

# Центр мониторинга и центр ГосСОПКА на базе решения ViPNet TDR



техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

Светлана Старовойт  
Руководитель продуктового направления

# Что такое Центр мониторинга и Центр ГосСОПКА

# Определения

## 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 инвентаризация ресурсов 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.<br>Должны иметь сертификаты соответствия ФСТЭК России   |
| 24. | Средства управления информацией об угрозах безопасности информации       | Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации.<br>Должны иметь формуляры, оформленные разработчиками (производителями) данных средств.<br>В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии) |
| 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.<br>Должны иметь сертификаты соответствия ФСТЭК России   |

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79. Перечень утвержден директором ФСТЭК России 19 апреля 2017 г.

# Мониторинг информационной безопасности средств и систем информатизации

| Наименование оборудования   | Технические и (или) функциональные характеристики   |
|---|---|
| 26. Средства управления инцидентами информационной безопасности   | <p>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.</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 | <p>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</p>   |



- 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

техно infotecs  
2023 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

# Варианты подключения

## Самостоятельное подключение



Субъект ГосСОПКА

- Заключение соглашения с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосСОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ



Объект КИИ

## Подключение через корпоративный центр



Корпоративный центр ГосСОПКА

- Заключение соглашения с корпоративным (ведомственным) центром ГосСОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности центра



# 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

# Общие требования к средствам ГосСОПКА

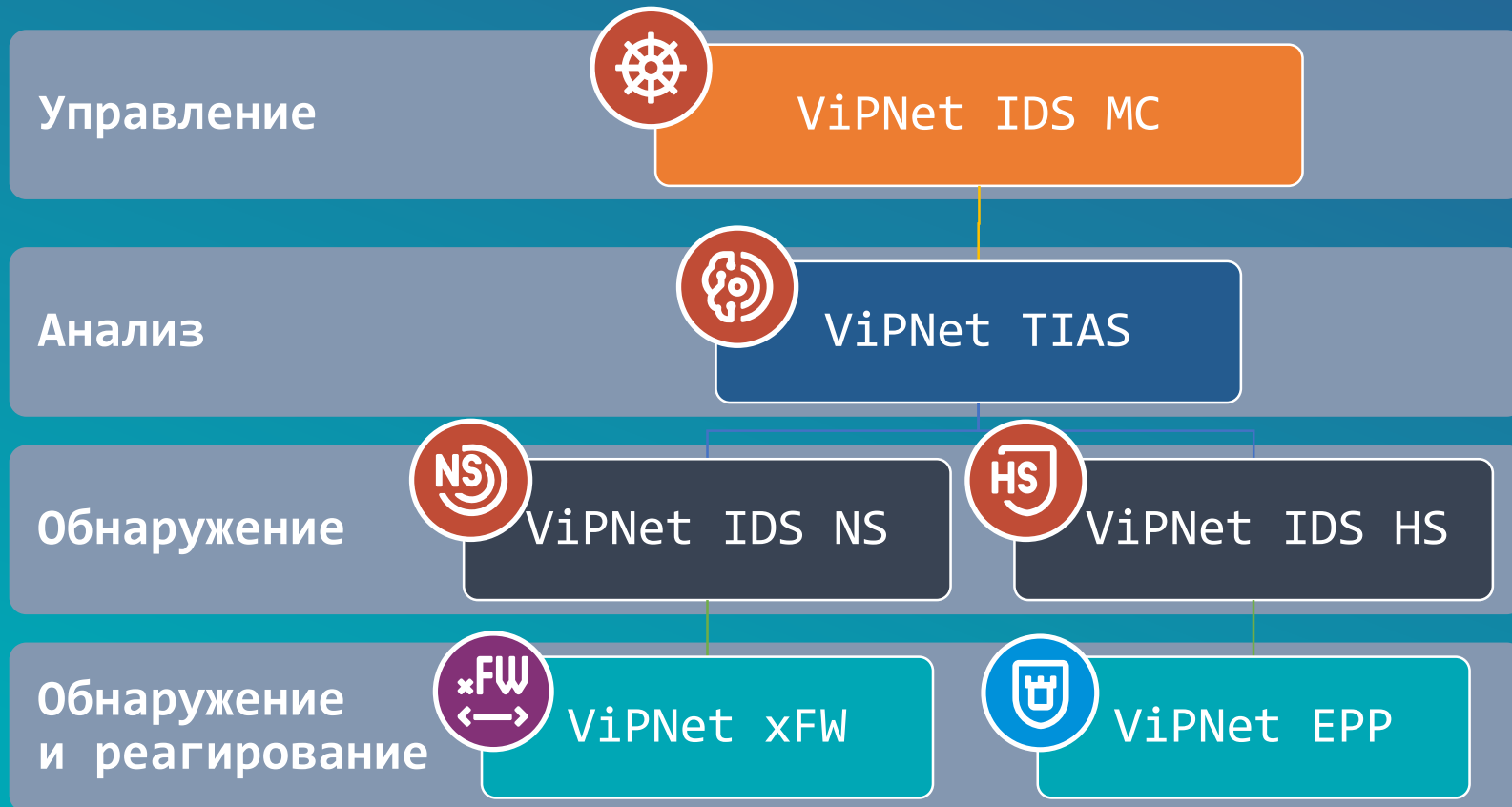


Средства ГосСОПКА должны соответствовать следующим требованиям:

- 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 гарантийной 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

# Решение ViPNet TDR

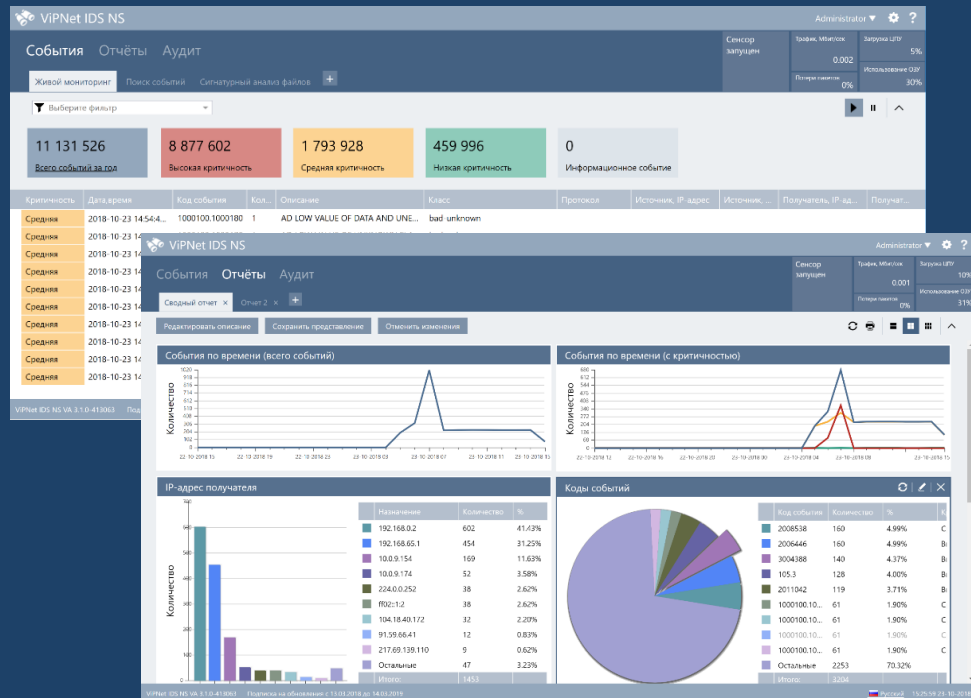
# Решение ViPNet TDR



# VIPNet IDS NS



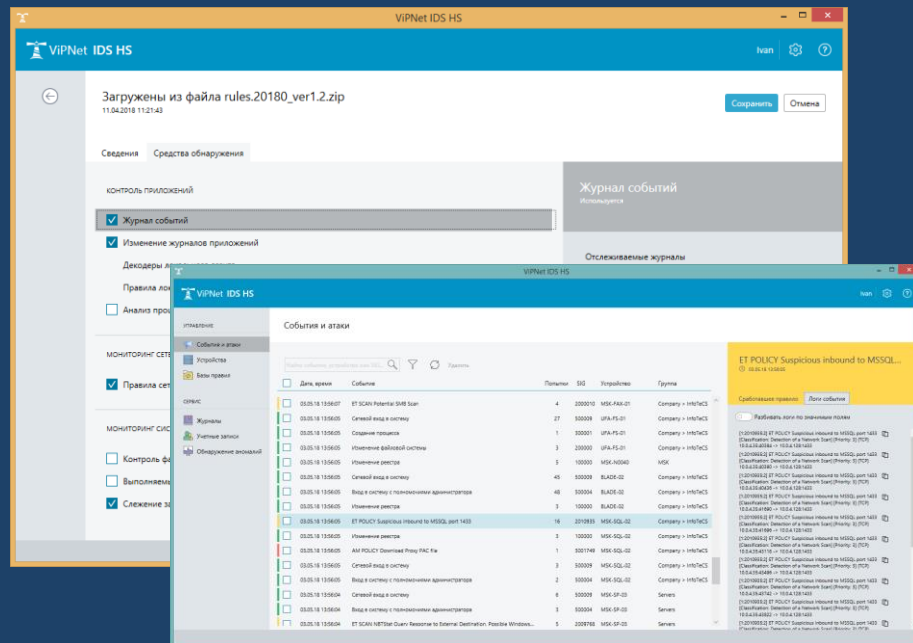
- Обнаруживать события ИБ в трафике
- Оповещать о событиях
- Хранить события
- Работать с событиями
- Управлять правилами и настройкой сигнатур



# VIPNet IDS HS



- **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



# VIPNet IDS MC



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

**Мониторинг**

| Устройство    | Статус  | Количество сенсоров |
|---------------|---------|---------------------|
| VIPNet IDS MC | Активен | 14 сенсоров         |
| VIPNet IDS MC | Активен | 1 сенсор            |
| VIPNet IDS MC | Активен | 2 сенсоров          |

**Зарегистрированные устройства**

| Имя устройства | Описание      | Тип устройства | Время ТП      | Типовые устройства |
|----------------|---------------|----------------|---------------|--------------------|
| 192.168.0.10   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.20   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.30   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.40   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.50   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.60   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.70   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.80   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.90   | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |
| 192.168.0.100  | VIPNet IDS MC | VIPNet IDS MC  | 3.5.0.0.0.0.0 | Типовые устройства |

**СЛОМOT**

Свойства: Описание: Имя: Параметры: Настройка: История: ...

Состояние: Активен

IP: 192.168.0.10

MAC: 08:00:27:00:00:00

Имя: СЛОМOT

Описание: СЛОМOT

Тип устройства: Типовые устройства

Время ТП: 3.5.0.0.0.0.0

Типовые устройства: Типовые устройства

Создан: 10.10.2024

Обновлен: 10.10.2024

Создан: 10.10.2024

Обновлен: 10.10.2024

Создан: 10.10.2024

Обновлен: 10.10.2024

Создан: 10.10.2024

Обновлен: 10.10.2024

Создан: 10.10.2024

Обновлен: 10.10.2024

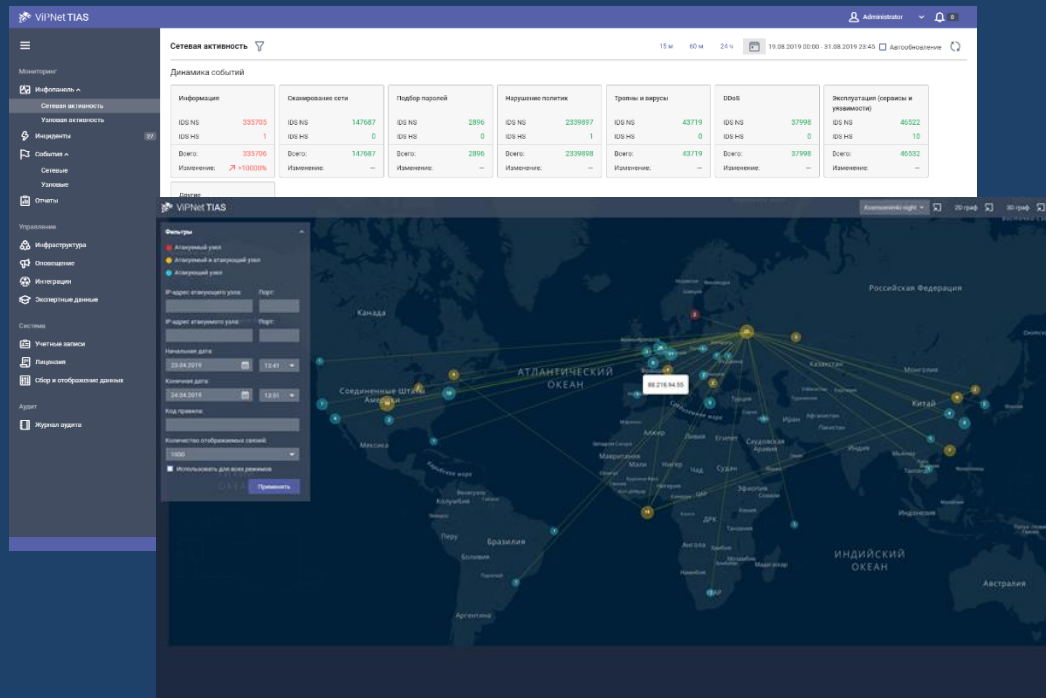
Создан: 10.10.2024

Обновлен: 10.10.2024

# VIPNet TIAS



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







**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

### Параметры сетевого фильтра

Название:

Состояние:  Включено

Действие:

- Блокировать трафик
- Пропускать трафик
- Отклонять трафик, с ответом:

Признаки трафика, по группам

Добавить

- ^ Прикладные протоколы (1)
  - Microsoft Exchange
- ^ Пользователи (1)
  - Ivanov

Сетевой фильтр применяется всегда для любого приложения, транспортного протокола, источника и назначения.



**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 Межсетевое экрана
- списков ПО для Черного и Белого списка
- правил HIPS

Виджет: **Персональный межсетевой экран**

| Режим                     | Хосты |
|---------------------------|-------|
| Полная блокировка трафика | 0     |
| Публичная сеть            | 0     |
| Частная сеть              | 1     |
| Защищенная сеть           | 0     |
| Сетевой экран отключен    | 0     |
| Всего                     | 1     |

Виджет: **Контроль приложений**

| Режим       | Хосты |
|-------------|-------|
| Блокировать | 0     |
| Разрешать   | 1     |
| Отключен    | 0     |
| Всего       | 1     |

Виджет: **Обнаружение и предотвращение вторжений**

| Режим       | Хосты |
|-------------|-------|
| Усиленный   | 0     |
| Базовый     | 1     |
| Минимальный | 0     |
| Отключен    | 0     |
| Всего       | 1     |

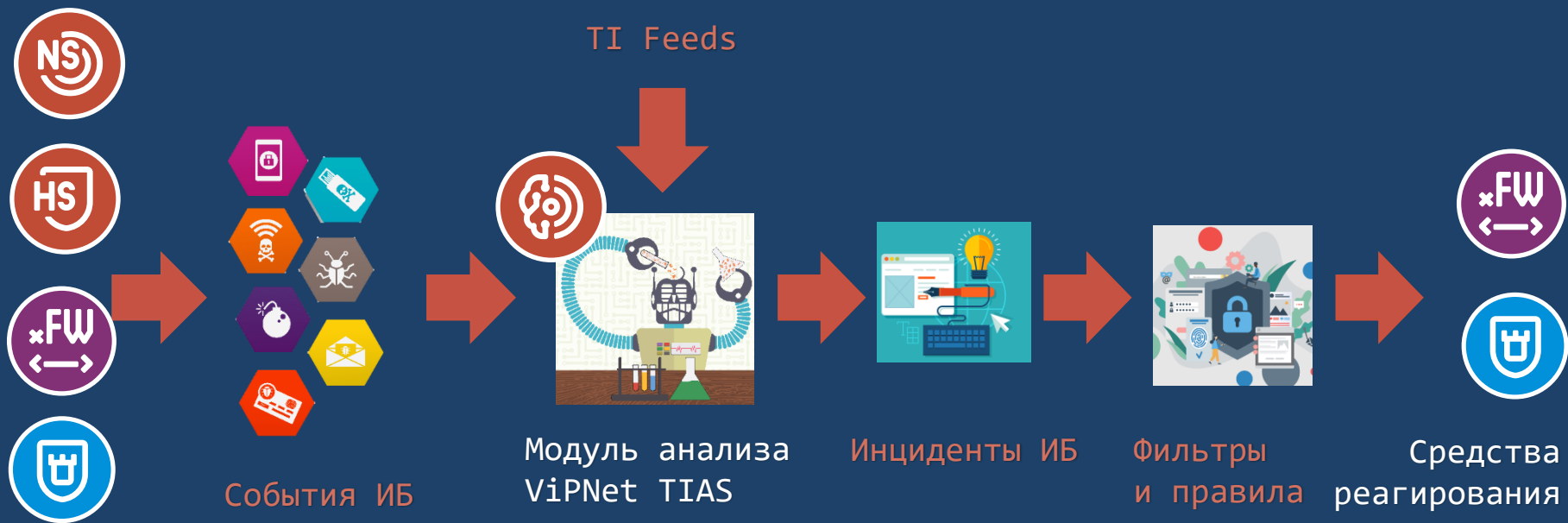
Запросы на подключение: Всего запросов: 0, Доступно лицензий: 24

Сводка событий: 15 мин, 1 час, 4 часа, 8 часов

Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы "Усиленный"

| Правило                       | Действие    | Протокол | Адрес источника | Порт источника | Направление | Адрес назначения | Порт назначения |
|-------------------------------|-------------|----------|-----------------|----------------|-------------|------------------|-----------------|
| 3055560 - AM Trojan's Suspici | Блокировать | TCP      | SHOME_NET       | Все            | →           | EXTERNAL_NET     | 1433            |
| 3063112 - AM SCAN RDP brute   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 3053796 - AM SCAN SSH brute   | Блокировать | TCP      | SHOME_NET       | Все            | →           | EXTERNAL_NET     | 22              |
| 3023530 - AM SCAN Possible C  | Блокировать | TCP      | EXTERNAL_NET    | 4786           | →           | SHOME_NET        | Все             |
| 3023529 - AM SCAN Possible C  | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | 4786            |
| 3006441 - AM SCAN Bruteforc   | Блокировать | TCP      | EXTERNAL_NET    | 23             | →           | EXTERNAL_NET     | Все             |
| 3004674 - AM SCAN Bruteforc   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | 3306            |
| 3004672 - AM SCAN Hydra Bru   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | 25              |
| 2101918 - GPL SCAN SolarWind  | Блокировать | ICMP     | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 2101638 - GPL SCAN SSH Versi  | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | 22              |
| 2100617 - GPL SCAN ssh-versa  | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | 22              |
| 2029577 - ET SCAN Polaris Bot | Блокировать | TCP      | EXTERNAL_NET    | SHFTP_PORTS    | →           | SHOME_NET        | Все             |
| 2028473 - ET SCAN ELF/MitM U  | Блокировать | TCP      | EXTERNAL_NET    | SHFTP_PORTS    | →           | SHOME_NET        | Все             |
| 2028318 - ET SCAN Tomato Ro   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | SHFTP_PORTS     |
| 2028317 - ET SCAN Tomato Ro   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | SHFTP_PORTS     |
| 2100484 - GPL SCAN PING Sni   | Блокировать | TCP      | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 2100483 - GPL SCAN PING Cys   | Блокировать | ICMP     | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 2100476 - GPL SCAN webtend    | Блокировать | ICMP     | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 2100474 - GPL SCAN iperf2     | Блокировать | ICMP     | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |
| 2100465 - GPL SCAN ISS Ping   | Блокировать | ICMP     | EXTERNAL_NET    | Все            | →           | SHOME_NET        | Все             |

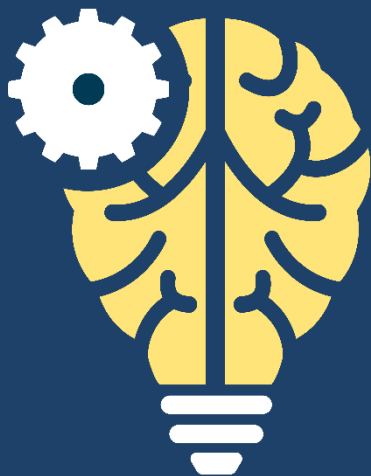
# Как это работает?



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

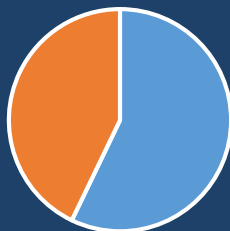
# Обновление правил и экспертных данных

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

## сервис-провайдер



ViPNet TIAS



ViPNet IDS MC



ViPNet IDS HS Server

## организация 1



ViPNet IDS NS



ViPNet IDS HS Agents

## организация 2



ViPNet IDS HS Agents

## организация 3



ViPNet IDS NS



ViPNet IDS NS



# 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

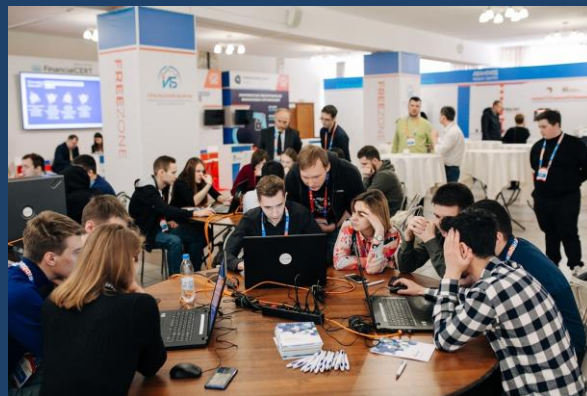


# Экспертное сопровождение и обучение

# Перспективный мониторинг



- Центр мониторинга компьютерных атак
- Корпоративный центр ГосСОПКА
- Разработка правил Snort IDS
- Внедрение процедур безопасной разработки ПО
- Анализ защищённости
- Пентесты
- Подготовка специалистов на киберполигоне



# Учебный центр



237 человек обучено на курсе  
«Администрирование IDS и TIAS»



12 ВУЗов имеют лаборатории,  
оснащенные ViPNet IDS и TIAS

техно infotecs  
2023 Фест

Спасибо  
за внимание!

---

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)