз безопасности

Сколько событий обрабатывает SOC?

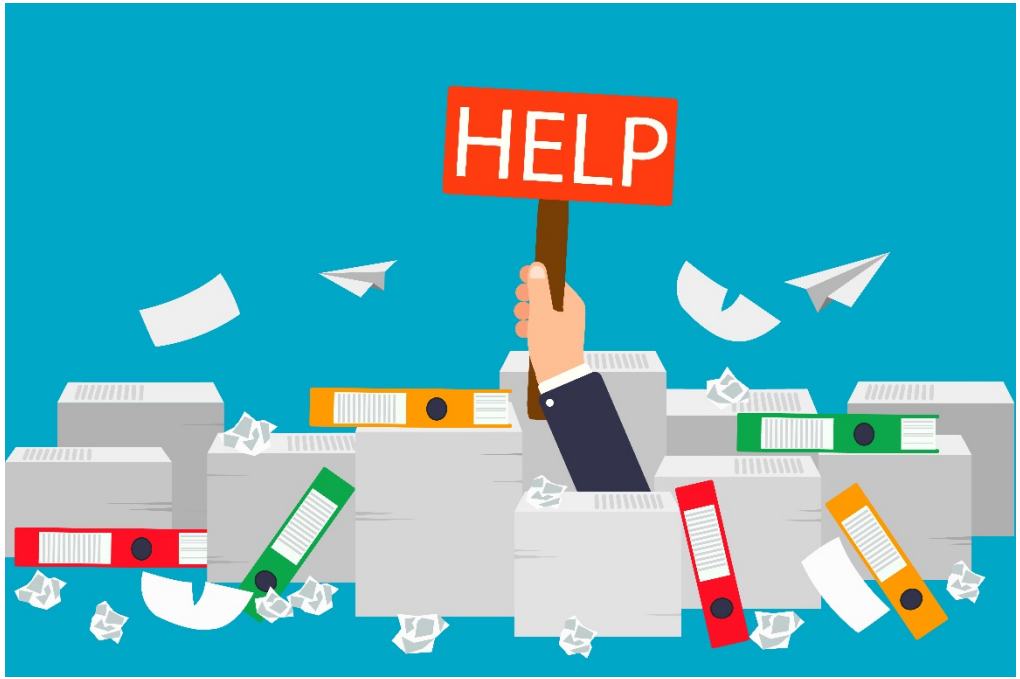
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

SOLAR SECURITY
software&services

Результаты исследований



Важные события остаются незамеченными



Средства ИБ создают «информационный шум»!

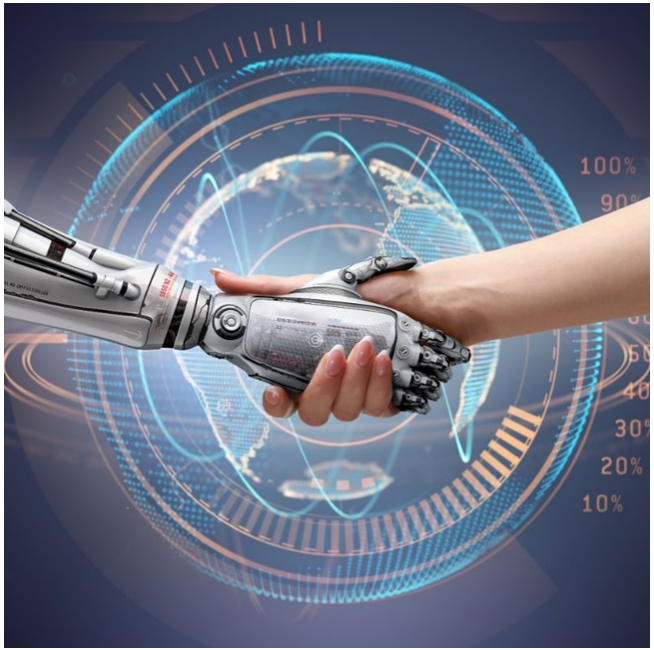
Квалифицированные сотрудники стоят дорого

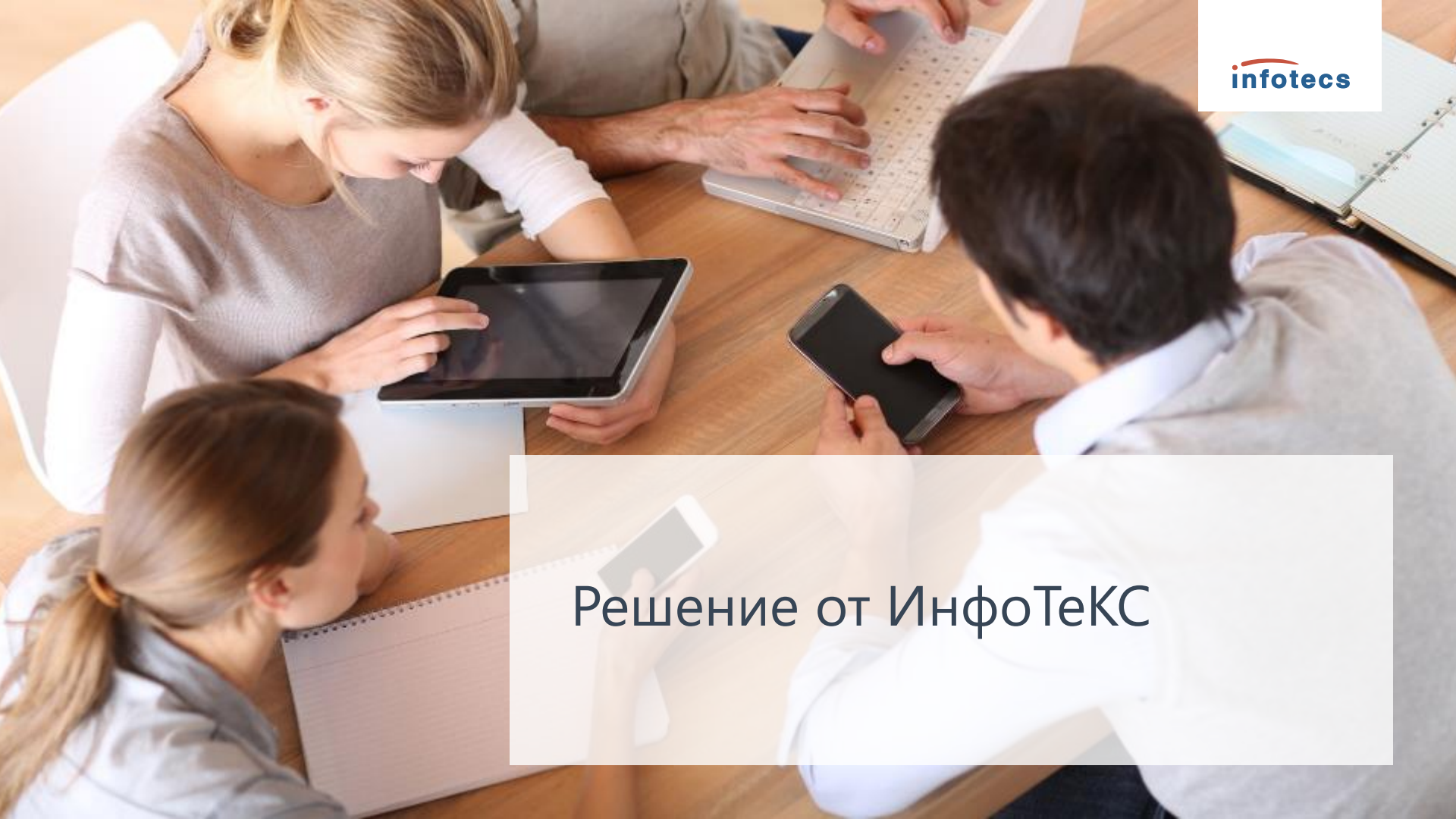
Причины неудовлетворенности системой SIEM

Что делать?

- **Снижать количество ручной работы –** высококвалифицированный персонал для проведения расследований

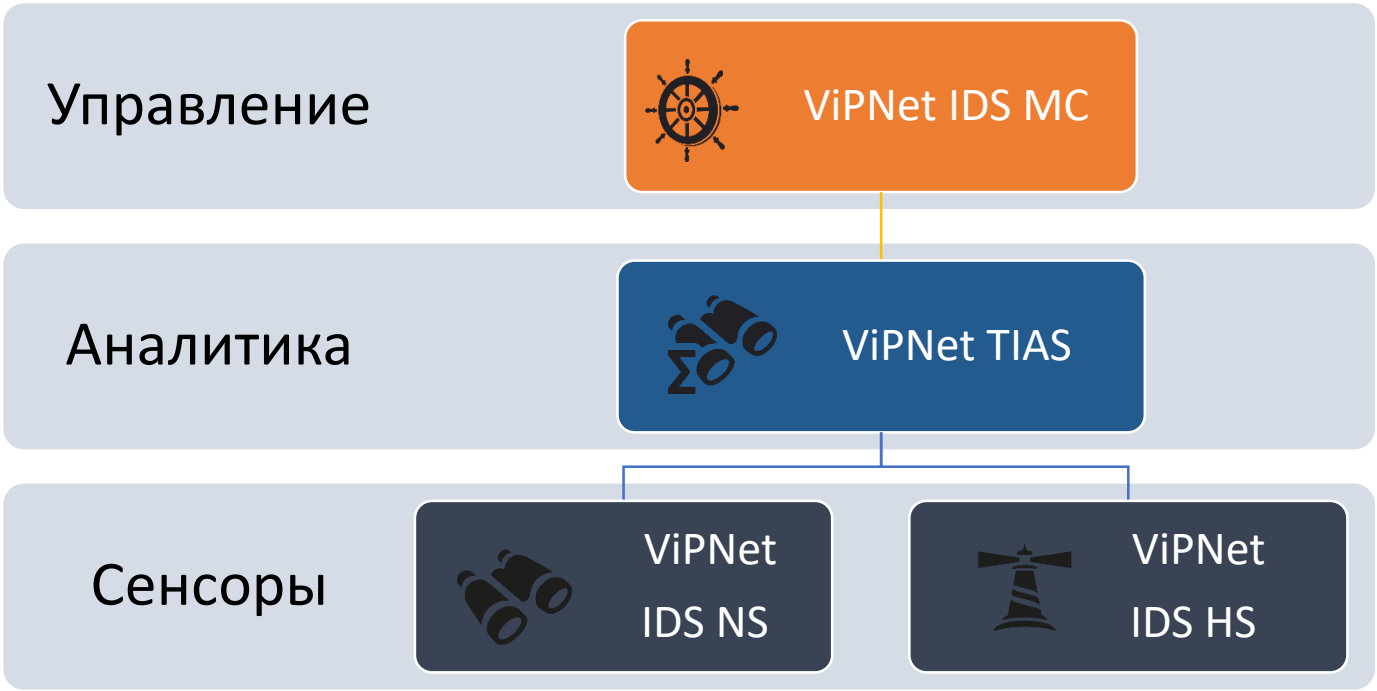
- **Использовать технологии машинного обучения –** инструменты и средства для автоматизации анализа событий





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

ViPNet IDS Network Sensor

Анализ сетевого трафика

- **Сигнатурные метод анализа:**
  - анализ заголовков протоколов и содержимого сетевых пакетов на основе правил.
  - анализ передаваемых в сетевом трафике файлов на наличие вредоносного программного обеспечения.

- **Эвристические методы анализа:**
  - отслеживание отклонений отдельных параметров сетевого трафика от эталонной модели.
  - анализ служебных заголовков пакетов на наличие аномалий для следующих сетевых протоколов: RPC, HTTP, SMTP, FTP, SSH, MODBUS, GTP, SIP, Telnet, TCP, DNS, SSL, IMAP, DNP3, MODBUS и POP.
  - отслеживание попыток сетевых атак типа ARP-spoofing.

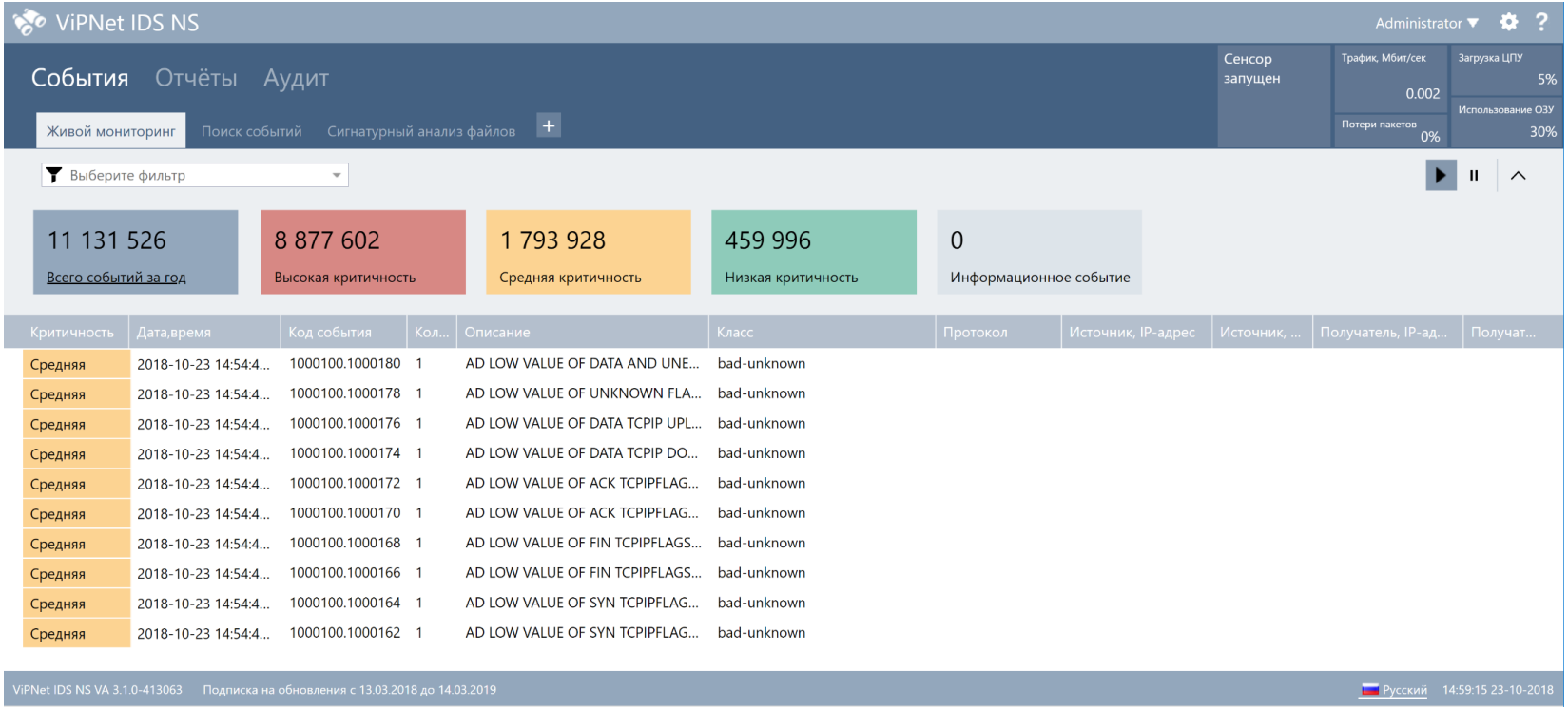
ViPNet IDS Network Sensor

- **Отображение**
  - дэшборды в режиме реального времени
  - таблицы с возможностью поиска по различным параметрам
  - Отчеты и графики

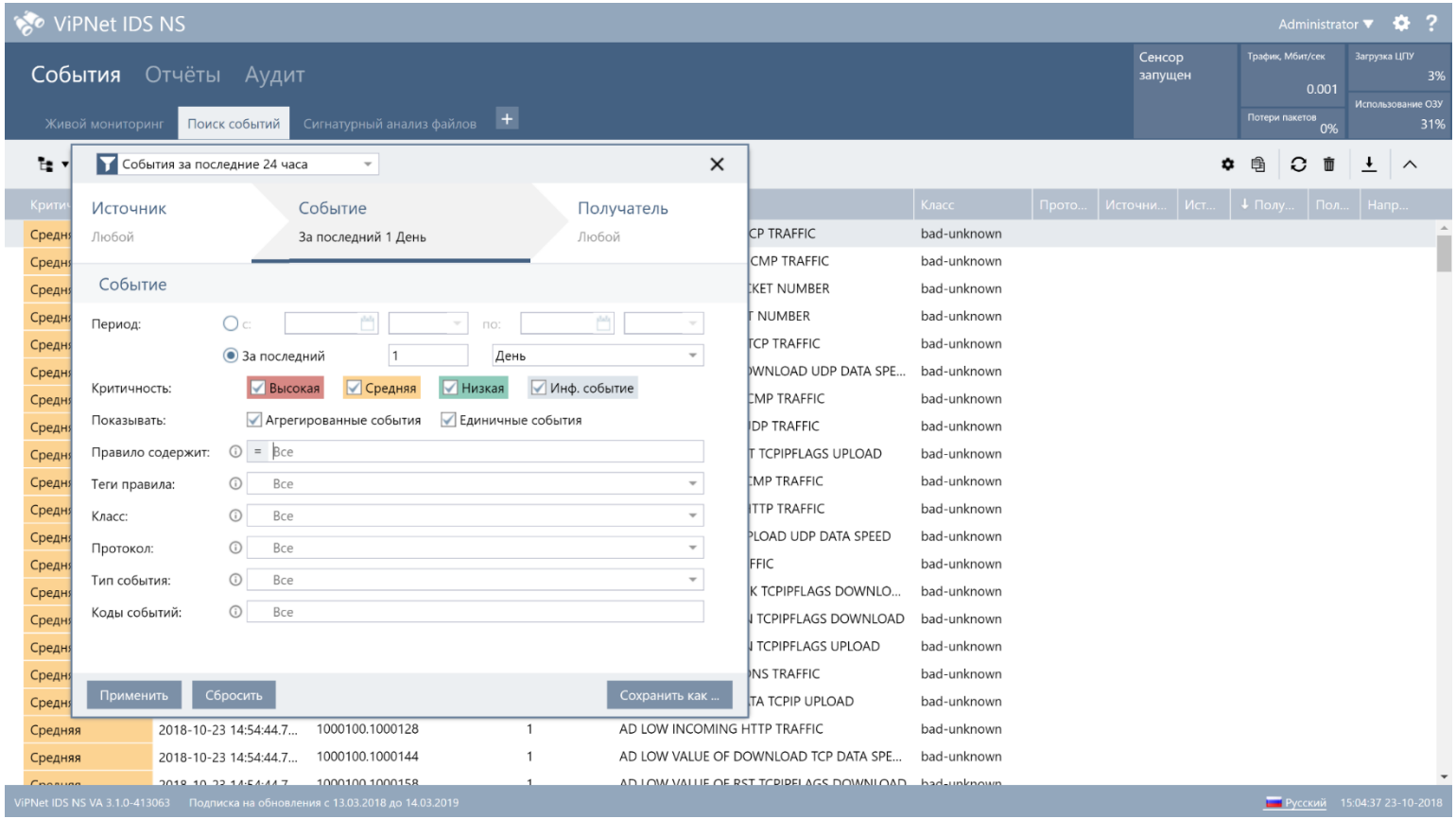
- **Оповещение**
  - web-интерфейс,
  - e-mail,
  - Syslog

- **Служебные функции –**
  - журнал аудита событий безопасности;
  - самотестирование,
  - контроль целостности.

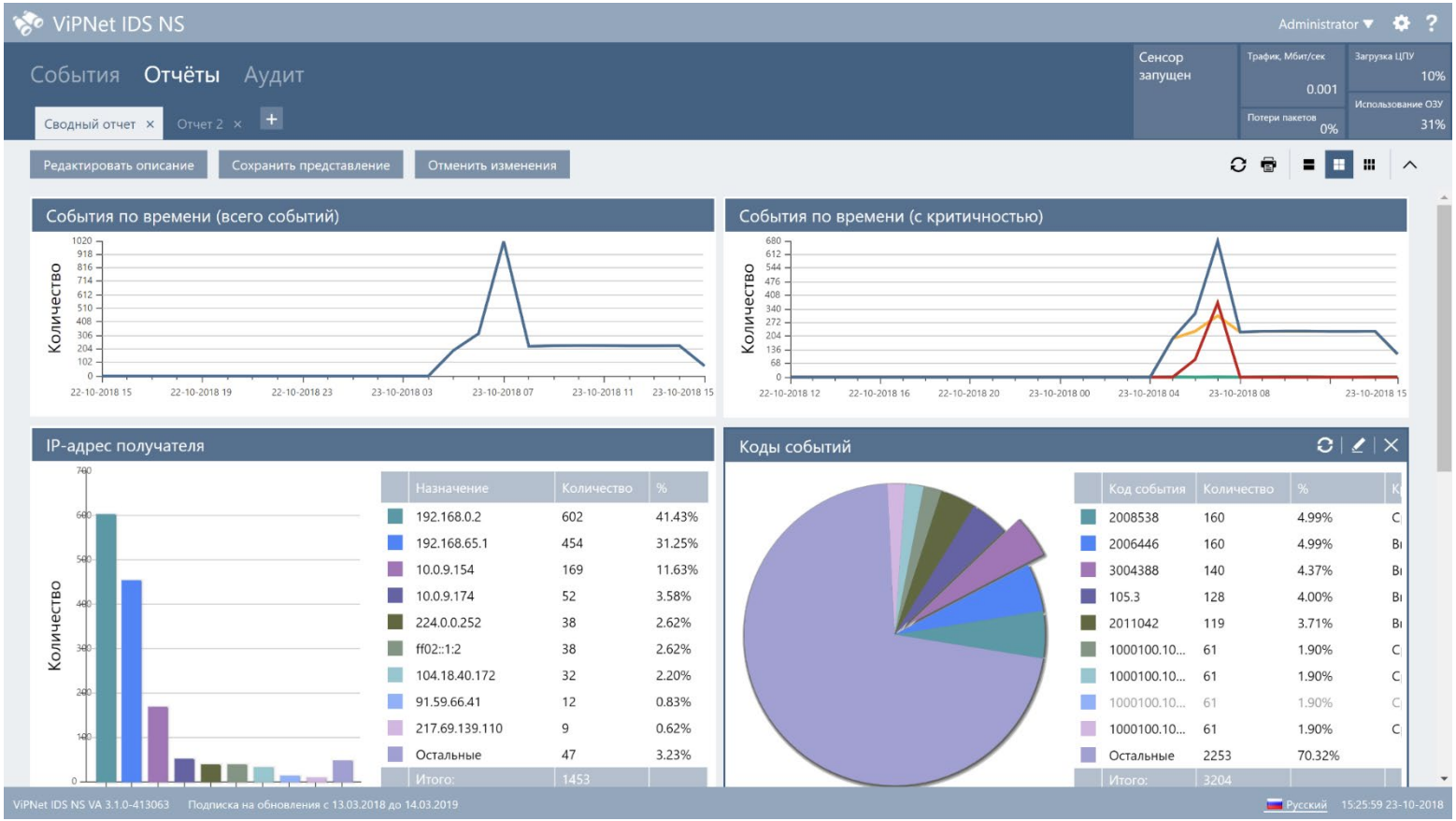
Панель живого мониторинга



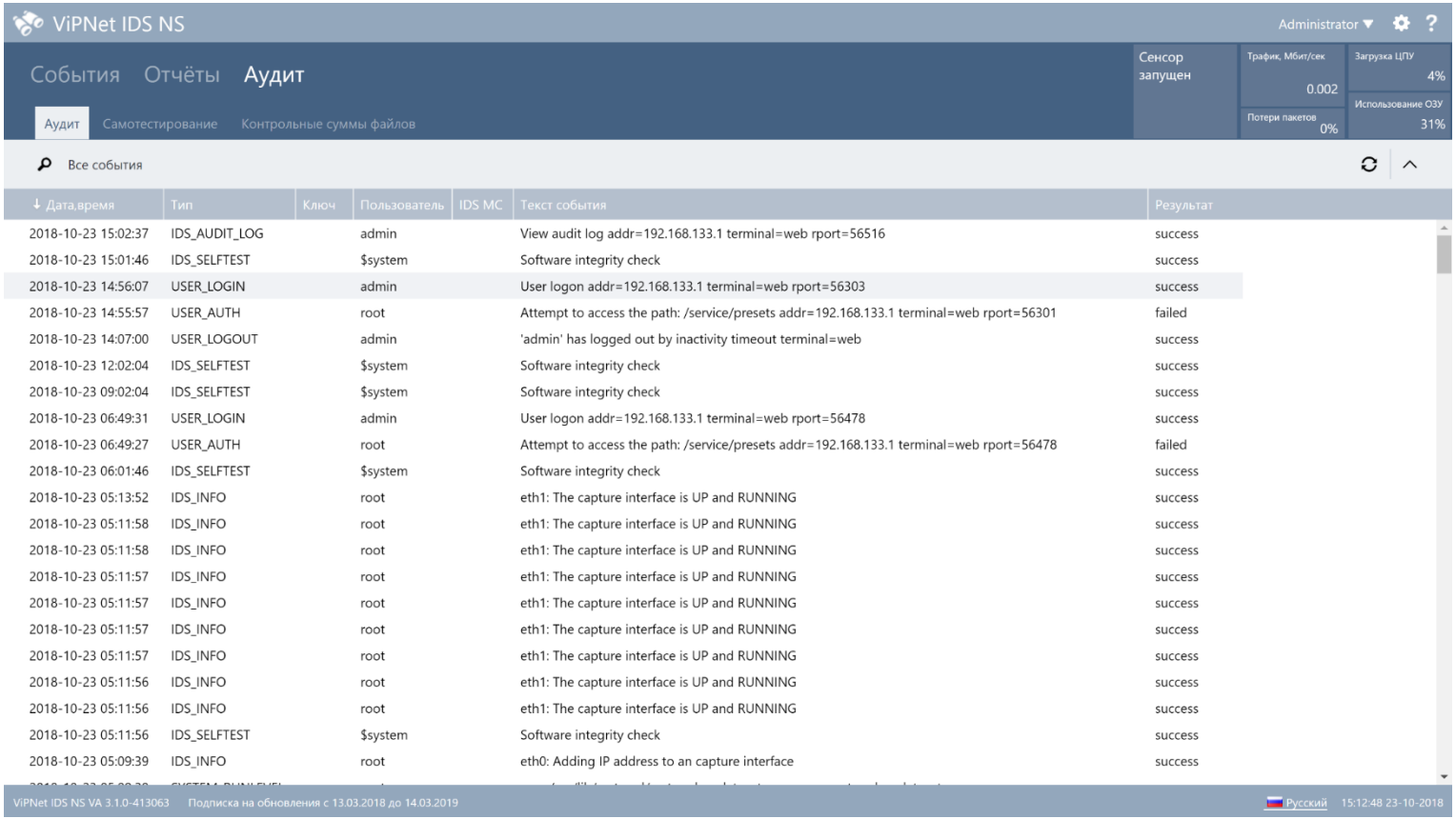
Поиск событий



Отчеты

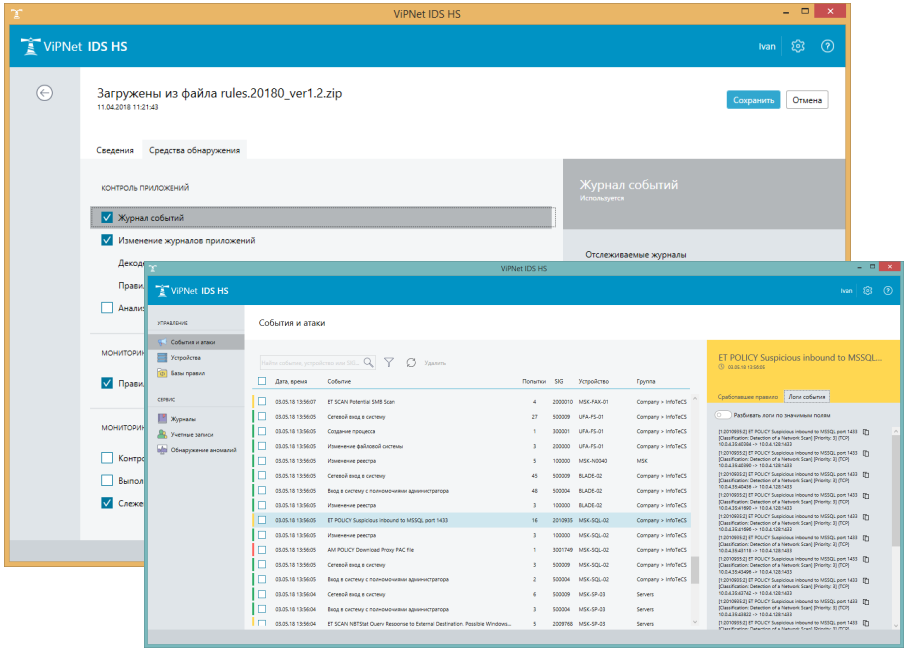


Сервисные функции



ViPNet IDS Host Sensor

- **Определять** атаки, которые “не видит” сетевой сенсор;
- **Обнаруживать** атаки после расшифровки входящего трафика;
- **Выявлять** подозрительную активность внутри ОС:
  - файловая активность,
  - изменения в реестре,
  - неизвестные процессы.



Сертификация IDS

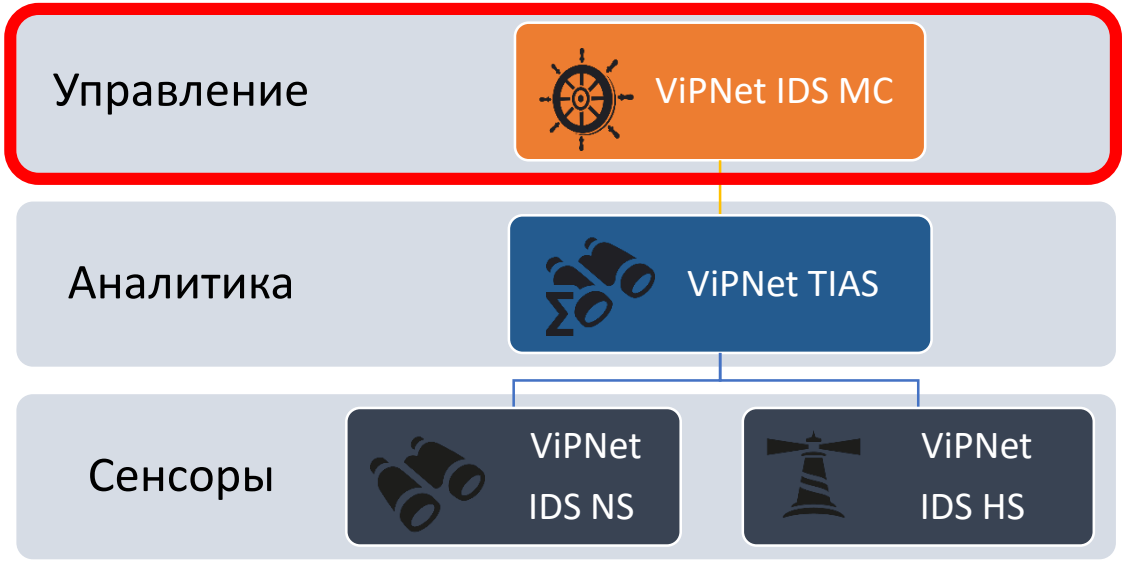
ФСТЭК

- **IDS NS —** СОВ уровня сети (до 4 класса)
- **IDS HS —** СОВ уровня узла (до 4 класса)

ФСБ

- СОА класс В (в составе IDS 3)

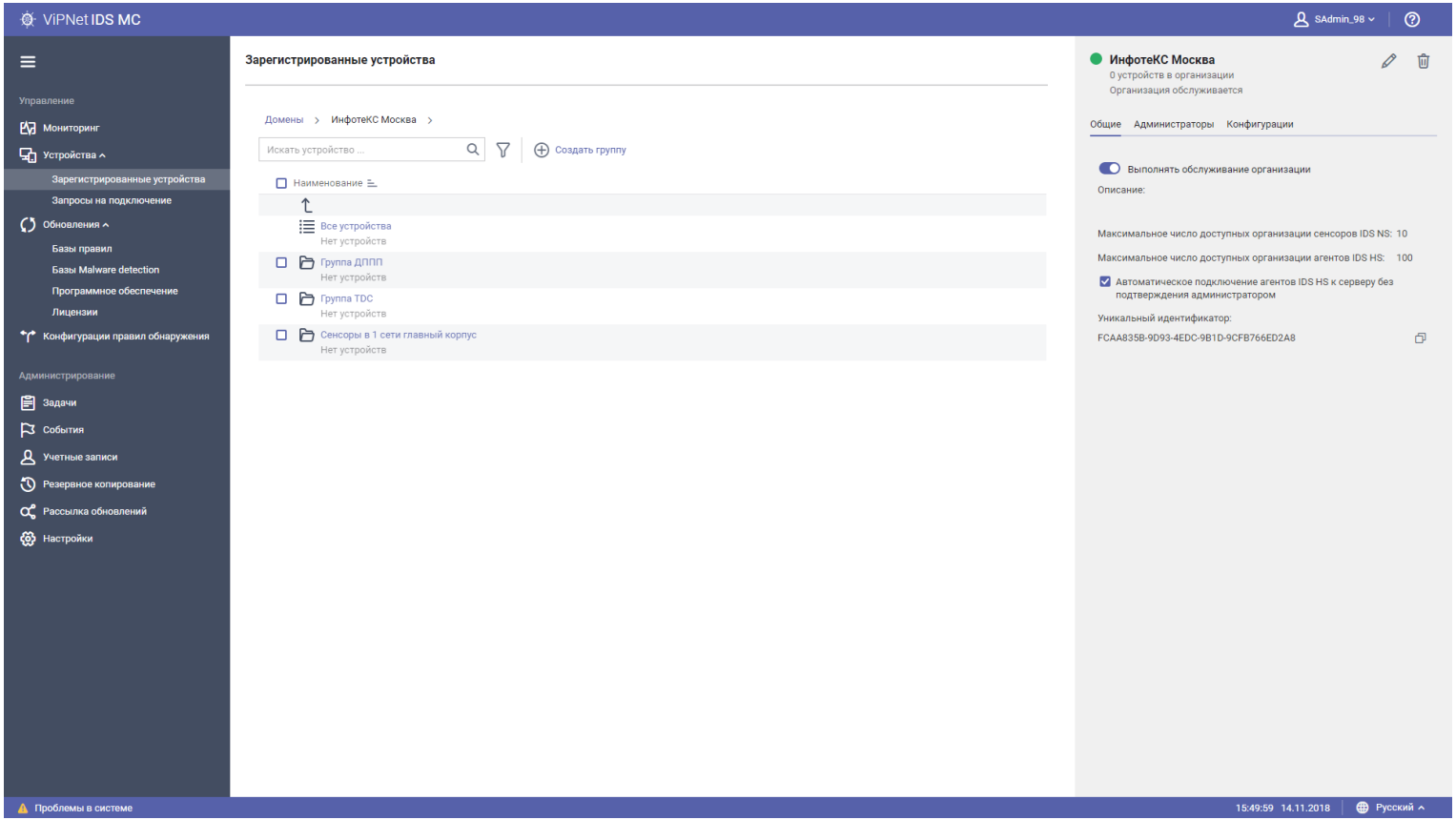
Система управления



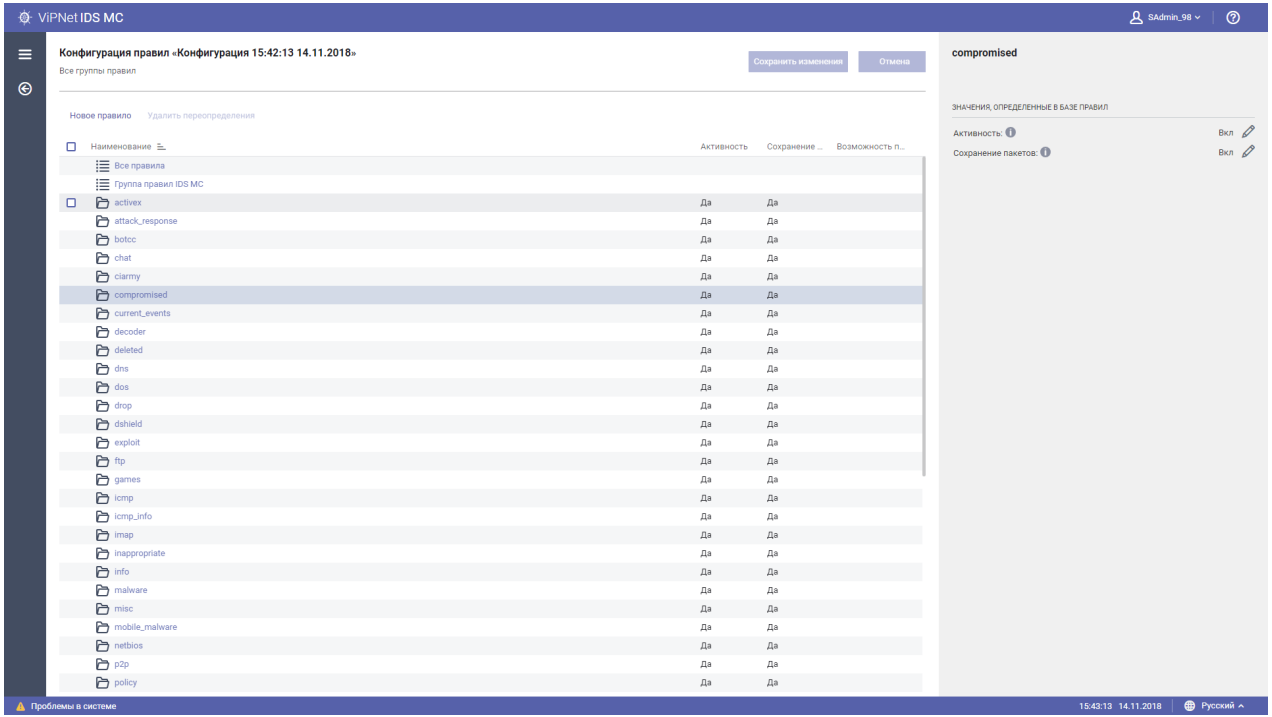
Система управления IDS MC

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

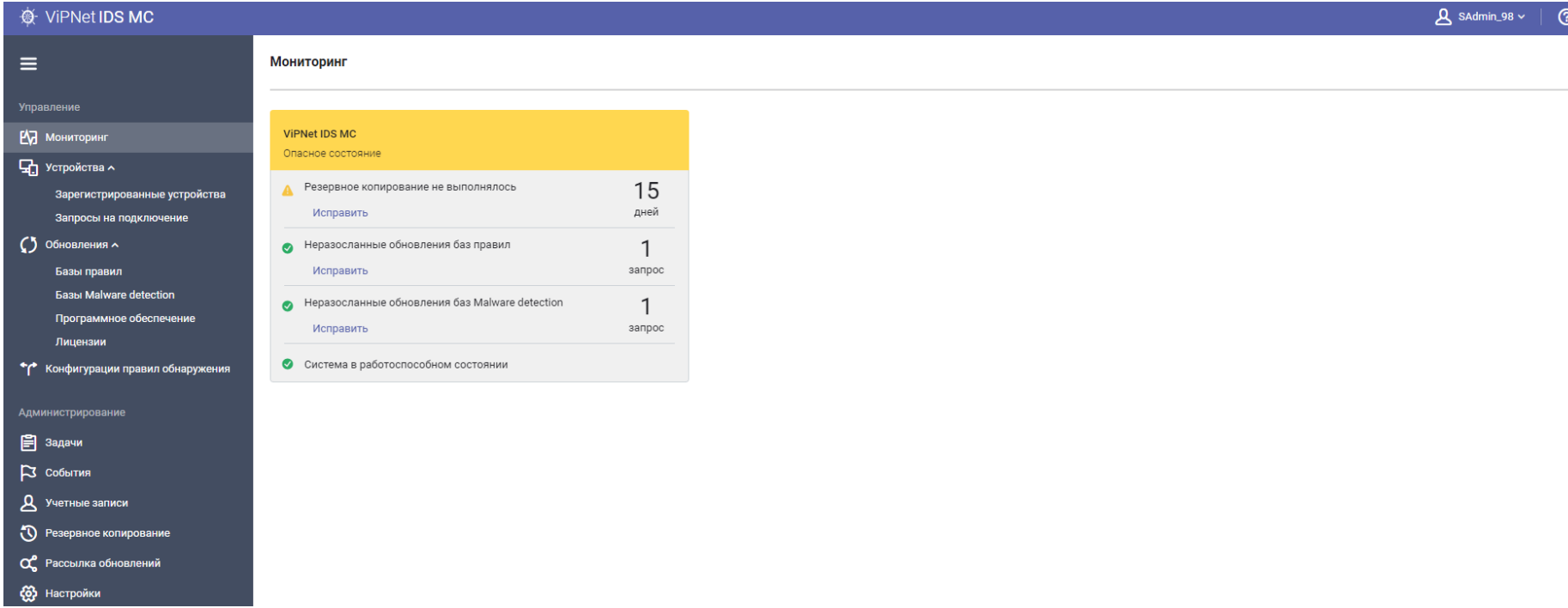
Управление сенсорами



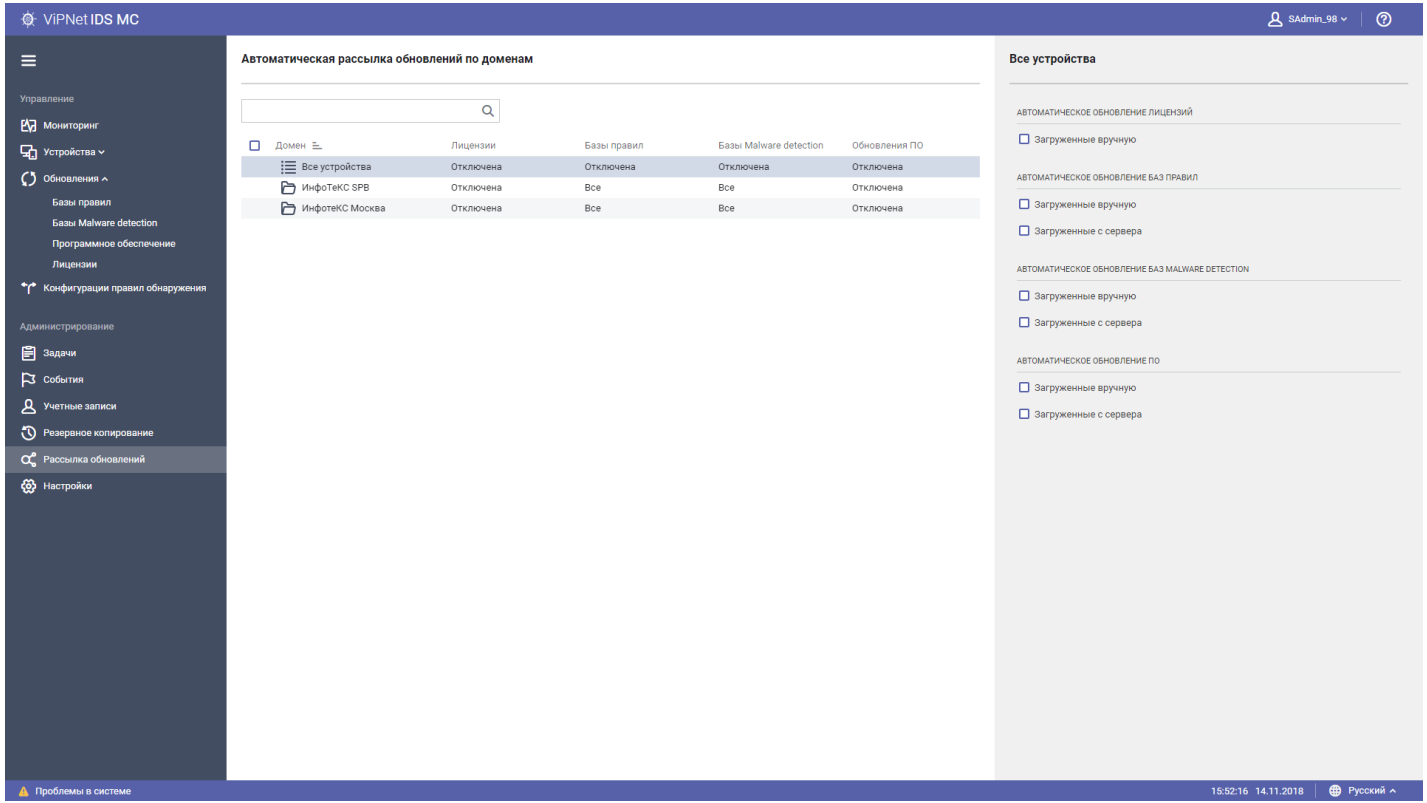
Управление конфигурациями правил



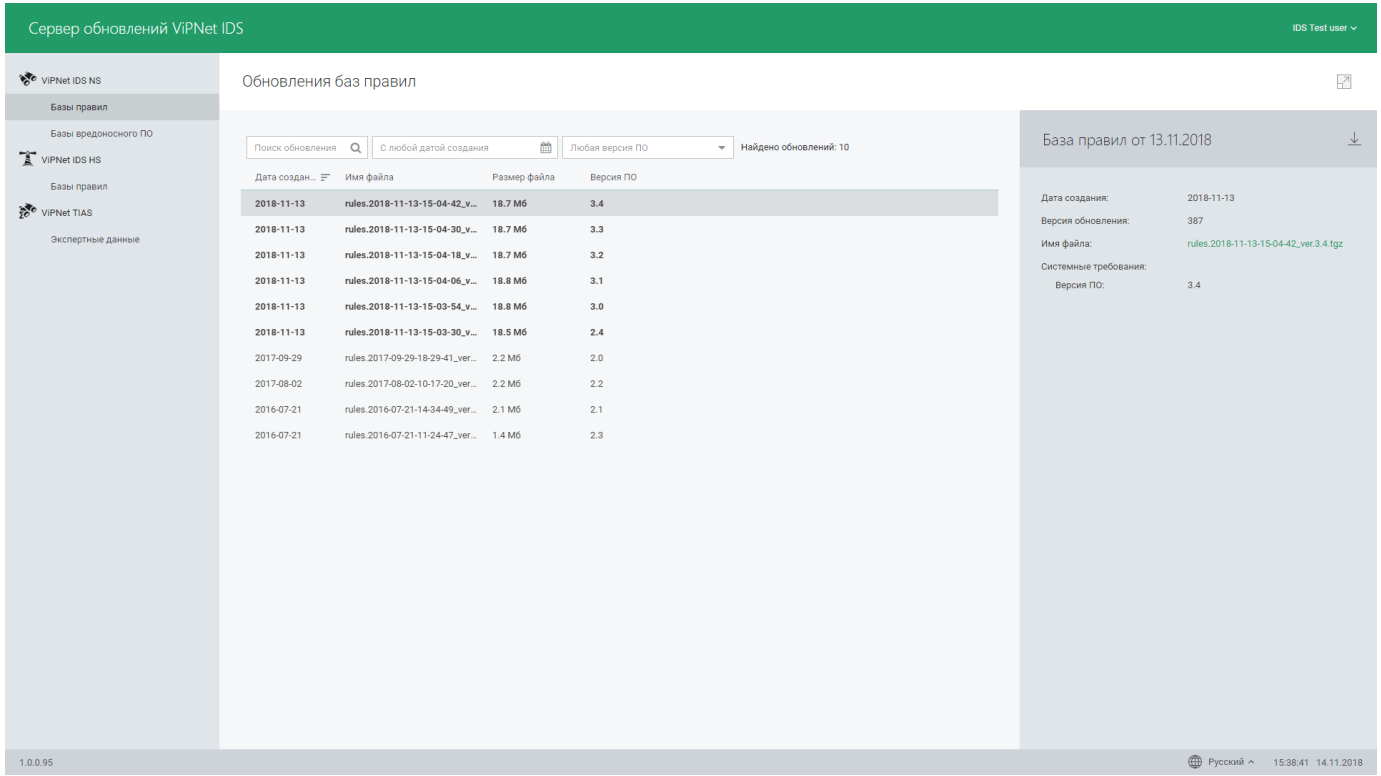
Мониторинг состояния



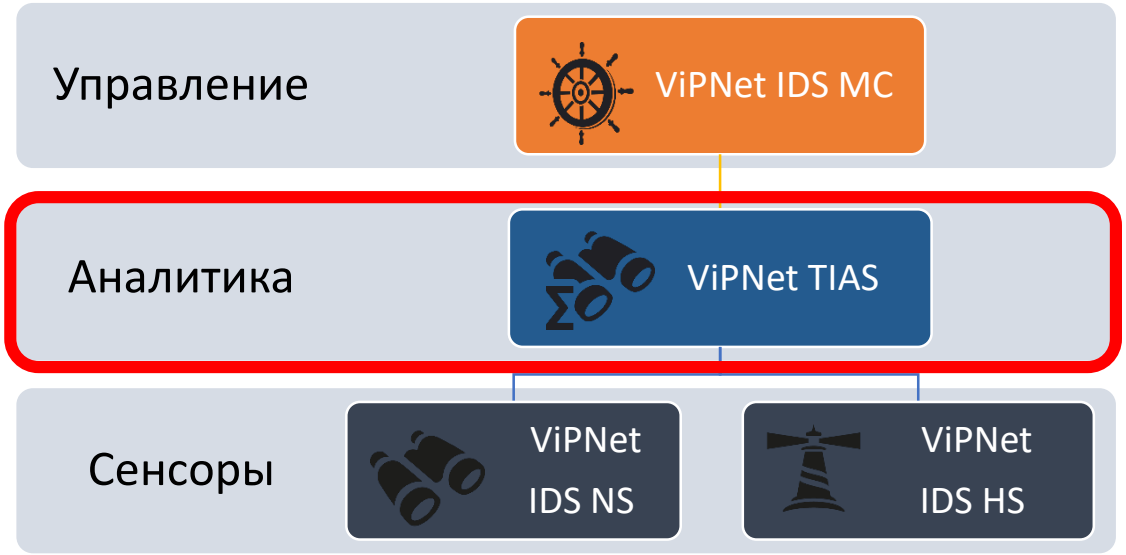
Обновления правил



Сервер обновлений ViPNet IDS



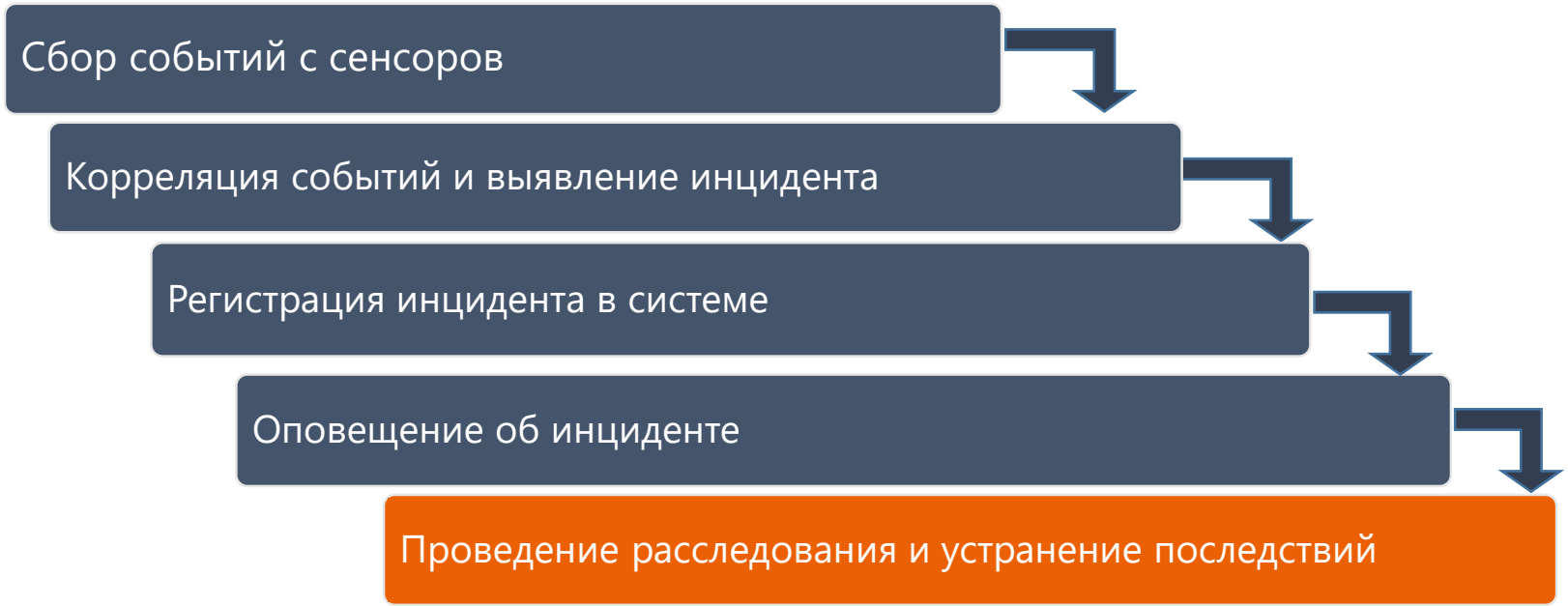
Система анализа



Основные функции ViPNet TIAS

- сбор и анализ событий от сенсоров ViPNet IDS;
- автоматическое выявление инцидентов;
- оповещение об инцидентах;
- инструменты для проведения расследований;
- формирование отчетов

Сценарий обработки событий



Как это работает?

Threat Intelligence

События ИБ

Модуль анализа
ViPNet TIAS

Инциденты ИБ

Статистика и отчеты

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:

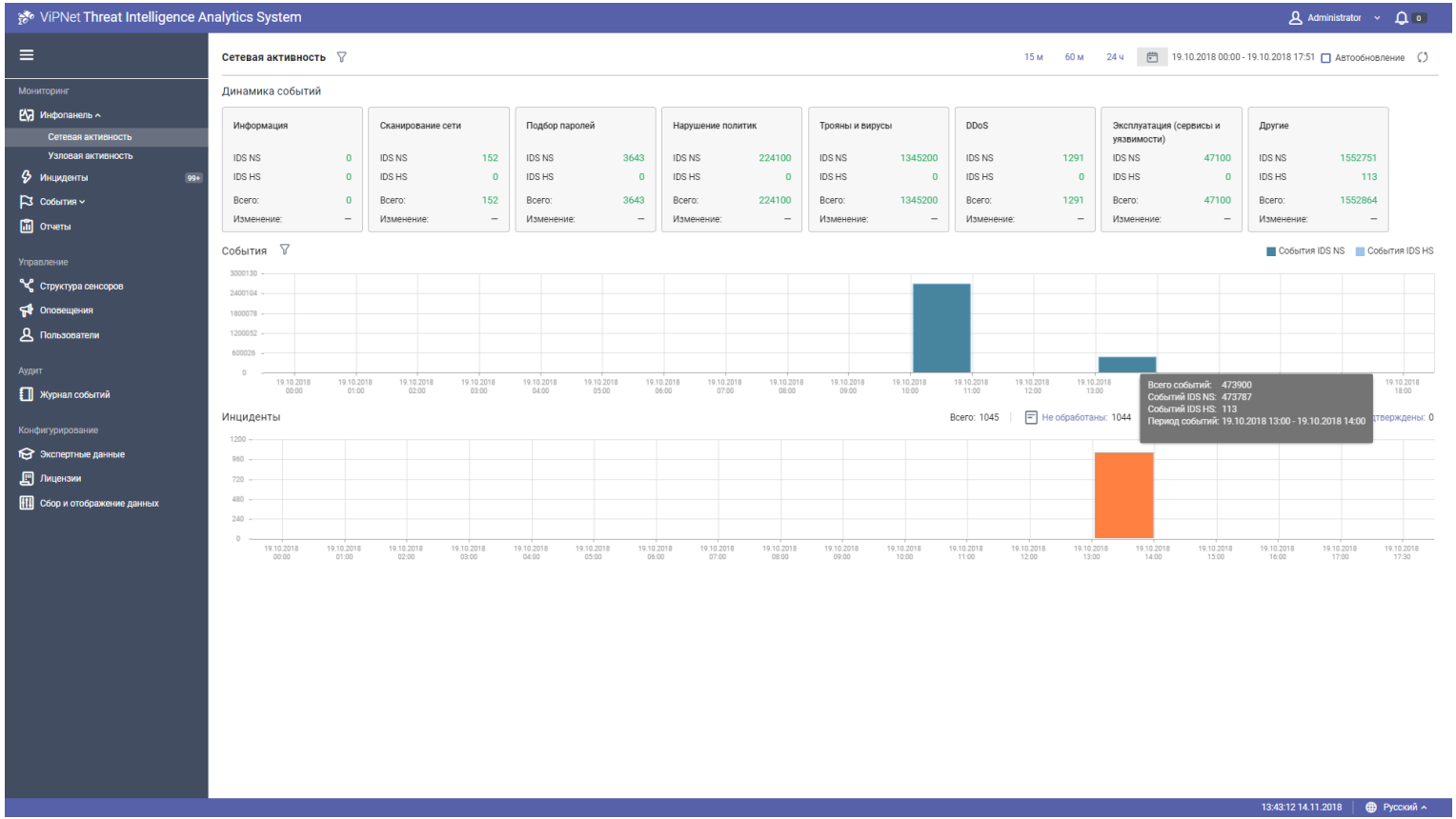
- **Индикаторы** атак и компрометации;
- **ТТП -** тактики, техники, процедуры;
- **Информационный обмен:**
- СОПКА, ФСТЭК, RU-CERT;
- **Опыт клиентов -** верифицированная и обезличенная информация

Комбинирование двух методов

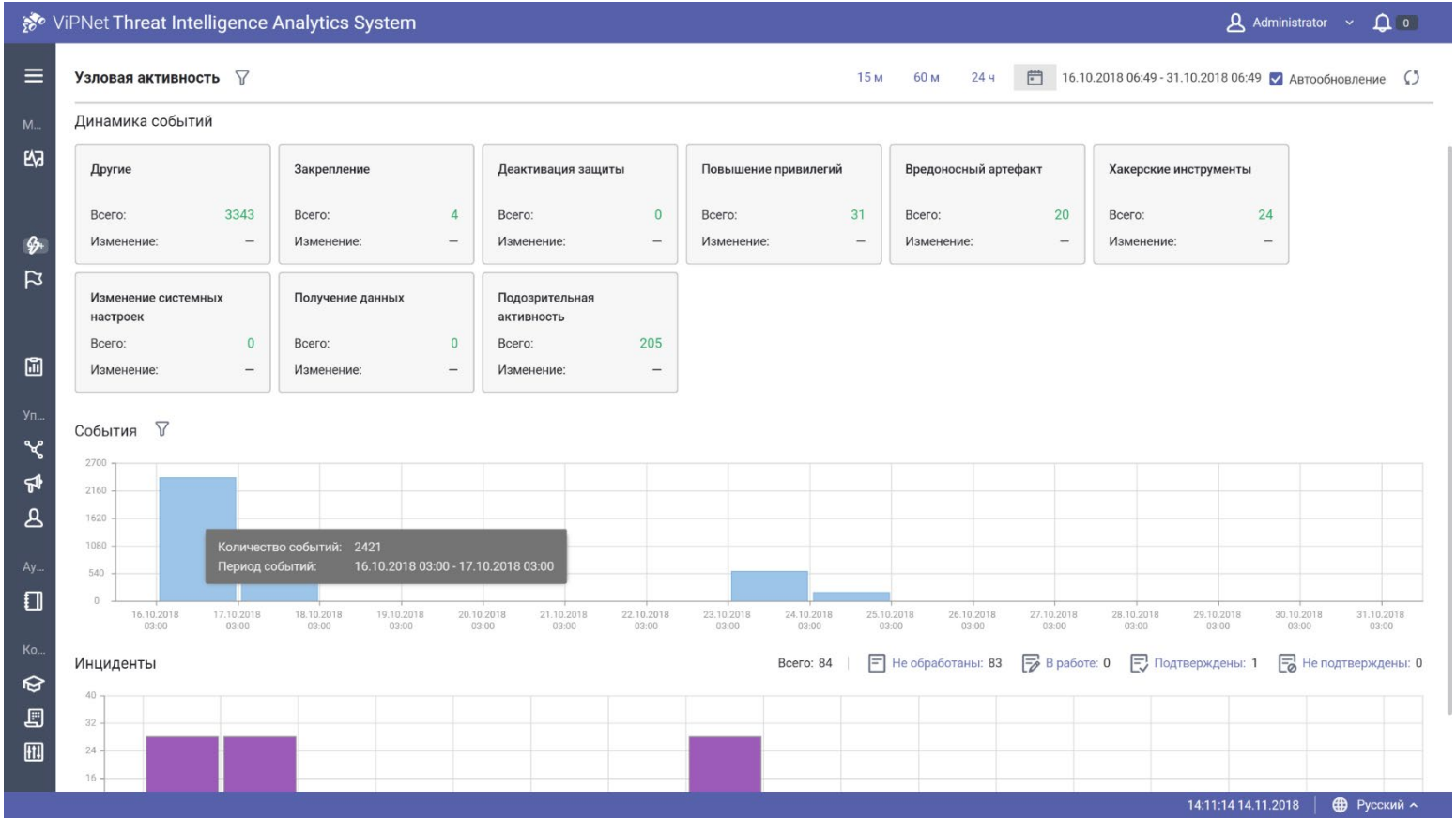
- **Сигнатурный метод —** на основе метаправил выявления инцидентов

- **Эвристический метод —** на основе машинного обучения математической модели принятия решений

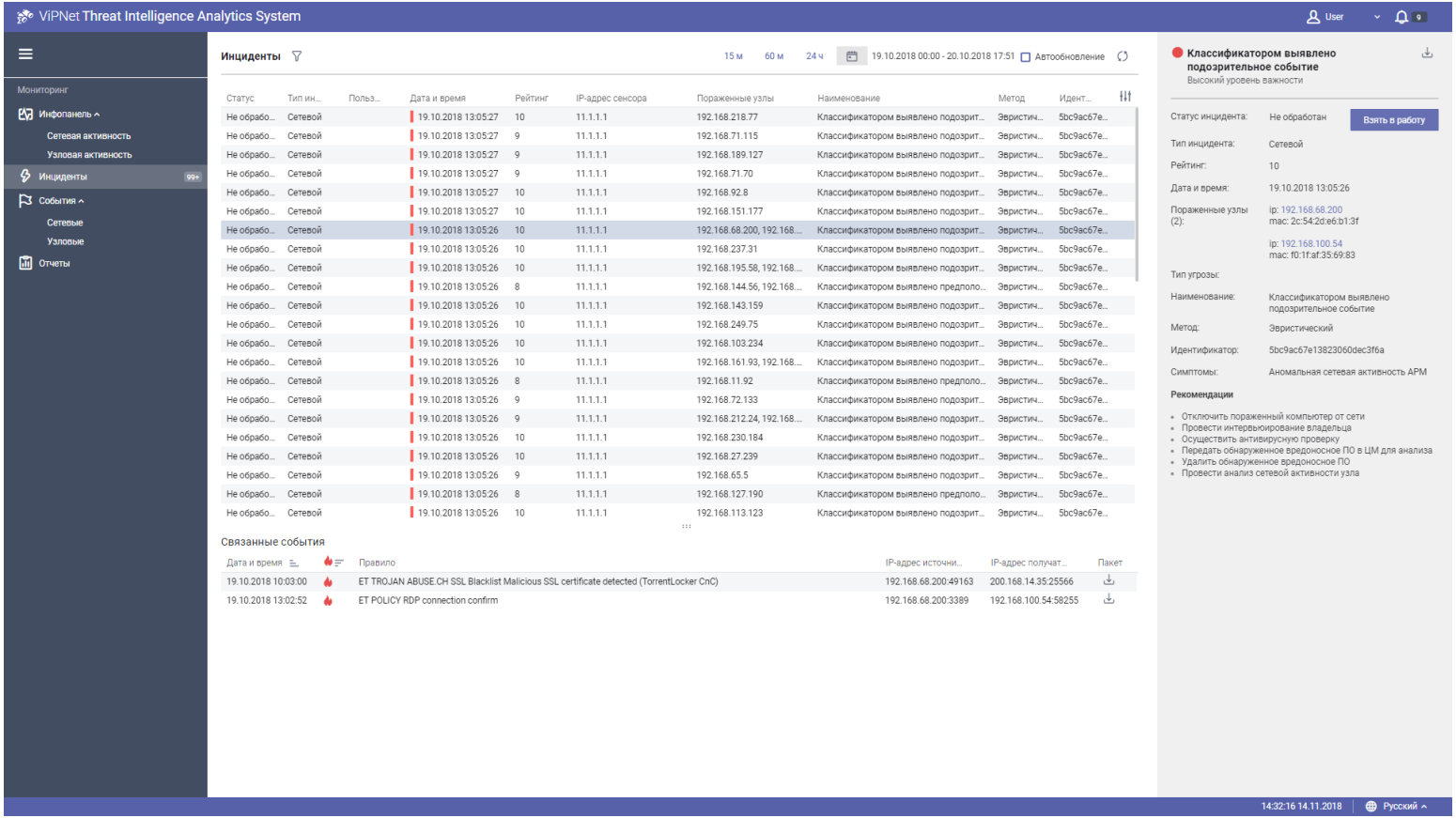
Сетевая активность



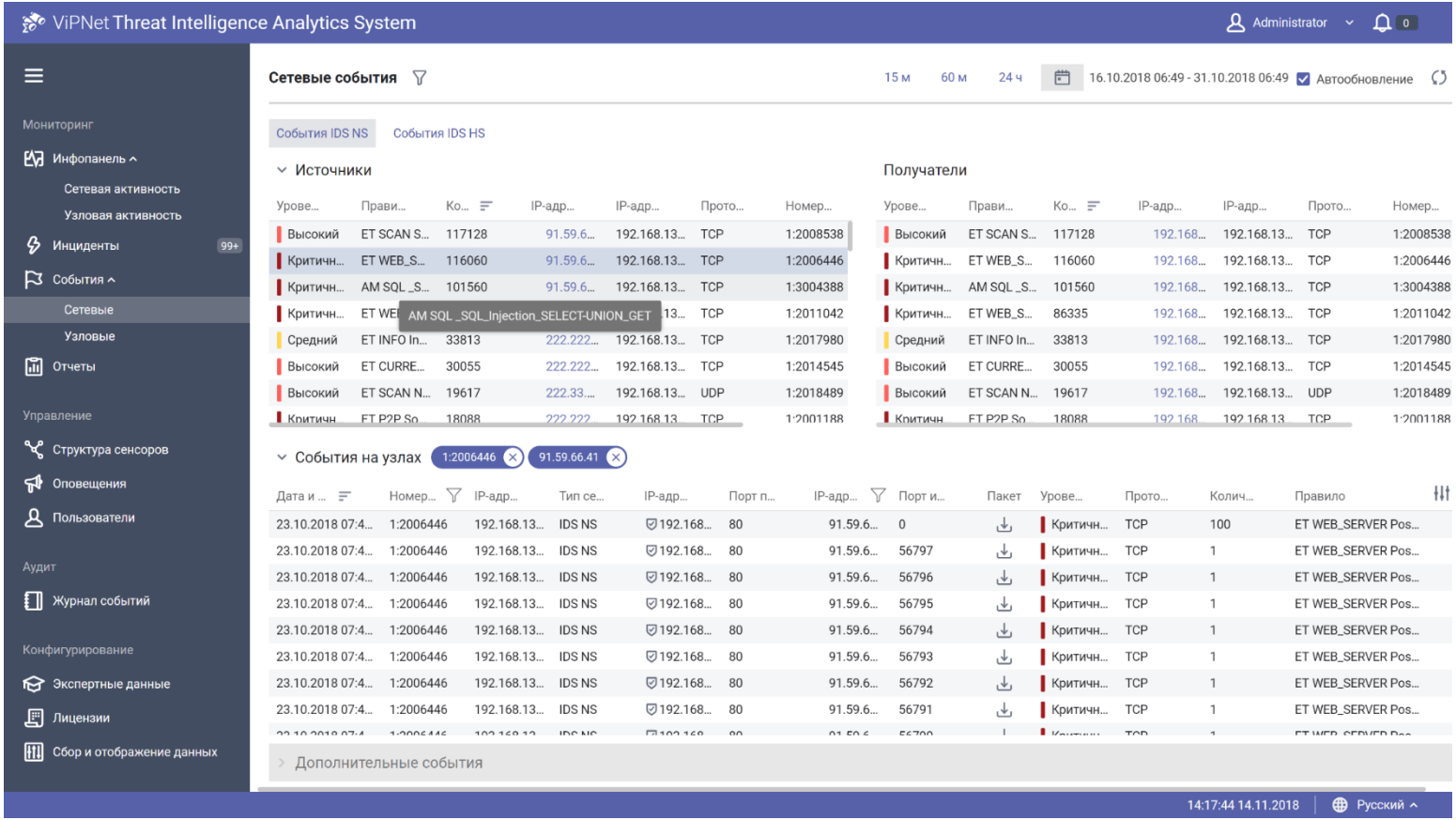
Узловая активность



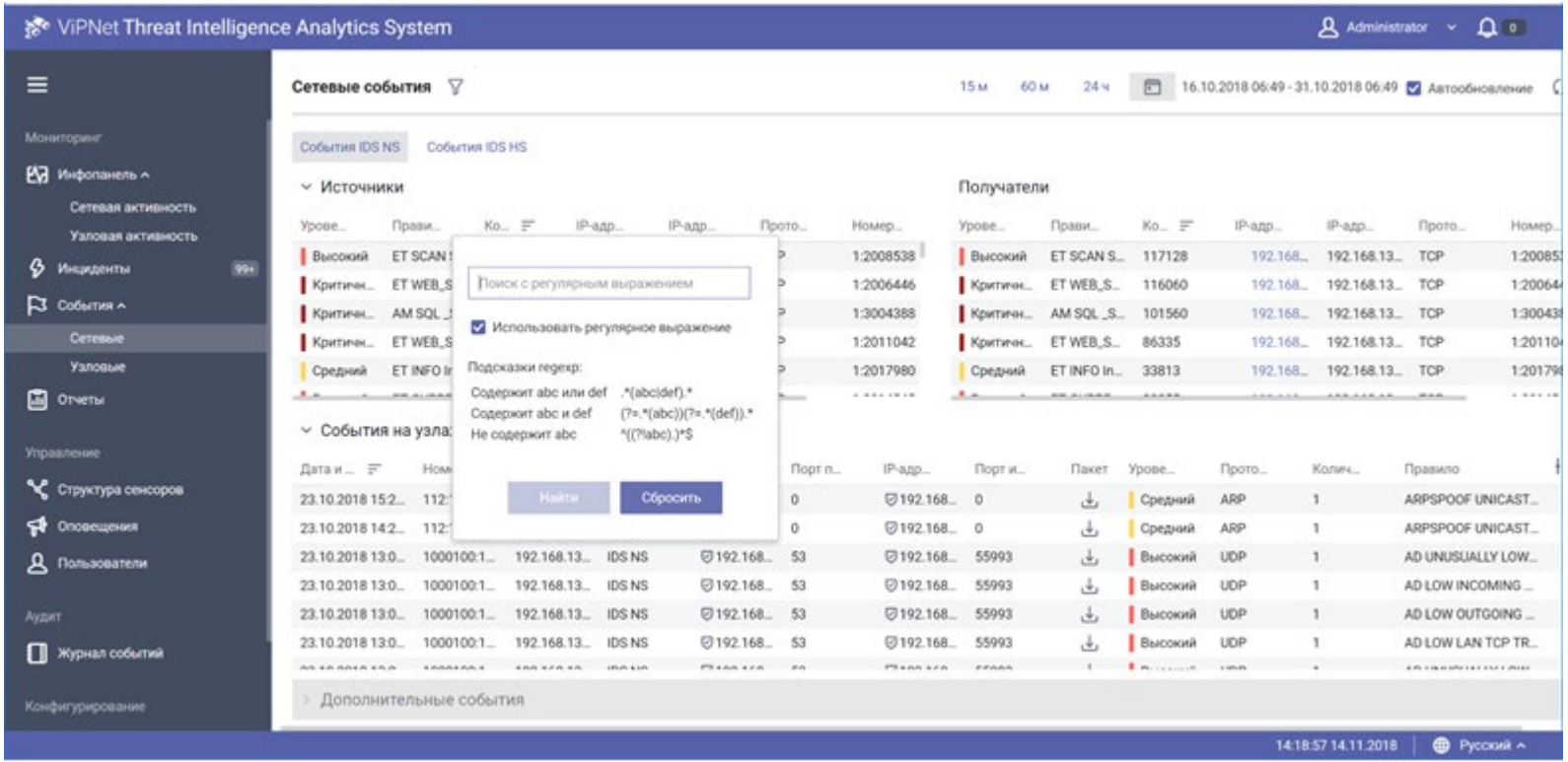
Инциденты



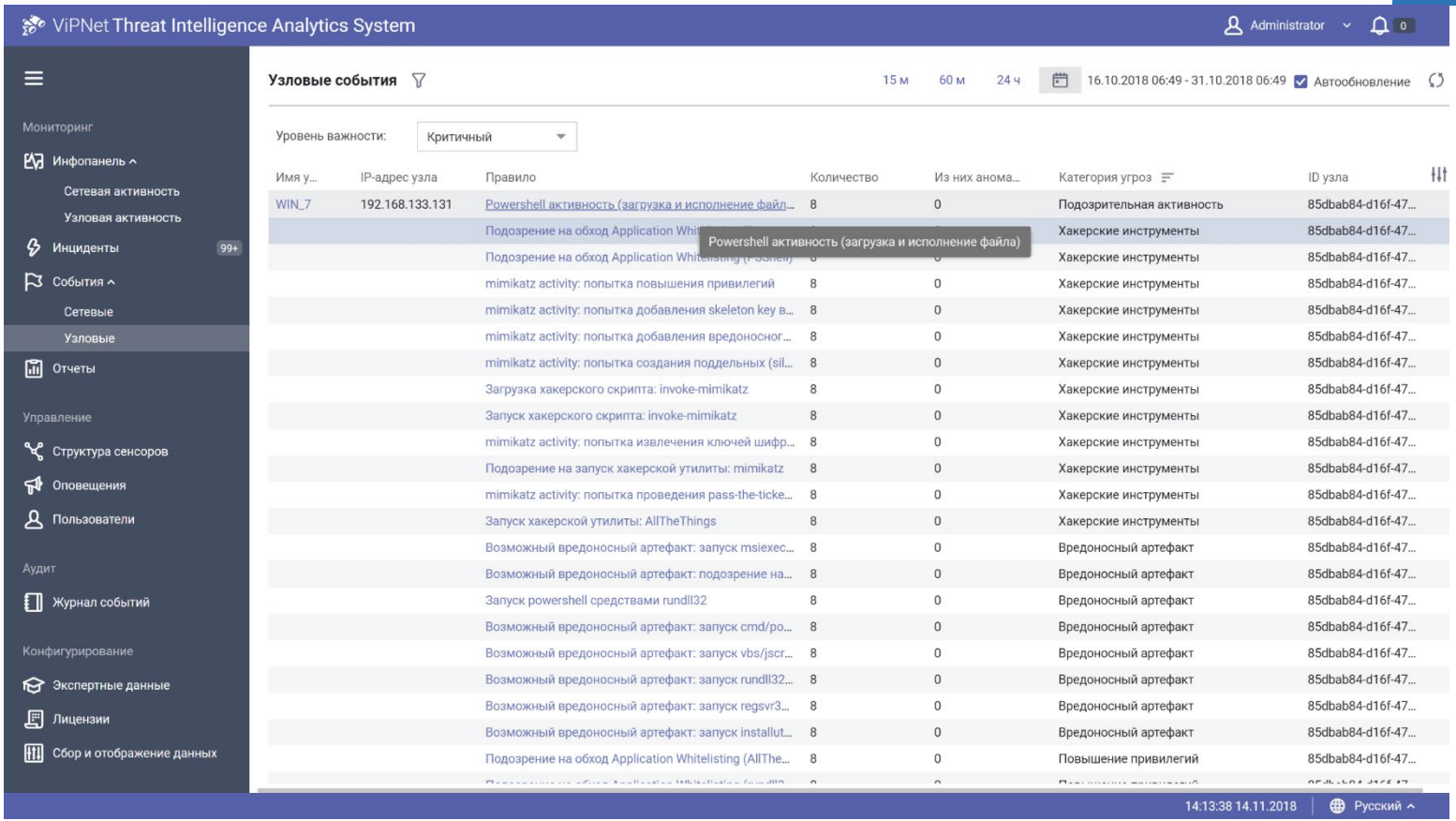
Сетевые события



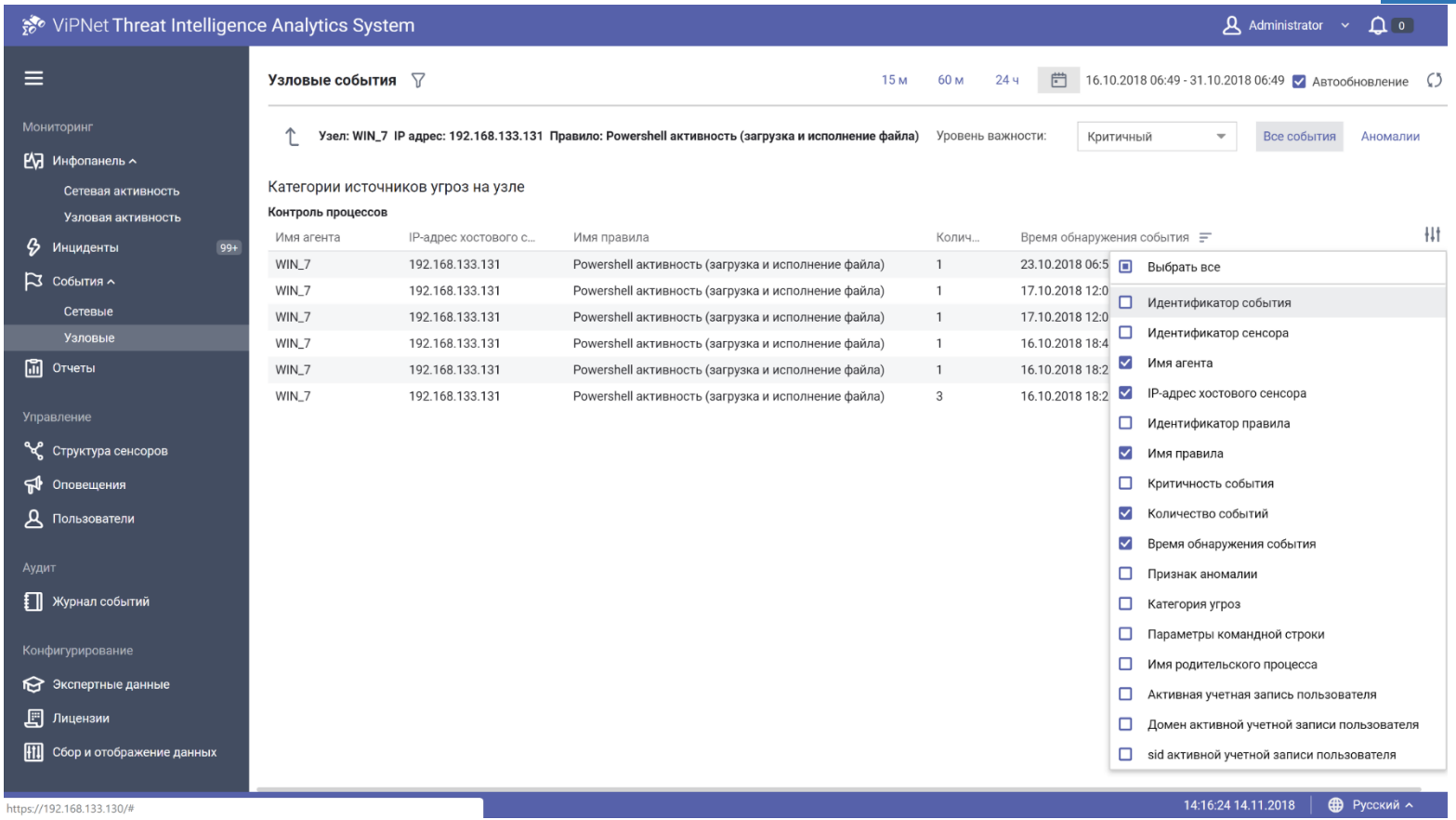
Поиск и фильтрация



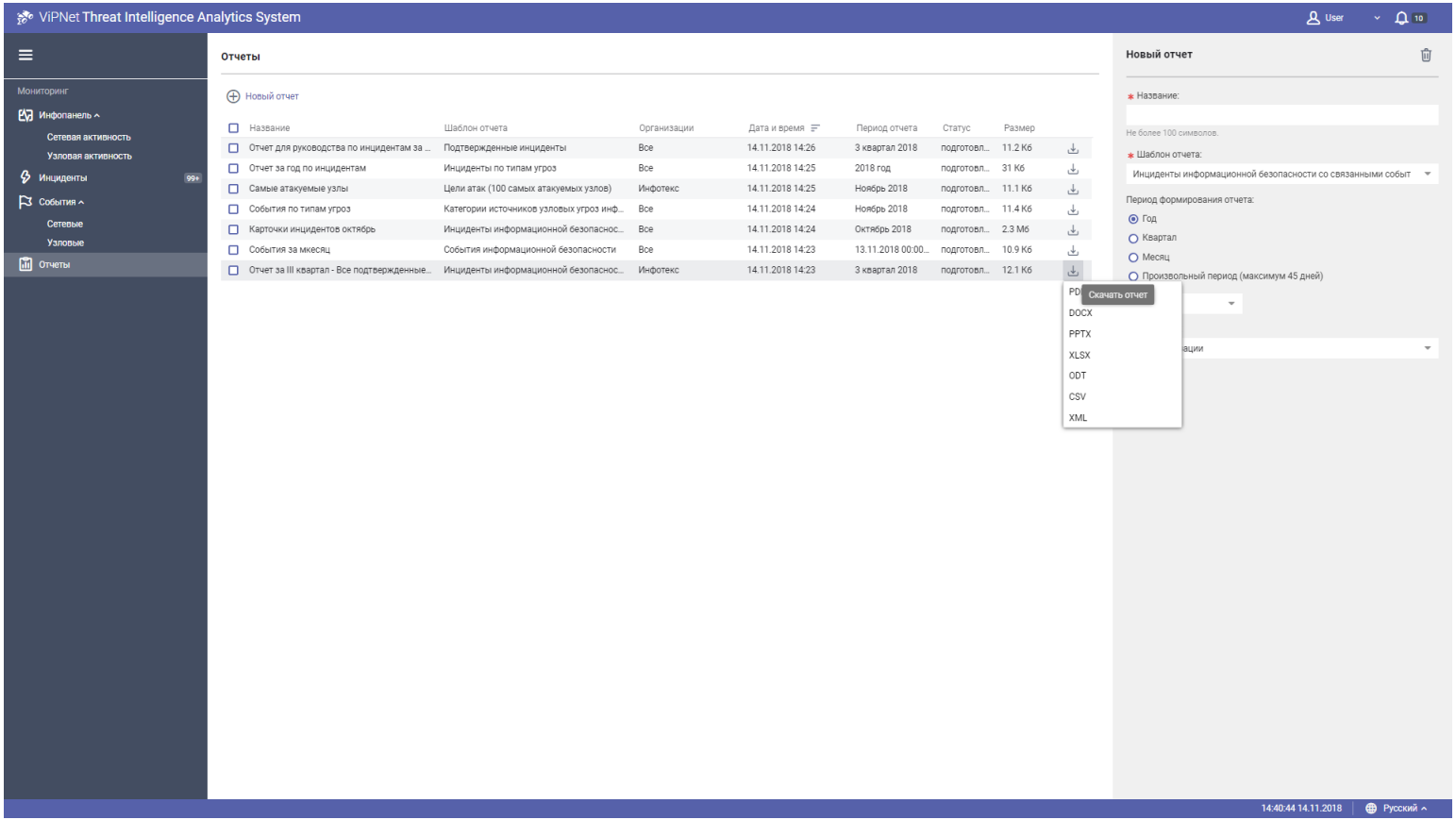
Узловые события



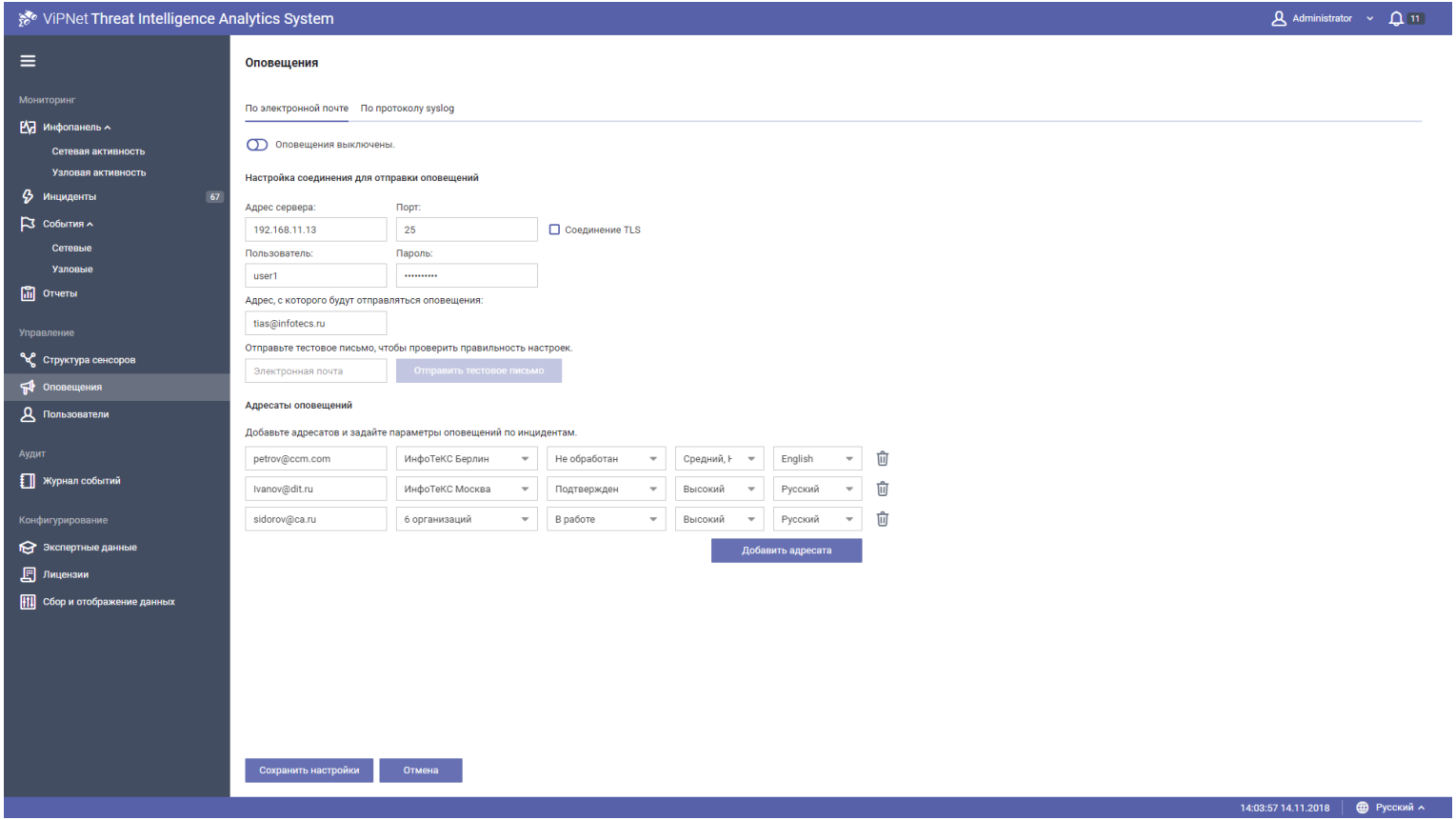
Узловые события детализация



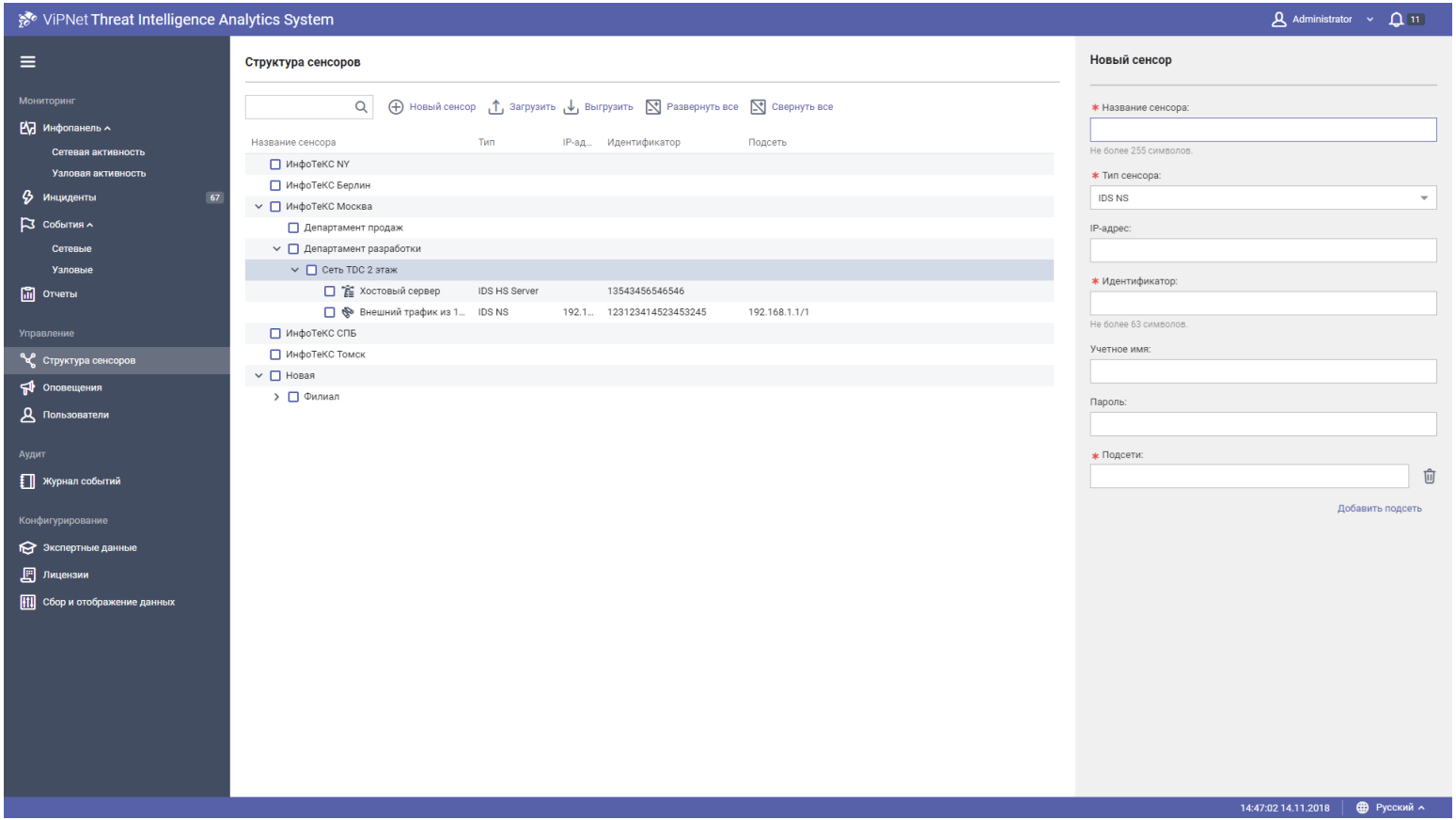
Отчеты



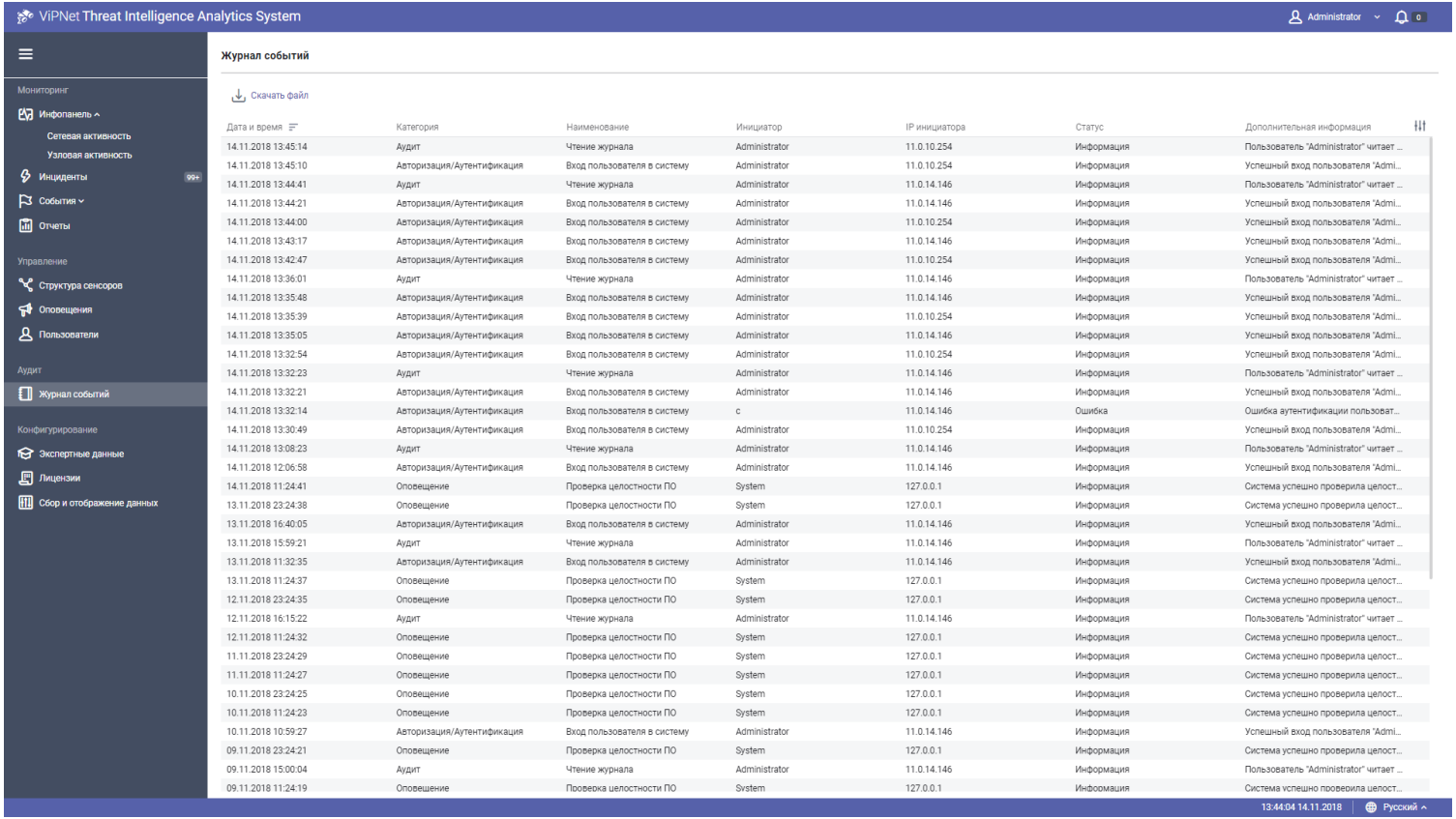
Оповещения



Многоуровневая структура



Журнал событий



Варианты исполнения ViPNet TIAS

Desktop

ПАК ViPNet TIAS 100

Server 1U

ПАК ViPNet TIAS 1000
ПАК ViPNet TIAS 2000
ПАК ViPNet TIAS 5000

Virtual Appliance

ViPNet TIAS VA

Сертификация

ФСТЭК

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

ФСБ

- СОА класс В (в составе IDS 3)

Меры по обеспечению безопасности для значимого объекта КИИ

VII. Предотвращение вторжений (компьютерных атак) (СОВ)		
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)	Для решения ViPNet базы решающих правил для выявления компьютерных атак, являющиеся частью политик предотвращения вторжений разрабатываются лабораторией ЗАО Перспективный Мониторинг, имеющей лицензию ФСТЭК. В ViPNet IDS NS и ViPNet IDS HS есть возможность написания собственных (пользовательских) правил и политик
СОВ.1	Обнаружение и предотвращение компьютерных атак	Все требования ФСТЭК к СОВ и ФСБ к СОА сетевого уровня и уровня узла закрываются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК и ФСБ
СОВ.2	Обновление базы решающих правил	Автоматическое централизованное обновление БРП на всех сенсорах с помощью ViPNet IDS MC

Приложение к Требованиям по обеспечению безопасности значимых объектов КИИ Российской Федерации, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239

Меры по обеспечению безопасности для значимого объекта КИИ

XII. Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	Политики реагирования на компьютерные инциденты разрабатываются экспертами компании ЗАО «Перспективный мониторинг» на основе анализа актуальных данных об угрозах, уязвимостях, инструментов и техник проведения атак. В ViPNet TIAS происходит выявление инцидентов и даются рекомендации по реагированию на них
ИНЦ.1	Выявление компьютерных инцидентов	Инциденты выявляются автоматически с помощью правил обнаружения инцидентов и математической модели принятия решений. Инциденты однозначно идентифицируются и регистрируются в системе
ИНЦ.2	Информирование о компьютерных инцидентах	В ViPNet TIAS настройкой оповещения заинтересованных лиц о произошедших инцидентах по e-mail либо передачей информации об инциденте во внешние системы. Есть возможность настройки информирования в зависимости от критичности инцидента, его статуса а так же контролируемого сегмента
ИНЦ.3	Анализ компьютерных инцидентов	ViPNet TIAS позволяет проводить глубокий анализ компьютерных инцидентов, предоставляя инструменты поиска и фильтрации данных в событиях, связанных с инцидентом, а так же предоставляя образцы исходного трафика и описания правил выявления событий безопасности
ИНЦ.4	Устранение последствий компьютерных инцидентов	Карточка инцидента в ViPNet TIAS содержит информацию о пострадавших в результате компьютерного инцидента активах, а так же рекомендации по устранению его последствий

Решение для оказания услуг мониторинга

№	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.

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79

Планы

- Соответствие требованиям по взаимодействию с ГосСОПКА;
- Соответствие требованиям к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты и требованиям к системам КИИ;
- Облачная версия TIAS с мультиарендным режимом работы;
- Обогащение информации об инцидентах.

Преимущества решения от ИнфоТеКС

Продукты и техподдержка от ИнфоТеКС

Авторизованные курсы от Учебного центра ИнфоТеКС

Экспертиза и сервисы от Перспективного мониторинга

Эффективное работающее решение!


infotecs
Вопросы