A person in a dark suit and tie is holding a large, metallic, 3D-rendered gear. The gear is the central focus, with several other smaller gears and mechanical parts floating around it, creating a sense of depth and complexity. The background is a blurred office setting.

# Системы обнаружения вторжений

Светлана Старовойт,  
Руководитель направления, ОАО ИнфоТеКс  
[StarovoytSG@infotecs.ru](mailto:StarovoytSG@infotecs.ru)

A high-angle photograph of a business meeting. Three people are seated around a wooden table. A woman on the left is using a tablet. A man on the right is using a smartphone. A woman in the foreground is looking at a notebook. A laptop is open in the background. A semi-transparent white box is overlaid on the bottom right of the image, containing the text 'Немного теории'.

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

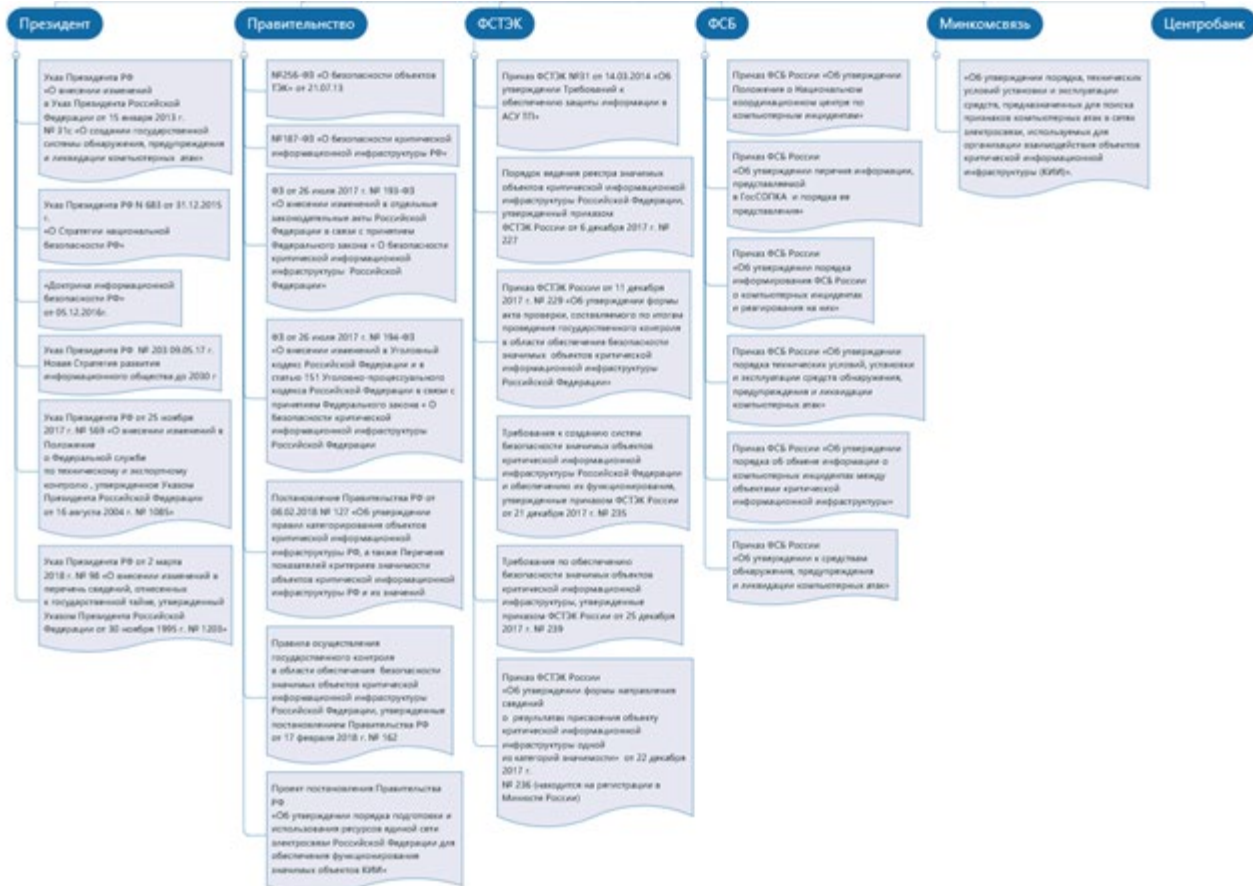
# Система обнаружения атак

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



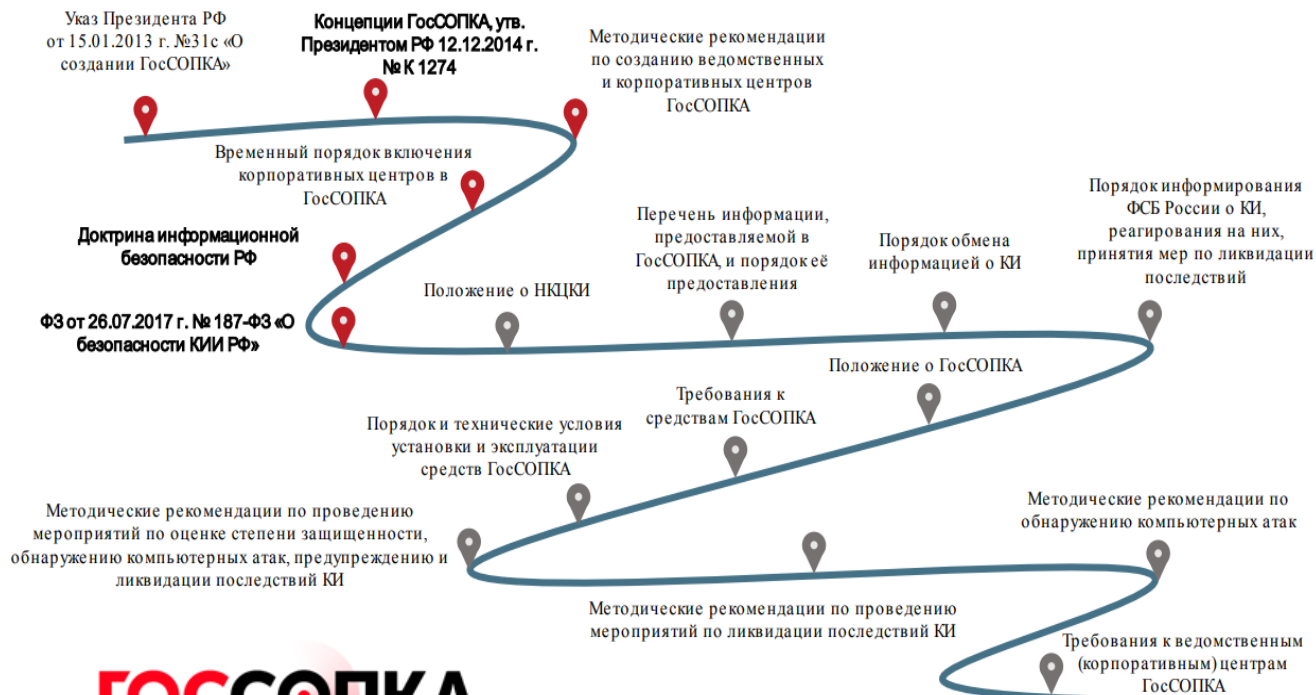
№	Предъявляемые требования	Класс	Класс	Класс	Класс
		Г	В	Б	А
1.	Обнаружение атак	*	=	+	
2.	Реакция на обнаруженную атаку	*	+	+	
3.	Контролируемые ресурсы АИС	-	*	+	
4.	Контролируемые протоколы	*	=	+	
5.	Управление СОА	*	=	+	
6.	Маскирование	-	*	+	
7.	Наличие механизмов собственной защиты	*	+	+	
8.	Оптимизация/модернизация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

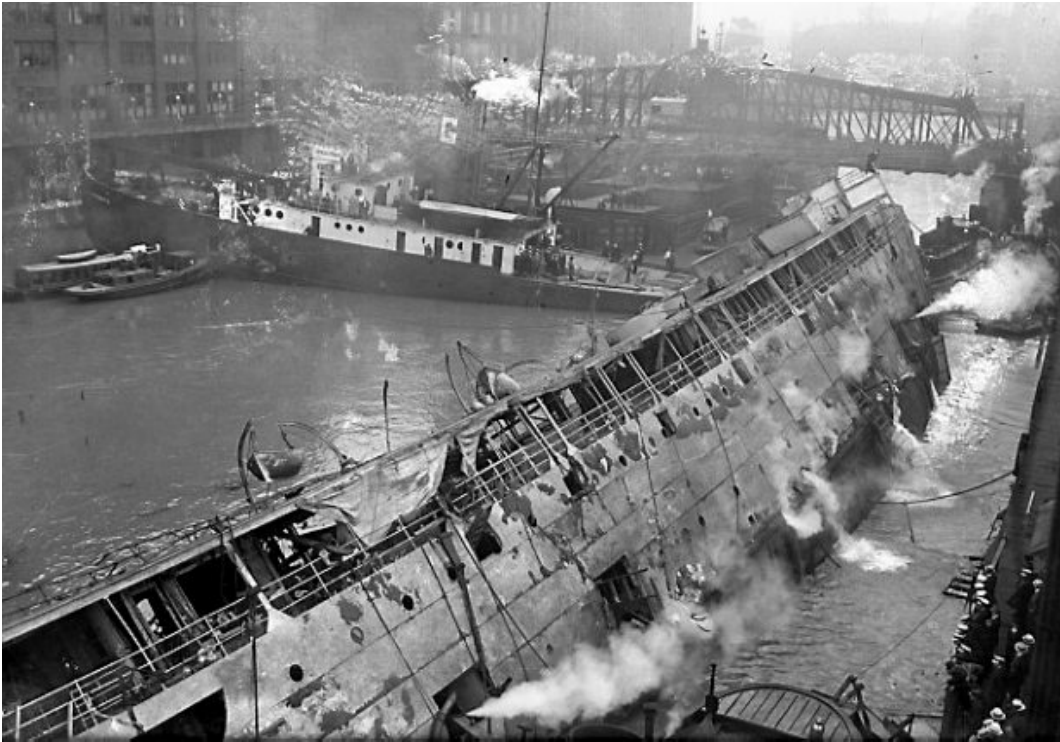
# Обеспечение выполнения следующих задач:

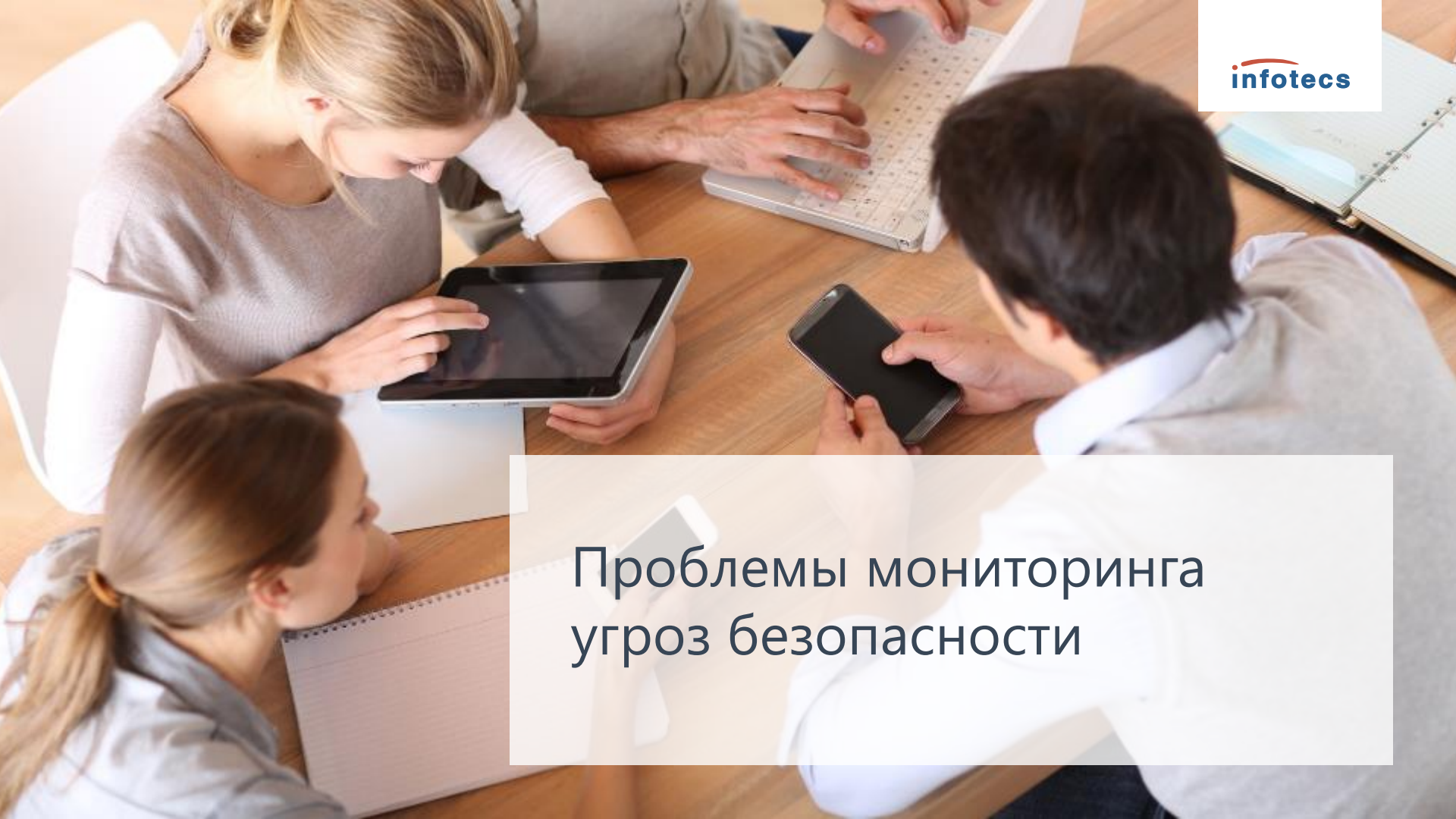
- обнаружение компьютерных атак;
- предупреждение компьютерных атак;
- ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;
- поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ;
- криптографическая защита обмена 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



A high-angle photograph of four business professionals sitting around a wooden table. A woman on the left is using a tablet, a man on the right is using a smartphone, and another woman in the foreground is looking at a laptop. The scene is brightly lit, suggesting a modern office environment.

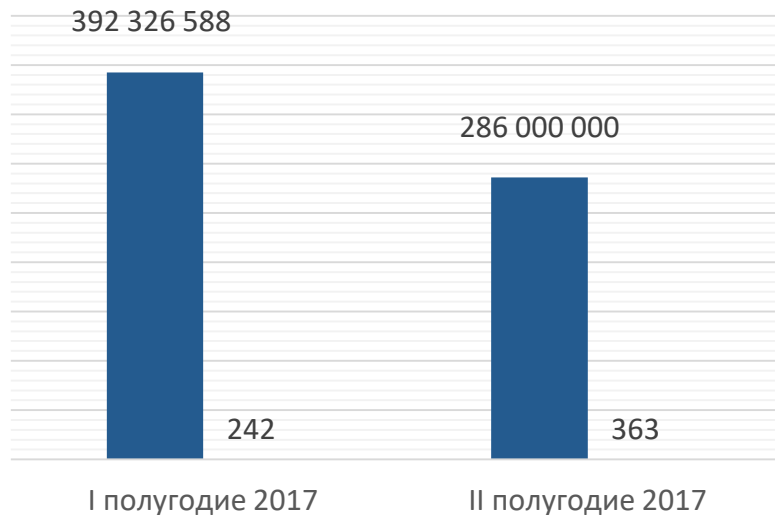
## Проблемы мониторинга угроз безопасности

# Сколько событий обрабатывает SOC?



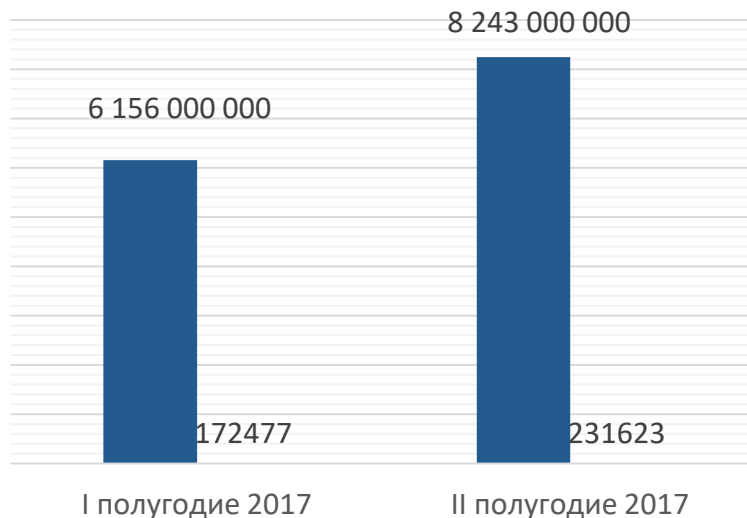
ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

■ События ■ Инциденты



SOLAR  
SECURITY  
software&services

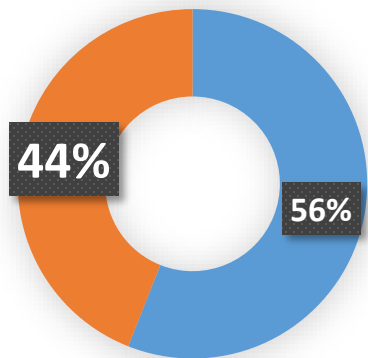
■ События ■ Инциденты



# Результаты исследований

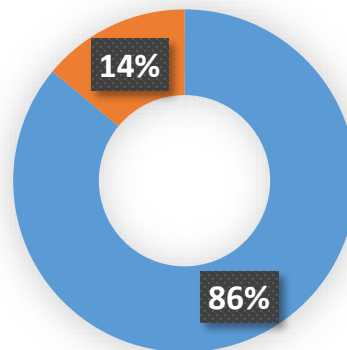
## Предупреждения от средств ИБ

- Были изучены
- Не были изучены

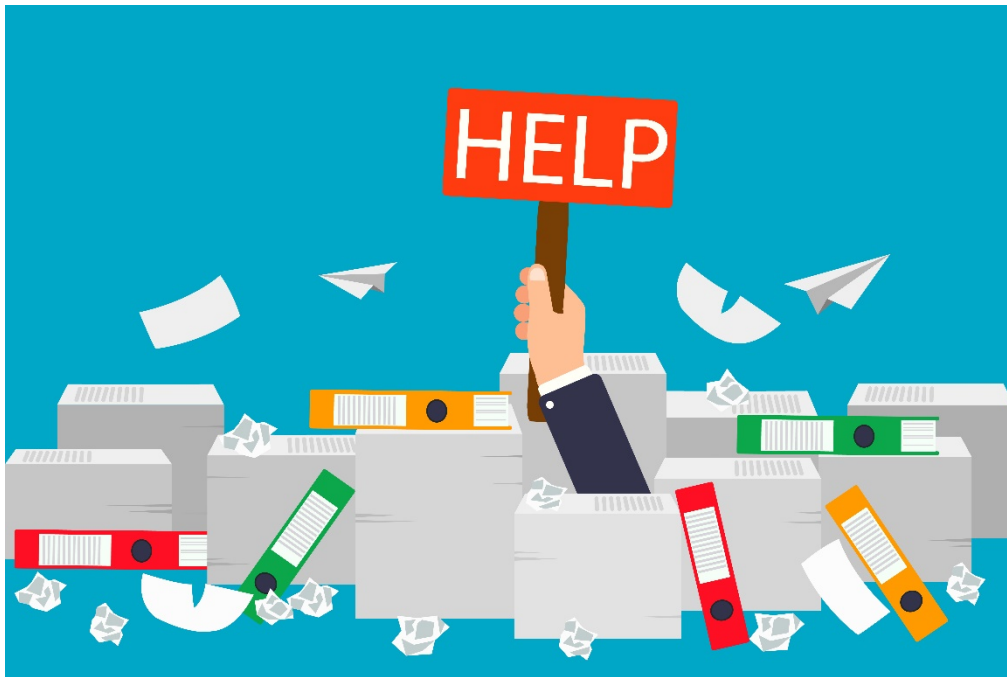


## Причины утечек

- Доказательства были в логах
- Отсутствие доказательств



# Важные события остаются незамеченными



Средства ИБ создают  
«информационный  
шум»!

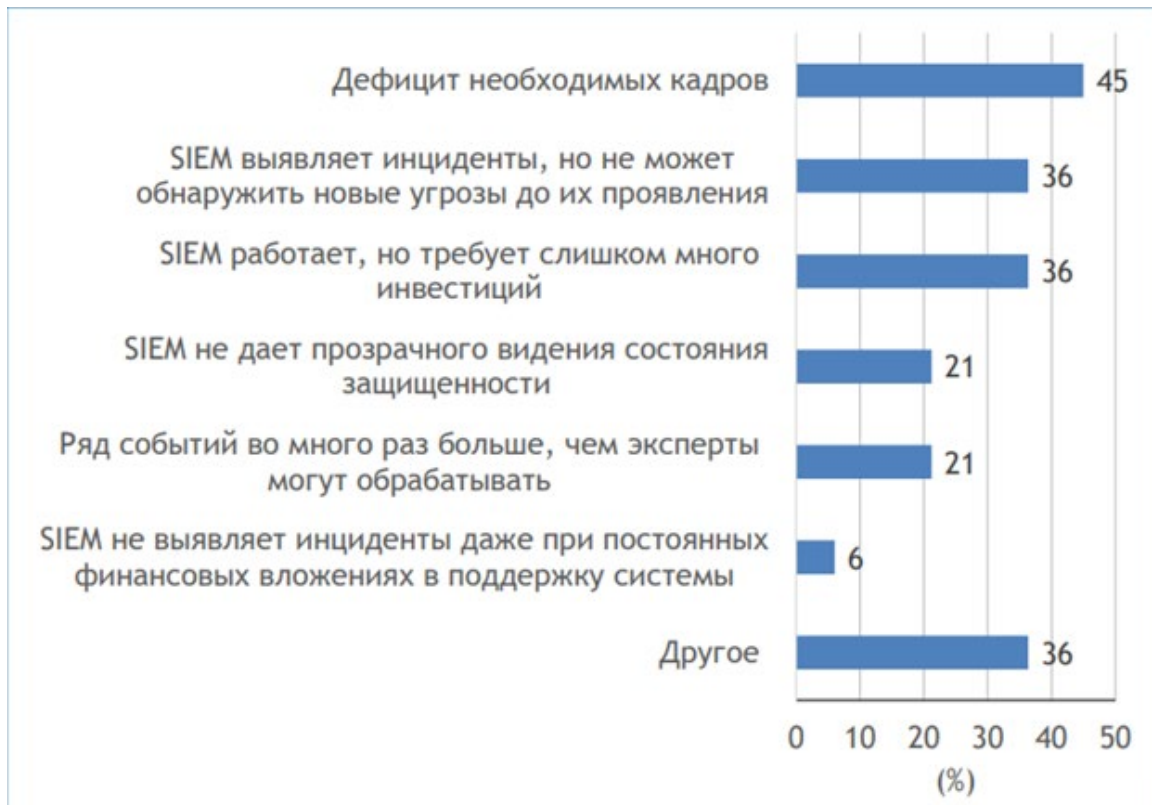


# Квалифицированные сотрудники стоят дорого



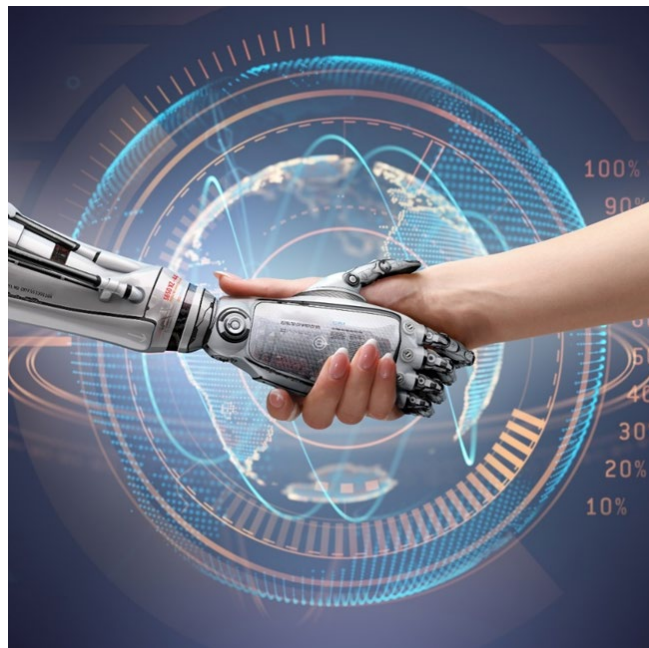


# Причины неудовлетворенности системой SIEM



# Что делать?

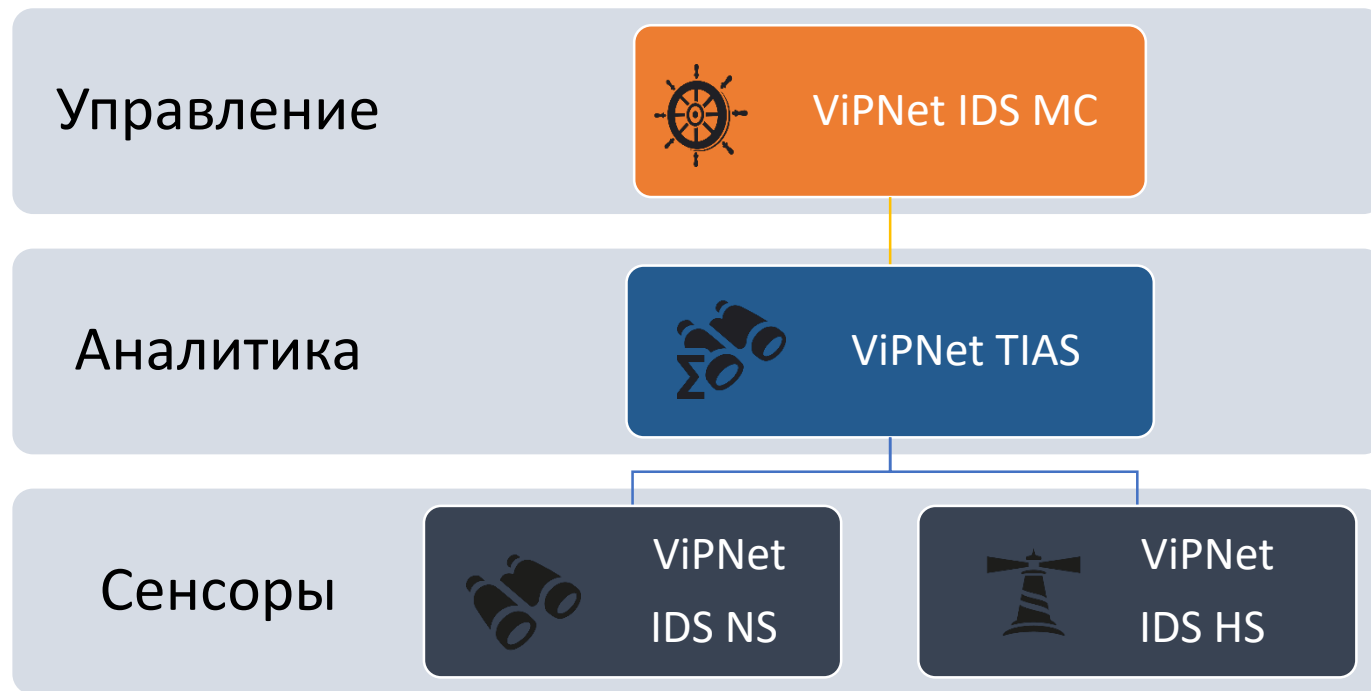
- **Снизить количество ручной работы** – высококвалифицированный персонал для проведения исследований
- **Использовать технологии машинного обучения** – инструменты и средства для автоматизации анализа событий



A high-angle photograph of a business meeting. Three people are seated around a wooden table. A woman on the left is using a tablet. A man on the right is using a smartphone. A woman in the foreground is looking at a notebook. A laptop is open in the background. A semi-transparent white box is overlaid on the bottom right of the image, containing the text 'Решение от ИнфоТеКС'.

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

ViPNet IDS NS Administrator

События Отчёты Аудит

Живой мониторинг Поиск событий Сигнатурный анализ файлов

Сенсор запущен Травфик, Мбит/сек 0.002 Загрузка ЦПУ 5%  
Использование ОЗУ 30%  
Потери пакетов 0%

Выберите фильтр

11 131 526 Всего событий за год

8 877 602 Высокая критичность

1 793 928 Средняя критичность

459 996 Низкая критичность

0 Информационное событие

Критичность	Дата, время	Код события	Кол...	Описание	Класс	Протокол	Источник, IP-адрес	Источник, ...	Получатель, IP-ад...	Получат...
Средняя	2018-10-23 14:54:4...	1000100.1000180	1	AD LOW VALUE OF DATA AND UNE...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000178	1	AD LOW VALUE OF UNKNOWN FLA...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000176	1	AD LOW VALUE OF DATA TCPIP UPL...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000174	1	AD LOW VALUE OF DATA TCPIP DO...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000172	1	AD LOW VALUE OF ACK TCPIPFLAG...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000170	1	AD LOW VALUE OF ACK TCPIPFLAG...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000168	1	AD LOW VALUE OF FIN TCPIPFLAG...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000166	1	AD LOW VALUE OF FIN TCPIPFLAG...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000164	1	AD LOW VALUE OF SYN TCPIPFLAG...	bad-unknown					
Средняя	2018-10-23 14:54:4...	1000100.1000162	1	AD LOW VALUE OF SYN TCPIPFLAG...	bad-unknown					

ViPNet IDS NS VA 3.1.0-413063 Подписка на обновления с 13.03.2018 до 14.03.2019

Русский 14:59:15 23-10-2018

# Поиск событий

ViPNet IDS NS Administrator

События Отчёты Аудит

Сенсор запущен | Трафик, Мбит/сек: 0.001 | Загрузка ЦПУ: 3% | Потери пакетов: 0% | Использование ОЗУ: 31%

Живой мониторинг Поиск событий Сигнатурный анализ файлов

События за последние 24 часа

Критичность: Любой | Событие: За последний 1 День | Получатель: Любой

Событие

Период:  с:  по:   За последний  День

Критичность:  Высокая  Средняя  Низкая  Инф. событие

Показывать:  Агрегированные события  Единичные события

Правило содержит:

Теги правила:

Класс:

Протокол:

Тип события:

Коды событий:

Применить Сбросить Сохранить как ...

Критичность	Событие	Получатель	Класс	Протокол	Источник	История	Получатель	Получатель	Направление
Средняя	CP TRAFFIC	Любой	bad-unknown						
Средняя	CMP TRAFFIC		bad-unknown						
Средняя	PACKET NUMBER		bad-unknown						
Средняя	T NUMBER		bad-unknown						
Средняя	TCP TRAFFIC		bad-unknown						
Средняя	DOWNLOAD UDP DATA SPE...		bad-unknown						
Средняя	CMP TRAFFIC		bad-unknown						
Средняя	DP TRAFFIC		bad-unknown						
Средняя	T TCPIPFLAGS UPLOAD		bad-unknown						
Средняя	CMP TRAFFIC		bad-unknown						
Средняя	HTTP TRAFFIC		bad-unknown						
Средняя	LOAD UDP DATA SPEED		bad-unknown						
Средняя	FFIC		bad-unknown						
Средняя	K TCPIPFLAGS DOWNLO...		bad-unknown						
Средняя	J TCPIPFLAGS DOWNLOAD		bad-unknown						
Средняя	J TCPIPFLAGS UPLOAD		bad-unknown						
Средняя	NS TRAFFIC		bad-unknown						
Средняя	TA TCPIP UPLOAD		bad-unknown						
Средняя	AD LOW INCOMING HTTP TRAFFIC		bad-unknown						
Средняя	AD LOW VALUE OF DOWNLOAD TCP DATA SPE...		bad-unknown						
Средняя	AD LOW VALUE OF BEST TCPIPFLAGS DOWNLO...		bad-unknown						

ViPNet IDS NS VA 3.1.0-413063 Подписка на обновления с 13.03.2018 до 14.03.2019

Русский 15:04:37 23-10-2018

# Отчеты

ViPNet IDS NS

Administrator

События Отчёты Аудит

Сенсор  
запущен

Трафик, Мбит/сек

Загрузка ЦПУ

0.001

10%

Потери пакетов

0%

Использование ОЗУ

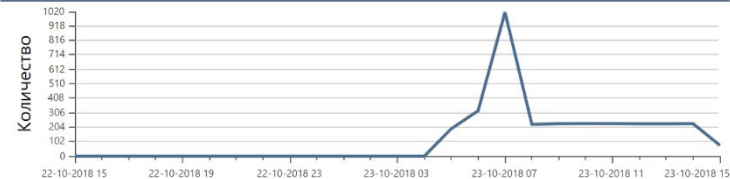
31%

Редактировать описание

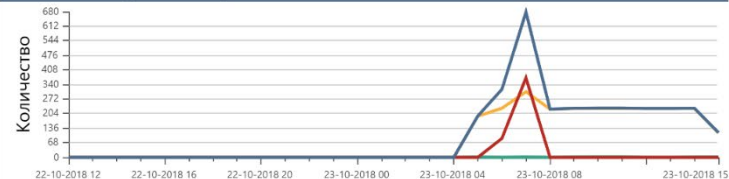
Сохранить представление

Отменить изменения

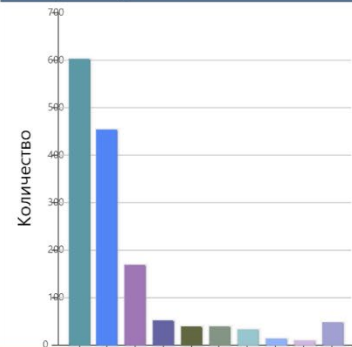
События по времени (всего событий)



События по времени (с критичностью)

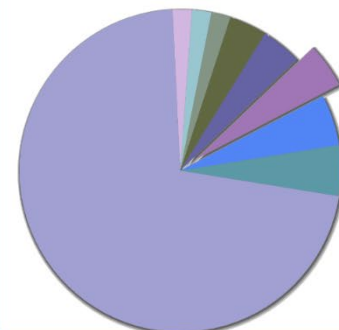


IP-адрес получателя



Назначение	Количество	%
192.168.0.2	602	41.43%
192.168.65.1	454	31.25%
10.0.9.154	169	11.63%
10.0.9.174	52	3.58%
224.0.0.252	38	2.62%
ff02::1:2	38	2.62%
104.18.40.172	32	2.20%
91.59.66.41	12	0.83%
217.69.139.110	9	0.62%
Остальные	47	3.23%
Итого:	1453	

Коды событий



Код события	Количество	%
2008538	160	4.99%
2006446	160	4.99%
3004388	140	4.37%
105.3	128	4.00%
2011042	119	3.71%
1000100.10...	61	1.90%
1000100.10...	61	1.90%
1000100.10...	61	1.90%
1000100.10...	61	1.90%
Остальные	2253	70.32%
Итого:	3204	

# Сервисные функции

ViPNet IDS NS Administrator

События Отчёты Аудит

Аудит Самотестирование Контрольные суммы файлов

Сенсор запущен

Трафик, Мбит/сек 0.002

Загрузка ЦПУ 4%

Потери пакетов 0%

Использование ОЗУ 31%

Все события

Дата, время	Тип	Ключ	Пользователь	IDS MC	Текст события	Результат
2018-10-23 15:02:37	IDS_AUDIT_LOG		admin		View audit log addr=192.168.133.1 terminal=web rport=56516	success
2018-10-23 15:01:46	IDS_SELFTEST		\$system		Software integrity check	success
2018-10-23 14:56:07	USER_LOGIN		admin		User logon addr=192.168.133.1 terminal=web rport=56303	success
2018-10-23 14:55:57	USER_AUTH		root		Attempt to access the path: /service/presets addr=192.168.133.1 terminal=web rport=56301	failed
2018-10-23 14:07:00	USER_LOGOUT		admin		'admin' has logged out by inactivity timeout terminal=web	success
2018-10-23 12:02:04	IDS_SELFTEST		\$system		Software integrity check	success
2018-10-23 09:02:04	IDS_SELFTEST		\$system		Software integrity check	success
2018-10-23 06:49:31	USER_LOGIN		admin		User logon addr=192.168.133.1 terminal=web rport=56478	success
2018-10-23 06:49:27	USER_AUTH		root		Attempt to access the path: /service/presets addr=192.168.133.1 terminal=web rport=56478	failed
2018-10-23 06:01:46	IDS_SELFTEST		\$system		Software integrity check	success
2018-10-23 05:13:52	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:58	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:58	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:57	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:57	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:57	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:57	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:56	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:56	IDS_INFO		root		eth1: The capture interface is UP and RUNNING	success
2018-10-23 05:11:56	IDS_SELFTEST		\$system		Software integrity check	success
2018-10-23 05:09:39	IDS_INFO		root		eth0: Adding IP address to an capture interface	success

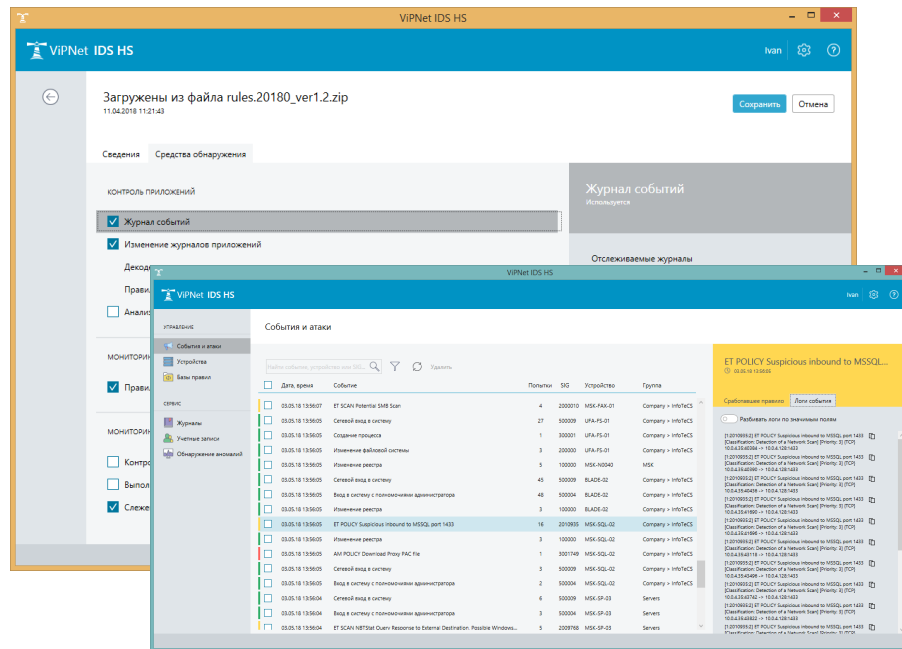
ViPNet IDS NS VA 3.1.0-413063 Подписка на обновления с 13.03.2018 до 14.03.2019

Русский 15:12:48 23-10-2018



# 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

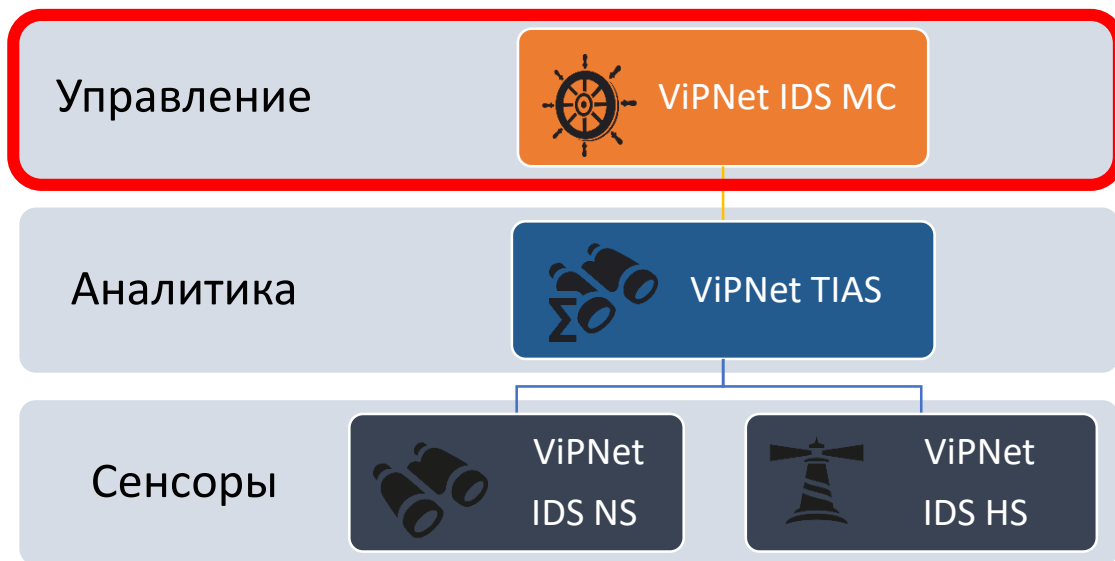
- **IDS NS** — COB уровня сети (до 4 класса)
- **IDS HS** — COB уровня узла (до 4 класса)



## ФСБ

- COA 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

The screenshot displays the 'VIPNet IDS MC' web interface. The left sidebar contains navigation options: 'Управление' (Management), 'Мониторинг' (Monitoring), 'Устройства' (Devices), 'Зарегистрированные устройства' (Registered devices), 'Запросы на подключение' (Connection requests), 'Обновления' (Updates), 'Базы правил' (Rule bases), 'Базы Malware detection', 'Программное обеспечение' (Software), 'Лицензии' (Licenses), 'Конфигурации правил обнаружения' (Detection rule configurations), 'Администрирование' (Administration), 'Задачи' (Tasks), 'События' (Events), 'Учетные записи' (Accounts), 'Резервное копирование' (Backup), 'Рассылка обновлений' (Update distribution), and 'Настройки' (Settings).

The main content area is titled 'Зарегистрированные устройства' (Registered devices) and shows the domain 'ИнфотеКС Москва'. It includes a search bar, a filter icon, and a 'Создать группу' (Create group) button. A table lists the following device groups:

Наименование	Устройства
Все устройства	Нет устройств
Группа ДППП	Нет устройств
Группа TDC	Нет устройств
Сенсоры в 1 сети главный корпус	Нет устройств

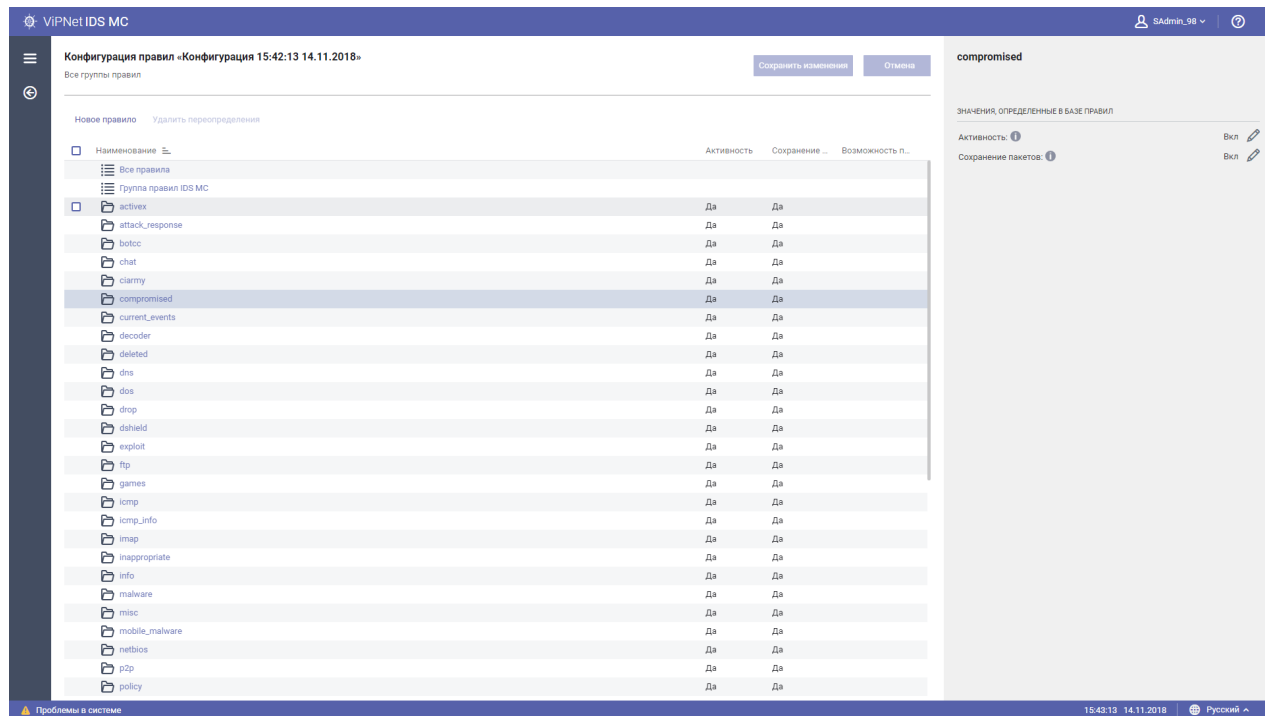
The right sidebar shows the configuration for 'ИнфотеКС Москва'. It includes a toggle for 'Выполнять обслуживание организации' (Perform organization maintenance) and the following statistics:

- Максимальное число доступных организации сенсоров IDS NS: 10
- Максимальное число доступных организации агентов IDS HS: 100
- Автоматическое подключение агентов IDS HS к серверу без подтверждения администратором (checked)

The unique identifier is FCAA835B-9D93-4EDC-9B1D-9CFB766ED2A8.

At the bottom, a status bar shows 'Проблемы в системе' (System problems), the time '15:49:59 14.11.2018', and the language 'Русский'.

# Управление конфигурациями правил



The screenshot displays the configuration page for rules in the VIPNet IDS MC system. The main title is "Конфигурация правил «Конфигурация 15:42:13 14.11.2018»". Below the title, there are buttons for "Сохранить изменения" and "Отмена". The interface is divided into two main sections: a table of rules and a details panel for the selected "compromised" rule.

**Table of Rules:**

Наименование	Активность	Сохранение	Возможность п...
Все правила			
Группа правил IDS MC			
active_x	Да	Да	
attack_response	Да	Да	
botcc	Да	Да	
chat	Да	Да	
clamy	Да	Да	
<b>compromised</b>	<b>Да</b>	<b>Да</b>	
current_events	Да	Да	
decoder	Да	Да	
deleted	Да	Да	
dns	Да	Да	
dos	Да	Да	
drop	Да	Да	
dshield	Да	Да	
exploit	Да	Да	
ftp	Да	Да	
games	Да	Да	
icmp	Да	Да	
icmp_info	Да	Да	
imap	Да	Да	
inappropriate	Да	Да	
info	Да	Да	
malware	Да	Да	
misc	Да	Да	
mobile_malware	Да	Да	
netbios	Да	Да	
p2p	Да	Да	
policy	Да	Да	

**Details Panel for "compromised":**

ЗНАЧЕНИЯ, ОПРЕДЕЛЕННЫЕ В БАЗЕ ПРАВИЛ

Активность: 1  Вкл

Сохранение пакетов: 1  Вкл







# Мониторинг состояния

- Управление
- Мониторинг
- Устройства ^
  - Зарегистрированные устройства
  - Запросы на подключение
- Обновления ^
  - Базы правил
  - Базы Malware detection
  - Программное обеспечение
  - Лицензии
- Конфигурации правил обнаружения
- Администрирование
  - Задачи
  - События
  - Учетные записи
  - Резервное копирование
  - Рассылка обновлений
  - Настройки

## Мониторинг

### VIPNet IDS MC

Опасное состояние

 Резервное копирование не выполнялось	15
<a href="#">Исправить</a>	дней
 Неразсланные обновления баз правил	1
<a href="#">Исправить</a>	запрос
 Неразсланные обновления база Malware detection	1
<a href="#">Исправить</a>	запрос
 Система в работоспособном состоянии	

# Обновления правил

VIPNet IDS MC SAAdmin\_98

Управление

- Мониторинг
- Устройства
- Обновления
  - Базы правил
  - Базы Malware detection
  - Программное обеспечение
  - Лицензии
- Конфигурации правил обнаружения

Администрирование

- Задачи
- События
- Учетные записи
- Резервное копирование
- Расылка обновлений
- Настройки

Проблемы в системе

### Автоматическая рассылка обновлений по доменам

Домен

Домен	Лицензии	Базы правил	Базы Malware detection	Обновления ПО
Все устройства	Отключена	Отключена	Отключена	Отключена
ИнфоТекС SPB	Отключена	Все	Все	Отключена
ИнфотекС Москва	Отключена	Все	Все	Отключена

### Все устройства

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ЛИЦЕНЗИЙ

- Загруженные вручную

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ БАЗ ПРАВИЛ

- Загруженные вручную
- Загруженные с сервера

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ БАЗ MALWARE DETECTION

- Загруженные вручную
- Загруженные с сервера

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ПО

- Загруженные вручную
- Загруженные с сервера

16:52:16 14.11.2018 Русский

# Сервер обновлений ViPNet IDS

Сервер обновлений ViPNet IDS IDS Test user ▾

Обновления баз правил 🔗

Поиск обновлений   Найдено обновлений: 10

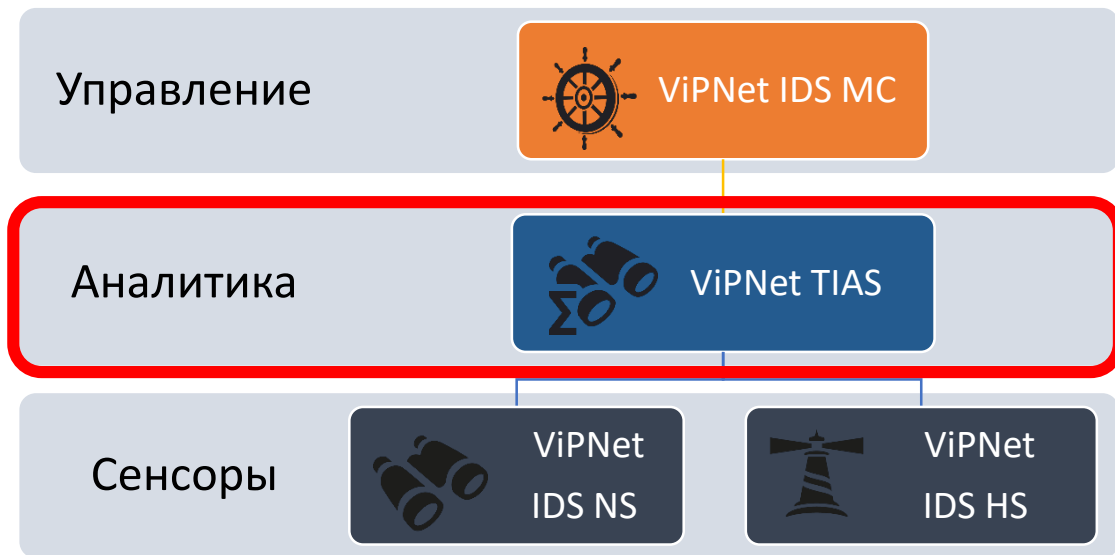
Дата создан...	Имя файла	Размер файла	Версия ПО
2018-11-13	rules.2018-11-13-15-04-42_v...	18.7 Mб	3.4
2018-11-13	rules.2018-11-13-15-04-30_v...	18.7 Mб	3.3
2018-11-13	rules.2018-11-13-15-04-18_v...	18.7 Mб	3.2
2018-11-13	rules.2018-11-13-15-04-06_v...	18.8 Mб	3.1
2018-11-13	rules.2018-11-13-15-03-54_v...	18.8 Mб	3.0
2018-11-13	rules.2018-11-13-15-03-30_v...	18.5 Mб	2.4
2017-09-29	rules.2017-09-29-18-29-41_ver...	2.2 Mб	2.0
2017-08-02	rules.2017-08-02-10-17-20_ver...	2.2 Mб	2.2
2016-07-21	rules.2016-07-21-14-34-49_ver...	2.1 Mб	2.1
2016-07-21	rules.2016-07-21-11-24-47_ver...	1.4 Mб	2.3

База правил от 13.11.2018 ↓

Дата создания: 2018-11-13  
Версия обновления: 387  
Имя файла: rules.2018-11-13-15-04-42\_ver.3.4.tgz  
Системные требования:  
Версия ПО: 3.4

1.0.0.95 Русский 15:38:41 14.11.2018

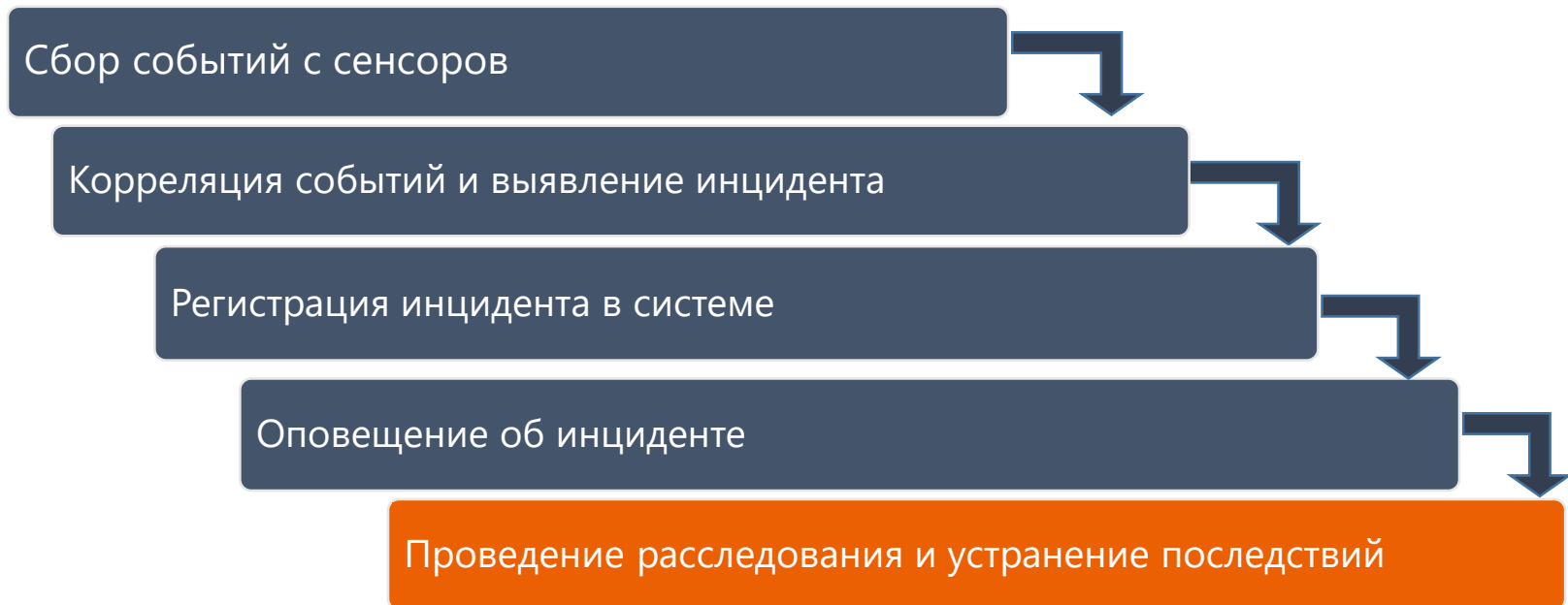
# Система анализа



# 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?



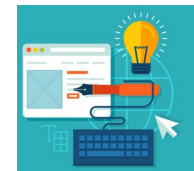
События ИБ



Threat Intelligence



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



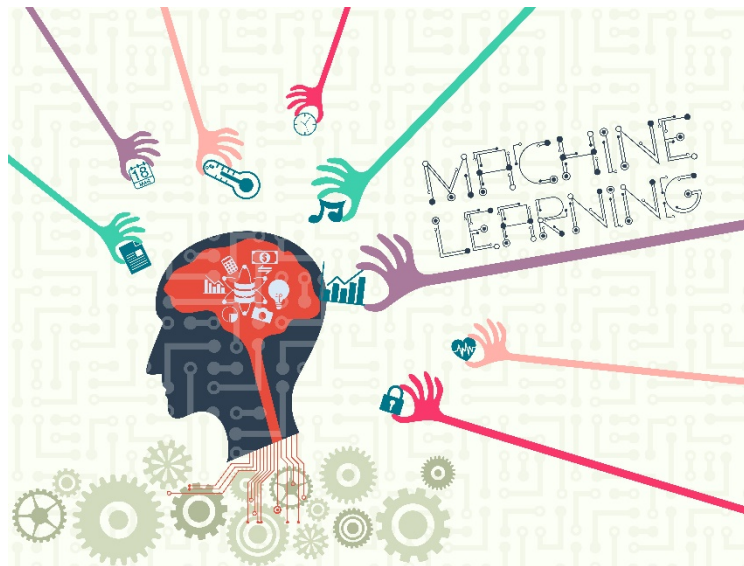
## Знания об угрозах:

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

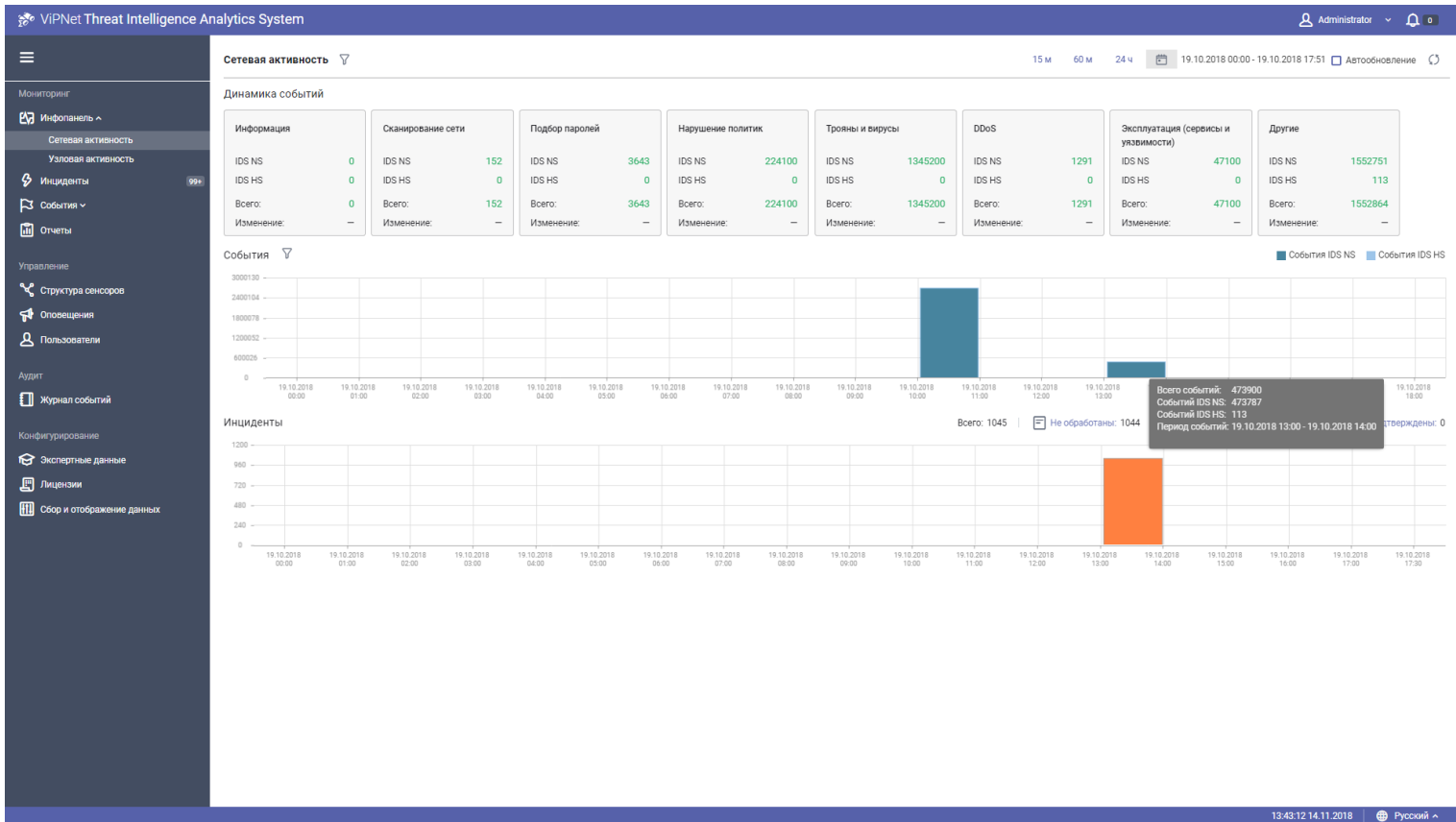


# Комбинирование двух методов

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



# Сетевая активность



# Узловая активность

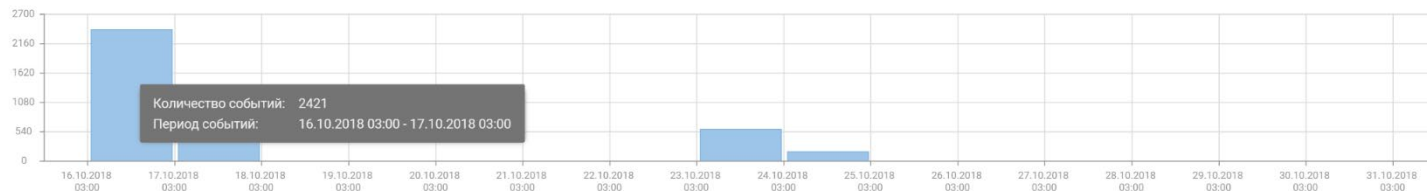
## Узловая активность

15 м 60 м 24 ч 16.10.2018 06:49 - 31.10.2018 06:49 Автообновление

### Динамика событий

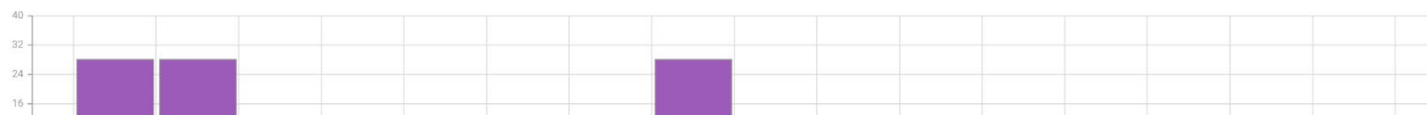
<b>Другие</b> Всего: 3343 Изменение: —	<b>Закрепление</b> Всего: 4 Изменение: —	<b>Деактивация защиты</b> Всего: 0 Изменение: —	<b>Повышение привилегий</b> Всего: 31 Изменение: —	<b>Вредоносный артефакт</b> Всего: 20 Изменение: —	<b>Хакерские инструменты</b> Всего: 24 Изменение: —
<b>Изменение системных настроек</b> Всего: 0 Изменение: —	<b>Получение данных</b> Всего: 0 Изменение: —	<b>Подозрительная активность</b> Всего: 205 Изменение: —			

### События



### Инциденты

Всего: 84 | Не обработаны: 83 | В работе: 0 | Подтверждены: 1 | Не подтверждены: 0



# Инциденты

VIPNet Threat Intelligence Analytics System User [v] [bell icon]

**Инциденты** 15 м 60 м 24 ч 19.10.2018 00:00 - 20.10.2018 17:51 Автообновление

Статус	Тип ин...	Польз...	Дата и время	Рейтинг	IP-адрес сенсора	Пораженные узлы	Наименование	Метод	Идент...
Не обрабо...	Сетевой		19.10.2018 13:05:27	10	11.1.1.1	192.168.218.77	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:27	9	11.1.1.1	192.168.71.115	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:27	9	11.1.1.1	192.168.189.127	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:27	9	11.1.1.1	192.168.71.70	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:27	10	11.1.1.1	192.168.92.8	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:27	10	11.1.1.1	192.168.151.177	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.68.200, 192.168...	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.237.31	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.195.58, 192.168...	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	8	11.1.1.1	192.168.144.56, 192.168...	Классификатором выявлено предполо...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.143.159	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.249.75	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.103.234	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.161.93, 192.168...	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	8	11.1.1.1	192.168.11.92	Классификатором выявлено предполо...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	9	11.1.1.1	192.168.72.133	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	9	11.1.1.1	192.168.212.24, 192.168...	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.230.184	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.27.239	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	9	11.1.1.1	192.168.65.5	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	8	11.1.1.1	192.168.127.190	Классификатором выявлено предполо...	Зерistisch...	5bc9ac67e...
Не обрабо...	Сетевой		19.10.2018 13:05:26	10	11.1.1.1	192.168.113.123	Классификатором выявлено подозрит...	Зерistisch...	5bc9ac67e...

Связанные события

Дата и время	Правило	IP-адрес источни...	IP-адрес получат...	Пакет
19.10.2018 10:03:00	ET TROJAN ABUSE CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)	192.168.68.200:49163	200.168.14.35:25566	↓
19.10.2018 13:02:52	ET POLICY RDP connection confirm	192.168.68.200:3389	192.168.100.54:58255	↓

**Классификатором выявлено подозрительное событие**  
Высокий уровень важности

Статус инцидента: Не обработан [Взять в работу](#)

Тип инцидента: Сетевой

Рейтинг: 10

Дата и время: 19.10.2018 13:05:26

Пораженные узлы (2):  
ip: 192.168.100.54  
mac: 10:1f:af:35:69:83

Тип угрозы:

Наименование: Классификатором выявлено подозрительное событие

Метод: Зеристический

Идентификатор: 5bc9ac67e13823060dec3f6a

Симптомы: Аномальная сетевая активность APM

**Рекомендации**

- Отключить пораженный компьютер от сети
- Провести интервьюирование владельца
- Осуществить антивирусную проверку
- Передать обнаруженное вредоносное ПО в ЦМ для анализа
- Удалить обнаруженное вредоносное ПО
- Провести анализ сетевой активности узла

# Сетевые события



Мониторинг

Инфопанель ^

Сетевая активность

Узловая активность

Инциденты 99+

События ^

Сетевые

Узловые

Отчеты

Управление

Структура сенсоров

Оповещения

Пользователи

Аудит

Журнал событий

Конфигурирование

Экспертные данные

Лицензии

Сбор и отображение данных

## Сетевые события

15 м 60 м 24 ч 16.10.2018 06:49 - 31.10.2018 06:49  Автообновление

События IDS NS События IDS HS

### Источники

Урове...	Прави...	Ко...	IP-адр...	IP-адр...	Прото...	Номер...
Высокий	ET SCAN S...	117128	91.59.6...	192.168.13...	TCP	1:2008538
Критичн...	ET WEB_S...	116060	91.59.6...	192.168.13...	TCP	1:2006446
Критичн...	AM SQL_S...	101560	91.59.6...	192.168.13...	TCP	1:3004388
Критичн...	ET WEB_ AM SQL_ SQL_Injection_SELECT-UNION_GET			13...	TCP	1:2011042
Средний	ET INFO In...	33813	222.222...	192.168.13...	TCP	1:2017980
Высокий	ET CURRE...	30055	222.222...	192.168.13...	TCP	1:2014545
Высокий	ET SCAN N...	19617	222.33...	192.168.13...	UDP	1:2018489
Критичн	ET P2P_So	18088	222.222	192.168.13	TCP	1:2001188

### Получатели

Урове...	Прави...	Ко...	IP-адр...	IP-адр...	Прото...	Номер...
Высокий	ET SCAN S...	117128	192.168...	192.168.13...	TCP	1:2008538
Критичн...	ET WEB_S...	116060	192.168...	192.168.13...	TCP	1:2006446
Критичн...	AM SQL_S...	101560	192.168...	192.168.13...	TCP	1:3004388
Критичн...	ET WEB_S...	86335	192.168...	192.168.13...	TCP	1:2011042
Средний	ET INFO In...	33813	192.168...	192.168.13...	TCP	1:2017980
Высокий	ET CURRE...	30055	192.168...	192.168.13...	TCP	1:2014545
Высокий	ET SCAN N...	19617	192.168...	192.168.13...	UDP	1:2018489
Критичн	ET P2P_So	18088	192.168	192.168.13	TCP	1:2001188

### События на узлах 1:2006446 91.59.66.41

Дата и ...	Номер...	IP-адр...	Тип се...	IP-адр...	Порт п...	IP-адр...	Порт и...	Пакет	Урове...	Прото...	Колич...	Правило
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	0	↓	Критичн...	TCP	100	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56797	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56796	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56795	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56794	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56793	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56792	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56791	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...
23.10.2018 07:4...	1:2006446	192.168.13...	IDS NS	192.168...	80	91.59.6...	56790	↓	Критичн...	TCP	1	ET WEB_SERVER Pos...

> Дополнительные события

# Поиск и фильтрация

The screenshot displays the ViPNet Threat Intelligence Analytics System interface. The main window shows a table of network events under the heading "Сетевые события". A search dialog box is open, allowing the user to search for events using a regular expression. The dialog box contains the following text:

Поиск с регулярным выражением

Использовать регулярное выражение

Подсказки regex:

- Содержит abc или def `.*(abc|def).*`
- Содержит abc и def `(?=.*(abc))(?=.*(def)).*`
- Не содержит abc `^(?!abc).*`

Buttons: Найти, Сбросить

The background table shows columns for "Источники" (Sources) and "Получатели" (Destinations). The "Источники" table has columns: Уровне..., Прави..., Ко..., IP-адр..., IP-адр..., Прото..., Номер... The "Получатели" table has columns: Уровне..., Прави..., Ко..., IP-адр..., IP-адр..., Прото..., Номер... Below these are two more tables: "События на узле" and "Дополнительные события".

# Узловые события



Мониторинг

Инфопанель

Сетевая активность

Узловая активность

Инциденты 99+

События

Сетевые

Узловые

Отчеты

Управление

Структура сенсоров

Оповещения

Пользователи

Аудит

Журнал событий

Конфигурирование

Экспертные данные

Лицензии

Сбор и отображение данных

## Узловые события

15 м 60 м 24 ч 16.10.2018 06:49 - 31.10.2018 06:49 Автообновление

Уровень важности: Критичный

Имя узла	IP-адрес узла	Правило	Количество	Из них анома...	Категория угроз	ID узла
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение фай...	8	0	Подозрительная активность	85dbab84-d16f-47...
		Подозрение на обход Application Whit...	0	0	Хакерские инструменты	85dbab84-d16f-47...
		Подозрение на обход Application Whitelisting (P-Shell)	0	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка повышения привилегий	8	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка добавления skeleton key в...	8	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка добавления вредоносног...	8	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка создания поддельных (sil...	8	0	Хакерские инструменты	85dbab84-d16f-47...
		Загрузка хакерского скрипта: invoke-mimikatz	8	0	Хакерские инструменты	85dbab84-d16f-47...
		Запуск хакерского скрипта: invoke-mimikatz	8	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка извлечения ключей шифр...	8	0	Хакерские инструменты	85dbab84-d16f-47...
		Подозрение на запуск хакерской утилиты: mimikatz	8	0	Хакерские инструменты	85dbab84-d16f-47...
		mimikatz activity: попытка проведения pass-the-ticke...	8	0	Хакерские инструменты	85dbab84-d16f-47...
		Запуск хакерской утилиты: AllTheThings	8	0	Хакерские инструменты	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск msiehex...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: подозрение на...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Запуск powershell средствами rundll32	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск cmd/po...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск vbs/jscr...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск rundll32...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск regsvr3...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Возможный вредоносный артефакт: запуск installu...	8	0	Вредоносный артефакт	85dbab84-d16f-47...
		Подозрение на обход Application Whitelisting (AllThe...	8	0	Повышение привилегий	85dbab84-d16f-47...

# Узловые события детализация

VIPNet Threat Intelligence Analytics System Administrator 0

Узловые события 15 м 60 м 24 ч 16.10.2018 06:49 - 31.10.2018 06:49 Автообновление

Узел: WIN\_7 IP адрес: 192.168.133.131 Правило: Powershell активность (загрузка и исполнение файла) Уровень важности: Критичный Все события Аномалии

Категории источников угроз на узле

Контроль процессов

Имя агента	IP-адрес хостового с...	Имя правила	Колич...	Время обнаружения события
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	1	23.10.2018 06:5
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	1	17.10.2018 12:0
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	1	17.10.2018 12:0
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	1	16.10.2018 18:4
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	1	16.10.2018 18:2
WIN_7	192.168.133.131	Powershell активность (загрузка и исполнение файла)	3	16.10.2018 18:2

- Выбрать все
- Идентификатор события
- Идентификатор сенсора
- Имя агента
- IP-адрес хостового сенсора
- Идентификатор правила
- Имя правила
- Критичность события
- Количество событий
- Время обнаружения события
- Признак аномалии
- Категория угроз
- Параметры командной строки
- Имя родительского процесса
- Активная учетная запись пользователя
- Домен активной учетной записи пользователя
- sid активной учетной записи пользователя



VIPNet Threat Intelligence Analytics System User 10

Мониторинг

- Инфопанель ^
  - Сетевая активность
  - Узловая активность
- Инциденты 99%
- События ^
  - Сетевые
  - Узловые
- Отчеты

### Отчеты

⊕ Новый отчет

<input type="checkbox"/>	Название	Шаблон отчета	Организации	Дата и время	Период отчета	Статус	Размер	
<input type="checkbox"/>	Отчет для руководства по инцидентам за ...	Подтвержденные инциденты	Все	14.11.2018 14:26	3 квартал 2018	подготовл...	11.2 Кб	↓
<input type="checkbox"/>	Отчет за год по инцидентам	Инциденты по типам угроз	Все	14.11.2018 14:25	2018 год	подготовл...	31 Кб	↓
<input type="checkbox"/>	Самые атакуемые узлы	Цели атак (100 самых атакуемых узлов)	Инфотекс	14.11.2018 14:25	Ноябрь 2018	подготовл...	11.1 Кб	↓
<input type="checkbox"/>	События по типам угроз	Категории источников узловых угроз инф...	Все	14.11.2018 14:24	Ноябрь 2018	подготовл...	11.4 Кб	↓
<input type="checkbox"/>	Карточки инцидентов октябрь	Инциденты информационной безопаснос...	Все	14.11.2018 14:24	Октябрь 2018	подготовл...	2.3 Mb	↓
<input type="checkbox"/>	События за месяц	События информационной безопасности	Все	14.11.2018 14:23	13.11.2018 00:00...	подготовл...	10.9 Кб	↓
<input type="checkbox"/>	Отчет за III квартал - Все подтвержденные...	Инциденты информационной безопаснос...	Инфотекс	14.11.2018 14:23	3 квартал 2018	подготовл...	12.1 Кб	↓

### Новый отчет

\* Название:

Не более 100 символов.

\* Шаблон отчета:  
Инциденты информационной безопасности со связанными событ

Период формирования отчета:

- Год
- Квартал
- Месяц
- Произвольный период (максимум 45 дней)

PDF **Скачать отчет**

- DOCX
- PPTX
- XLSX
- ODT
- CSV
- XML

14:40:44 14.11.2018 Русский

VIPNet Threat Intelligence Analytics System Administrator 11

Мониторинг

- Инфопанель ^
- Сетевая активность
- Узловая активность
- Инциденты 67
- События ^
- Сетевые
- Узловые
- Отчеты

Управление

- Структура сенсоров
- Оповещения**
- Пользователи

Аудит

- Журнал событий

Конфигурирование

- Экспертные данные
- Лицензии
- Сбор и отображение данных

## Оповещения

По электронной почте По протоколу syslog

Оповещения выключены.

### Настройка соединения для отправки оповещений

Адрес сервера:  Порт:   Соединение TLS

Пользователь:  Пароль:

Адрес, с которого будут отправляться оповещения:

Отправьте тестовое письмо, чтобы проверить правильность настроек.

### Адресаты оповещений

Добавьте адресатов и задайте параметры оповещений по инцидентам.

<input type="text" value="retov@ccm.com"/>	<input type="text" value="ИнфоТеКС Берлин"/>	<input type="text" value="Не обработан"/>	<input type="text" value="Средний, f"/>	<input type="text" value="English"/>	<input type="button" value="🗑"/>
<input type="text" value="ivanov@dit.ru"/>	<input type="text" value="ИнфоТеКС Москва"/>	<input type="text" value="Подтвержден"/>	<input type="text" value="Высокий"/>	<input type="text" value="Русский"/>	<input type="button" value="🗑"/>
<input type="text" value="sidorov@ca.ru"/>	<input type="text" value="6 организаций"/>	<input type="text" value="В работе"/>	<input type="text" value="Высокий"/>	<input type="text" value="Русский"/>	<input type="button" value="🗑"/>

14:08:57 14.11.2018

# Многоуровневая структура

VIPNet Threat Intelligence Analytics System Administrator 11

**Структура сенсоров**

Новый сенсор Загрузить Выгрузить Развернуть все Свернуть все

Название сенсора	Тип	IP-адрес	Идентификатор	Подсеть
<input type="checkbox"/> ИнфоТеКС NY				
<input type="checkbox"/> ИнфоТеКС Берлин				
<input checked="" type="checkbox"/> ИнфоТеКС Москва				
<input type="checkbox"/> Департамент продаж				
<input type="checkbox"/> Департамент разработки				
<input checked="" type="checkbox"/> Сеть TDC 2 этаж				
<input type="checkbox"/> Хостовый сервер	IDS HS Server		13543456546546	
<input type="checkbox"/> Внешний трафик из 1...	IDS NS	192.1...	123123414523453245	192.168.1.1/1
<input type="checkbox"/> ИнфоТеКС СПб				
<input type="checkbox"/> ИнфоТеКС Томск				
<input checked="" type="checkbox"/> Новая				
<input type="checkbox"/> Филиал				

**Новый сенсор**

\* Название сенсора:  
  
Не более 255 символов.

\* Тип сенсора:  
IDS NS

IP-адрес:

\* Идентификатор:  
  
Не более 63 символов.

Учетное имя:

Пароль:

\* Подсети:

Добавить подсеть

14:47:02 14.11.2018 Русский

# Журнал событий

- Мониторинг
- Информанель
- Сетевая активность
- Условная активность
- Инциденты
- События
- Отчеты
- Управление
- Структура сенсоров
- Оповещения
- Пользователи
- Аудит
- Журнал событий

## Журнал событий

[Скачать файл](#)

Дата и время	Категория	Наименование	Инициатор	IP инициатора	Статус	Дополнительная информация
14.11.2018 13:45:14	Аудит	Чтение журнала	Administrator	11.0.10.254	Информация	Пользователь "Administrator" читает ...
14.11.2018 13:45:10	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:44:41	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
14.11.2018 13:44:21	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:44:00	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:43:17	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:42:47	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:36:01	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
14.11.2018 13:35:48	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:35:39	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:35:05	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:32:54	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:32:23	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
14.11.2018 13:32:21	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:32:14	Авторизация/Аутентификация	Вход пользователя в систему	c	11.0.14.146	Ошибка	Ошибка аутентификации пользоват...
14.11.2018 13:30:49	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.10.254	Информация	Успешный вход пользователя "Admi...
14.11.2018 13:08:23	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
14.11.2018 12:06:58	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
14.11.2018 11:24:41	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
13.11.2018 23:24:38	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
13.11.2018 16:40:05	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
13.11.2018 15:59:21	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
13.11.2018 11:32:35	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
13.11.2018 11:24:37	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
12.11.2018 23:24:35	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
12.11.2018 16:15:22	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
12.11.2018 11:24:32	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
11.11.2018 23:24:29	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
11.11.2018 11:24:27	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
10.11.2018 23:24:25	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
10.11.2018 11:24:23	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
10.11.2018 10:59:27	Авторизация/Аутентификация	Вход пользователя в систему	Administrator	11.0.14.146	Информация	Успешный вход пользователя "Admi...
09.11.2018 23:24:21	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...
09.11.2018 15:00:04	Аудит	Чтение журнала	Administrator	11.0.14.146	Информация	Пользователь "Administrator" читает ...
09.11.2018 11:24:19	Оповещение	Проверка целостности ПО	System	127.0.0.1	Информация	Система успешно проверила целост...

# Варианты исполнения ViPNet TIAS

Desktop



Server 1U



Virtual Appliance



ПАК ViPNet TIAS 100

ПАК ViPNet TIAS 1000

ПАК ViPNet TIAS 2000

ПАК ViPNet TIAS 5000

ViPNet TIAS VA

# Сертификация

## ФСТЭК

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



## ФСБ

- COA класс B (в составе IDS 3)

# Меры по обеспечению безопасности для значимого объекта КИИ

## VII. Предотвращение вторжений (компьютерных атак) (COB)

COB.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
COB.1	Обнаружение и предотвращение компьютерных атак	Все требования ФСТЭК к COB и ФСБ к COA сетевого уровня и уровня узла закрываются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК и ФСБ
COB.2	Обновление базы решающих правил	Автоматическое централизованное обновление БПП 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!

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, there are several high-voltage power line towers with multiple cross-arms. The sun is low on the horizon, creating a strong glow and casting long shadows. The overall scene represents renewable energy and power infrastructure.

# Вопросы