

# Обнаружение и предотвращение компьютерных атак. Как сделать жизнь безопасносника чуть-чуть легче

Светлана Старовойт



техноФест  
infotechs

ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Что такое Центр мониторинга и Центр ГосСОПКА

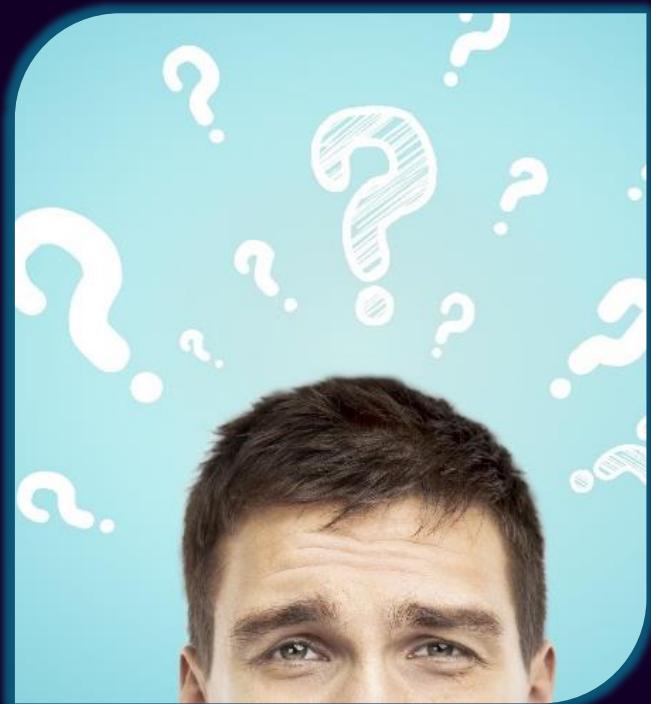
# Мониторинг информационной безопасности

Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей

В ходе мониторинга информационной безопасности осуществляются:

- Анализ событий безопасности и иных данных мониторинга
- Контроль (анализ) защищенности информации
- Анализ и оценка функционирования систем защиты информации информационных (автоматизированных) систем
- Периодический анализ изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе эксплуатации

ГОСТ Защита информации МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# Мониторинг информационной безопасности средств и систем информатизации

Наименование оборудования		Технические и (или) функциональные характеристики
22	Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная <b>инвентаризация ресурсов</b> информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей (кода, конфигурации и архитектуры) в них, анализ и управление выявленными уязвимостями с учетом угроз. Должны иметь сертификаты соответствия ФСТЭК России
24.	Средства управления информацией об угрозах безопасности информации	Автоматизированный <b>сбор и анализ</b> информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
25.	Средства управления событиями безопасности информации	Автоматизированный <b>сбор, анализ и корреляция</b> данных о <b>событиях безопасности</b> информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация. Должны иметь сертификаты соответствия ФСТЭК России

# Мониторинг информационной безопасности средств и систем информатизации

Наименование оборудования	Технические и (или) функциональные характеристики
26. Средства управления инцидентами информационной безопасности	<p>Автоматизированная <b>регистрация информации об инцидентах</b> информационной безопасности информационных систем, <b>предоставление рекомендаций по реагированию</b> на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них.</p> <p>Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)</p>
27. Средства защиты каналов передачи данных	<p>Должны обеспечивать конфиденциальность и целостность данных, передаваемых по каналам связи между информационной системой, используемой для управления информационной безопасностью, и информационными системами, в отношении которых осуществляется мониторинг.</p> <p>Должны иметь сертификаты соответствия ФСБ России</p>
28. Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	Системы защиты информации информационных систем, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, применительно к первому классу защищенности государственных информационных систем

# ГосСОПКА



- ГосСОПКА – это государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, нарушение или прекращение работы которых может крайне негативно повлиять на экономику страны или безопасность граждан.
- Центр ГосСОПКА – совокупность сил и средств субъекта ГосСОПКА, предназначенная для решения задач ГосСОПКА в своей зоне ответственности.

# Перечень мероприятий

**Класс В**

технο  **Фест**

- Взаимодействие с НКЦКИ
- Разработка регламентирующих документов
- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах
- Регистрация атак и инцидентов
- Анализ событий ИБ
- Инвентаризация
- Анализ угроз ИБ
- Составление и актуализация перечня угроз
- Выявление уязвимостей
- Подготовка предложений по повышению уровня защищенности
- Составление перечня инцидентов
- Ликвидация последствий
- Анализ результатов ликвидации последствий

# Требования к средствам ГосСОПКА

К средствам ГосСОПКА относятся:

- Технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак (далее – **средства обнаружения**)
- Технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак (далее – **средства предупреждения**)
- Технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак (далее – **средства ликвидации последствий**)
- Технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (далее – **средства ППКА**)
- Технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее – **средства обмена**)
- Криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак

Приказ № 196 от 6 мая 2019 года

# Варианты подключения

Самостоятельное подключение



Субъект ГосЗОПКА



- Заключить соглашение с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосЗОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ

с 13 ДЕКАБРЯ 2025: Пройти аккредитацию

Подключение через корпоративный центр



Корпоративный центр ГосЗОПКА

- Заключить соглашение с корпоративным (ведомственным) центром ГосЗОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности цента



Субъект КИИ

# Передача информации в ГосСОПКА

Центр ГосСОПКА



Субъекты КИИ и ФСТЭК

24 часа - инцидент



Сайт Роскомнадзор



Операторы ПД

24 часа - инцидент

3 суток - уведомление о результатах

# Общие требования к средствам ГосСОПКА



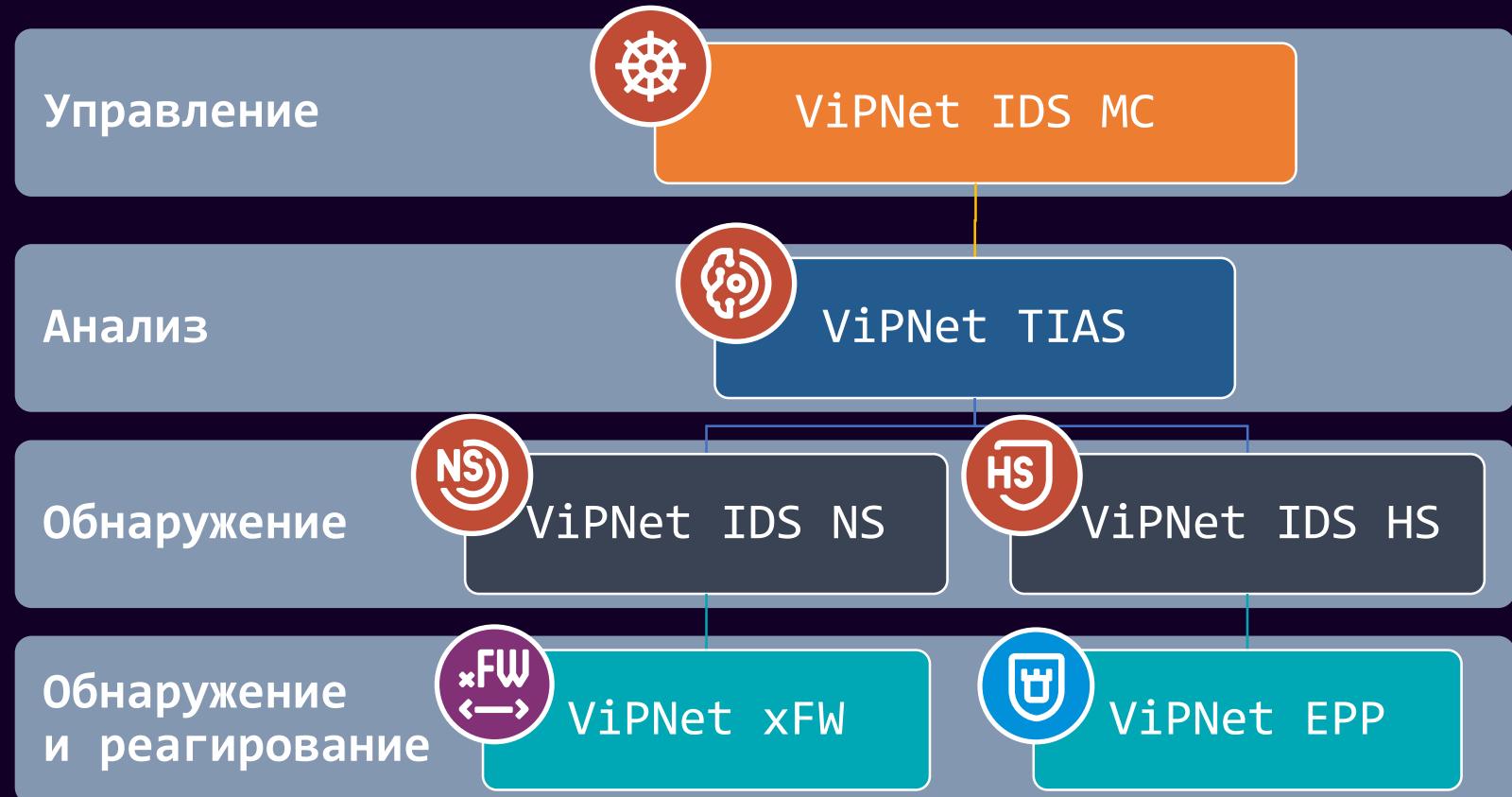
**Средства ГосСОПКА должны соответствовать следующим требованиям:**

- Должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта КИИ или привлекаемыми работниками
- Должна быть исключена возможность несанкционированной передачи обрабатываемой информации
- Должны иметь **возможность модернизации российскими организациями**, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц
- Должны быть **обеспечены гарантой и технической поддержкой российскими организациями**, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц
- Работа средств ГосСОПКА **не должна приводить к нарушениям функционирования информационных систем**
- В средствах ГосСОПКА **должны быть реализованы функции безопасности** в соответствии с главой VIII настоящих Требований

Приказ № 196  
от 6 мая 2019 года

# Решение ViPNet TDR

# Решение ViPNet TDR

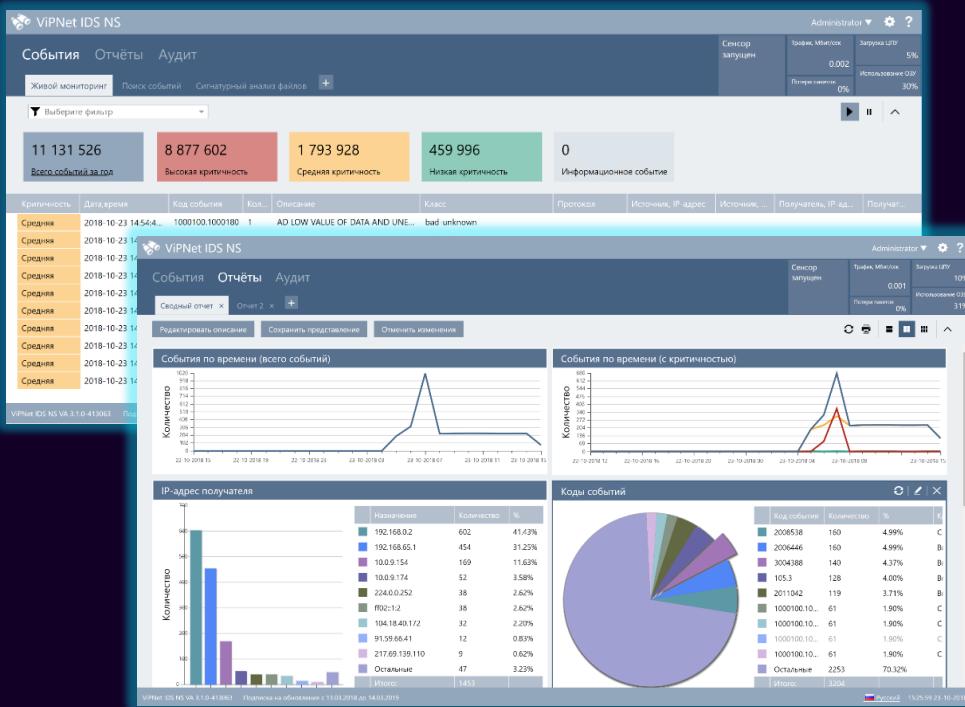


# ViPNet IDS NS



технο  
Фест  
infoteсs

- Обнаруживать события ИБ в трафике
- Оповещать о событиях
- Хранить события
- Работать с событиями
- Управлять правилами и настройкой сигнатур



# ViPNet IDS HS



технο infoteсs фест

- Выявлять подозрительную активность внутри ОС:
  - файловая активность
  - изменения в реестре
  - неизвестные процессы
- Определять атаки, которые «не видит» сетевой сенсор
- Обнаруживать атаки после расшифровки входящего трафика

The screenshot displays the ViPNet IDS HS software interface. The main window shows a list of events under 'События и атаки' (Events and Attacks). One specific event is highlighted: 'ET POLICY Suspicious inbound to MSSQL port 1433'. The event details show it originated from '192.168.1.10' and was detected by 'Company > Infoteсs'. The event ID is 207983, and the timestamp is '2018-04-11 11:21:43'. The event type is 'Изменение журналов приложений' (Change in application logs). Other events listed include various system and application log changes.



- Настраивать структуру и параметры сенсоров
- Управлять конфигурациями правил
- Мониторить работоспособность сенсоров
- Обновлять:
  - базы решающих правил
  - базы сигнатур вредоносного ПО
  - экспертические данные

The screenshot displays the ViPNet IDS MC software interface across three main windows:

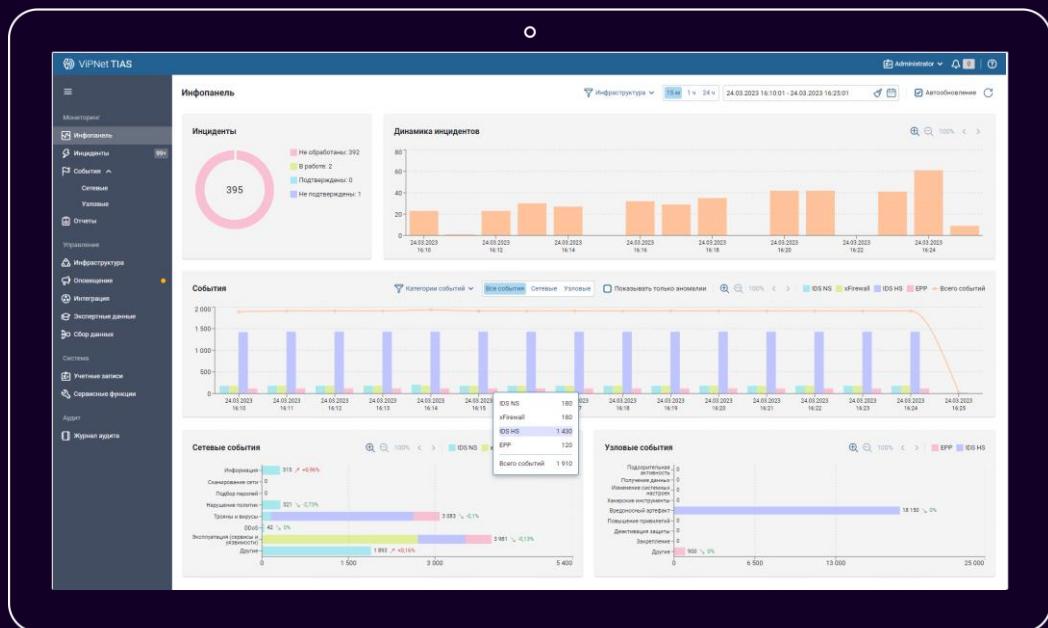
- Monitoring (Мониторинг) window:** Shows real-time statistics for various sensor types. For example, there are 14 network sensors, 23 physical sensors, 2 network-based detection sensors, 12 physical-based detection sensors, and 2 physical-based detection sensors.
- Device Management (Устройства) window:** Lists registered devices. One device, "192.168.0.76", is highlighted. It is a UTM device with IP address 192.168.0.76, MAC address 00:0C:29:00:00:00, and model UTM. Its status is "Проверка связи с устройством".
- Logs (Логи) window:** Displays log entries for a specific device. An entry for "192.168.0.71" shows a connection attempt from "192.168.0.71" at 10:07:2016, with a status message indicating it was blocked by a heuristic rule.

# ViPNet TIAS



технο infoteсs  
Фест

- Анализировать события от сенсоров ViPNet IDS
- Выявлять инциденты
- Оповещать об инцидентах
- Проводить расследования
- Давать рекомендации
- Формировать отчеты



# ViPNet xFirewall

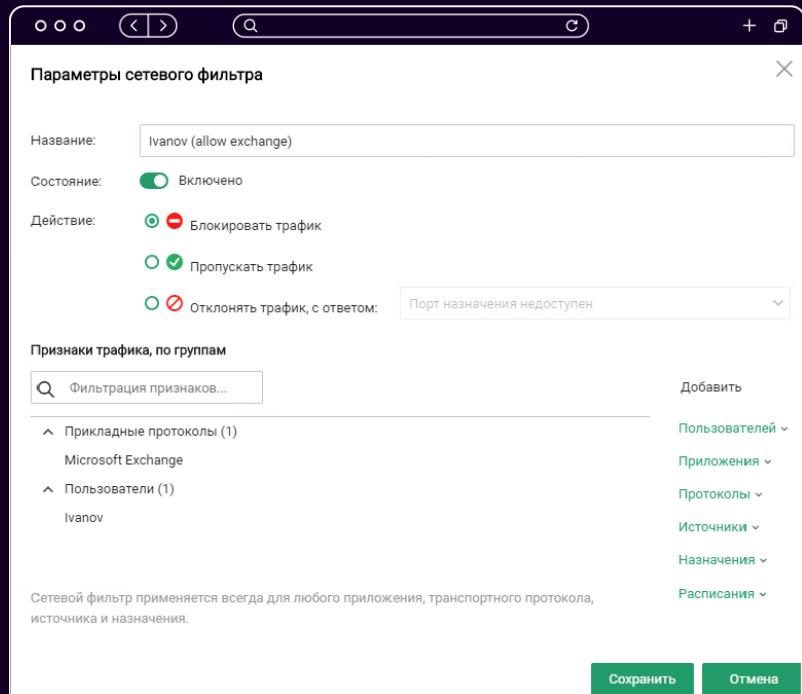


**Выявлять** подозрительную активность в сетевом трафике с помощью:

- правил IPS
- эвристического и поведенческого анализа

**Блокировать** компьютерные атаки и подозрительные действия с помощью:

- фильтров межсетевого экрана
- правил IPS + DPI
- фильтров контроля приложений



# ViPNet EPP



техноФест infoteсs

Выявлять подозрительную активность на конечных рабочих станциях с помощью:

- правил системы обнаружения и предотвращения вторжений
- эвристического анализа Anti-Malware
- обнаружения аномального поведения системных утилит

Блокировать компьютерные атаки и подозрительные действия с помощью:

- фильтров Межсетевого экрана
- списков ПО для Черного и Белого списка
- правил HIPS

The screenshot displays the ViPNet Endpoint Protection Server application. On the left is a sidebar with navigation links: Мониторинг (Monitoring), Инфопанель (Info Panel), События (Events), Управление защитой (Protection Management), Устройства (Devices), Базы правил (Rule Bases), Доверенная загрузка (Trusted Download), Обнаружение аномалий (Anomaly Detection), Критерии обнаружения аномалий (Anomaly detection criteria), Поведенческий анализ (Behavioral analysis), Anti-Malware, Сервис (Service), Журналы (Logs), Конфигурации (Configurations), Параметры системы (System parameters), Учетные записи (Accounts), Передача данных (Data transfer), Политика аудита (Audit policy), О программе (About the program), and Выход (Exit).

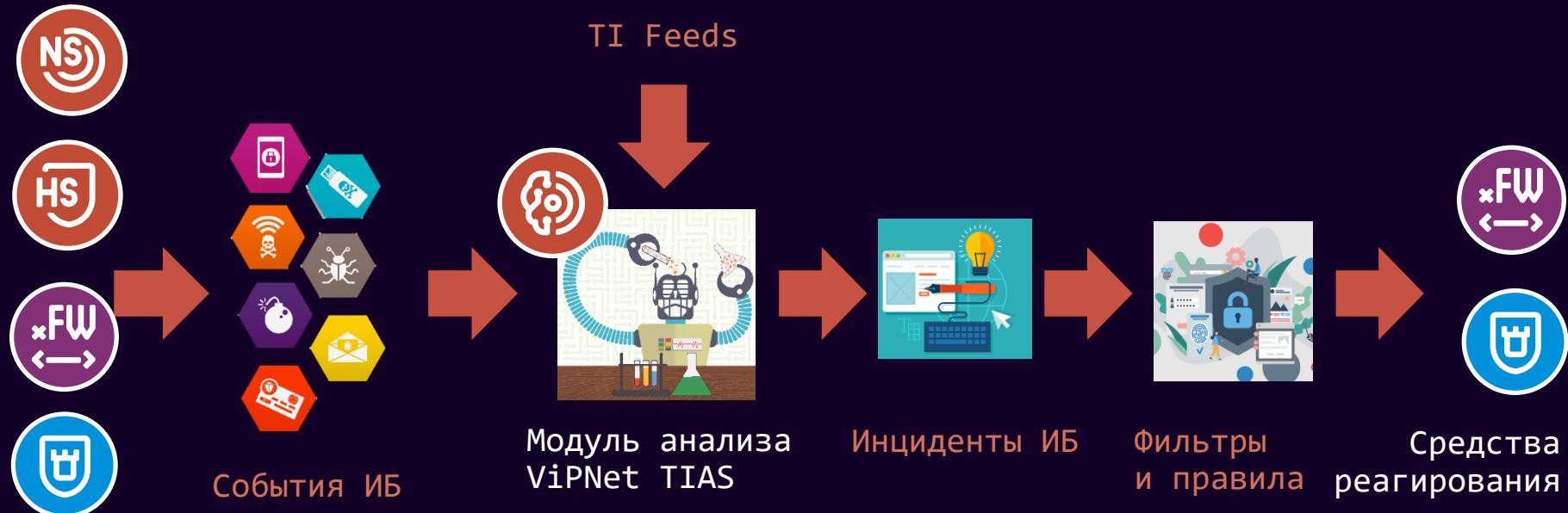
The main area is divided into three panels:

- Инфопанель (Info Panel):** Contains three cards:
  - Персональный межсетевой экран (Personal Firewall):** Shows 0 blocked traffic, 0 public network, 1 private network, 0 protected network, and 1 total host.
  - Контроль приложений (Application Control):** Shows 0 blocked, 1 allowed, 0 disabled, and 1 total host.
  - Обнаружение и предотвращение вторжений (Intrusion detection and prevention):** Shows 0 scanned, 1 basic, 0 minimal, 0 enhanced, and 1 total host.
- Запросы на подключение (Connection requests):** Shows 0 total requests and 24 available licenses.
- Сводка событий (Event summary):** Shows event counts for the last 15 minutes, 1 hour, 4 hours, and 8 hours.

At the bottom, there is a log viewer titled "Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы 'Усиленный'" (Rule editor - Intrusion detection and prevention - Rules for 'Enhanced' mode) with a table of rules.

Правило	Действие	Протокол	Адрес источника	Порт источника	Направление	Адрес назначения	Порт назначение
305560 - AM TROJAN_Suspect	Блокировать	TCP	\$HOME_NET	80	→	SEXTERNAL_NET	1433
306112 - AM SCAN RDP brute	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	22
305576 - AM SCAN SSH brute	Блокировать	TCP	\$HOME_NET	22	→	SEXTERNAL_NET	22
302350 - AM SCAN Possible C	Блокировать	TCP	SEXTERNAL_NET	4788	→	\$EXTERNAL_NET	80
302352 - AM SCAN BruteForce	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	4786
300641 - AM SCAN BruteForce	Блокировать	TCP	\$HOME_NET	23	→	SEXTERNAL_NET	80
300474 - AM SCAN BruteForce	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	3306
300472 - AM SCAN Hydra Br	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	25
210198 - GR SCAN Shodan	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80
210168 - GR SCAN SshWinn	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	22
2010017 - GR SCAN off-the-sh	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	22
2029577 - ET SCAN Polans Bot	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2029473 - ET SCAN ELF/JAR/Mal	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2029318 - ET SCAN Tomato Ro	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	HTTP_PORTS
2029317 - ET SCAN Tomato Ro	Блокировать	TCP	SEXTERNAL_NET	80	→	\$HOME_NET	HTTP_PORTS
2100484 - GPL SCAN PING Shf	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2100482 - GPL SCAN PING Cyb	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2100476 - GPL SCAN webmin	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2100474 - GPL SCAN supercal	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80
2100465 - GPL SCAN ISS Finger	Блокировать	ICMP	SEXTERNAL_NET	80	→	\$HOME_NET	80

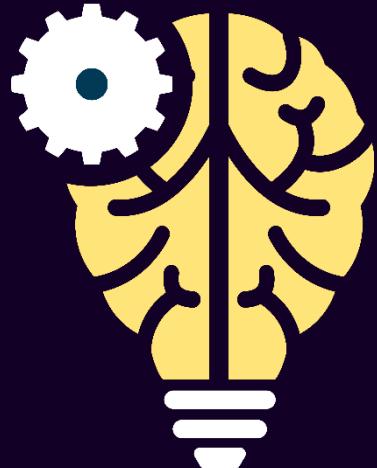
# Как это работает?



Источники событий

# Отличительные особенности

# Machine Learning



- Математическая модель принятия решений
- Алгоритмы машинного обучения
- Дообучение модели на данных пользователей
- Выявление атак нулевого дня

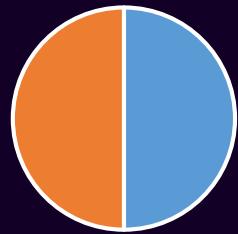
# Threat Intelligence



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

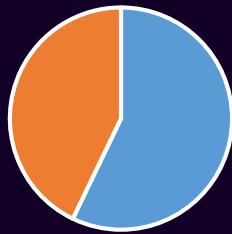
# Обновление правил и экспертных данных

Правила IDS NS



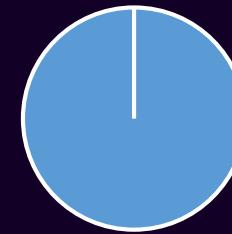
■ AM ■ ET ■ Всего: 27000

Правила IDS HS



■ AM ■ ET ■ Всего: 14000

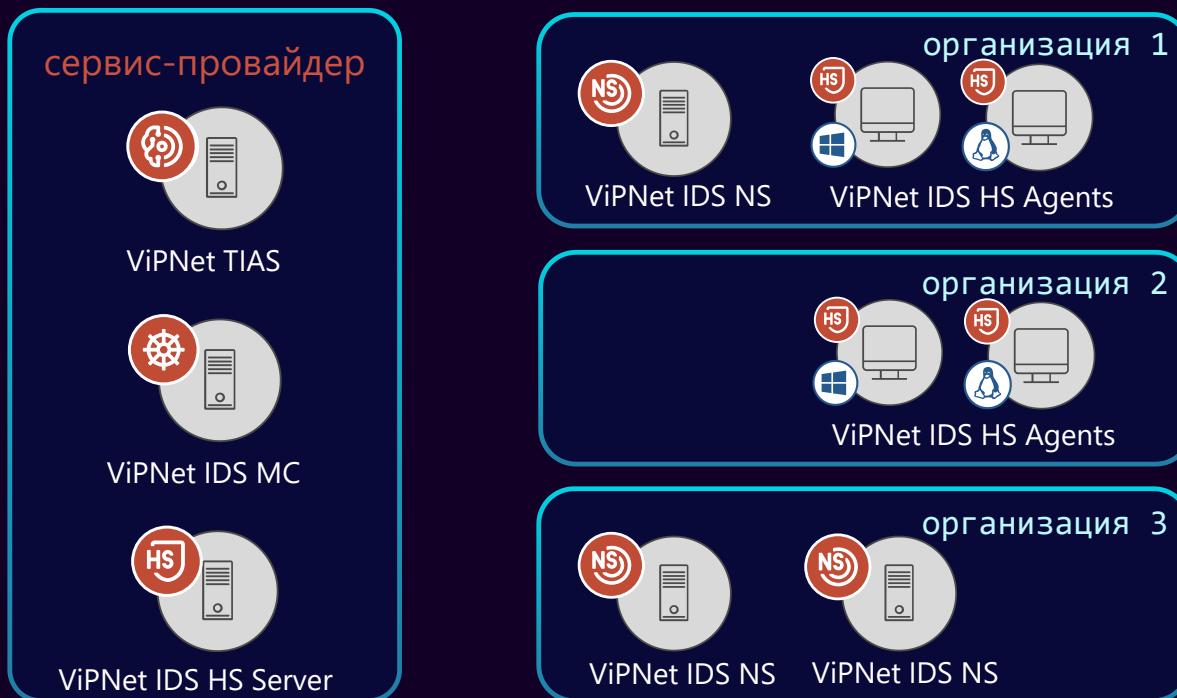
Правила TIAS



■ AM ■ Всего: 1015

Ежедневное обновление правил

# Облачный сервис на базе решения



# Производительность



**ViPNet IDS NS**

анализ трафика  
до 10 Гбит/с



**ViPNet TIAS**

анализ до 10 000 событий/с  
подключение до 200 IDS NS/xFW

подключение до 10 000 IDS/EPP agents  
*+ возможность построения иерархии*

# Сертификация

## СОА класса В Система IDS 3 в составе:

- ПАК ViPNet IDS NS
- ПО ViPNet IDS MC
- ПАК ViPNet TIAS



## СОВ 4 класс, ТДБ 4 уровень Система IDS 3 в составе:

- ПО ViPNet IDS NS
- ПО ViPNet IDS MC
- ПО ViPNet TIAS



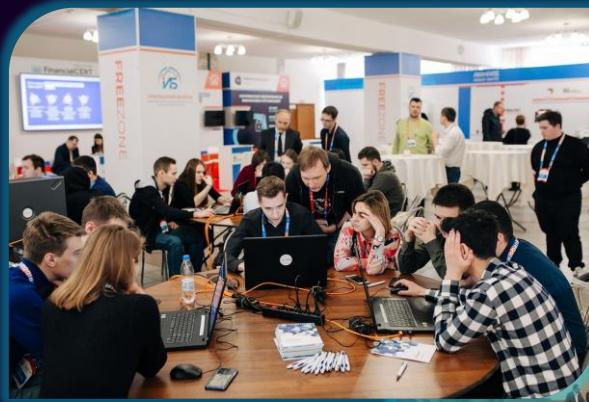
# Экспертное сопровождение и обучение

# Перспективный мониторинг



техноФест  
infotechs

- Киберучения на полигоне AMPIRE
- Центр мониторинга компьютерных атак
- Корпоративный центр ГосСОПКА
- Разработка правил
- Внедрение процедур безопасной разработки ПО
- Анализ защищённости
- Пентесты



# Учебный центр

infoteсs®  
УЧЕБНЫЙ ЦЕНТР

техноФест infoteсs



450 человек обучено на курсе  
«Администрирование IDS и TIAS»



18 ВУЗов имеют лаборатории,  
оснащенные ViPNet IDS и TIAS

# Техно infotechs фест

Подписывайтесь  
на наши соцсети,  
там много интересного

