

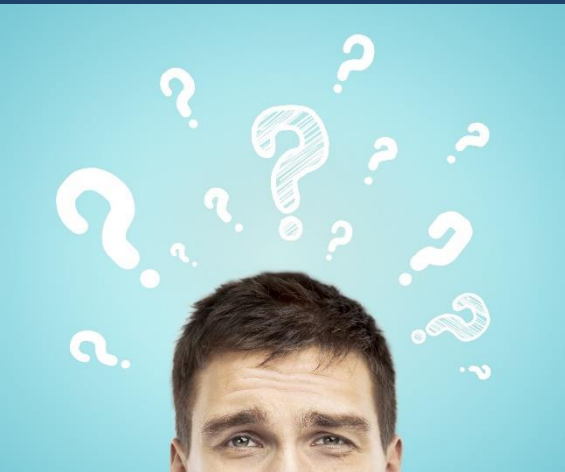
Центр мониторинга и центр ГосСОПКА на базе решения ViPNet TDR

Светлана Старовойт
Менеджер продуктов

техно infotecs
2022 Фест

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

Мониторинг информационной безопасности средств и систем информатизации

	Наименование оборудования	Технические и (или) функциональные характеристики
22.	Средства (системы) контроля (анализа) защищенности информационных систем	<p>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.</p> <p>Должны иметь сертификаты соответствия ФСТЭК России</p>
24.	Средства управления информацией об угрозах безопасности информации	<p>Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации.</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>
25.	Средства управления событиями безопасности информации	<p>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.</p> <p>Должны иметь сертификаты соответствия ФСТЭК России</p>

*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 А

- Взаимодействие с НКЦКИ
- Разработка регламентирующих документов
- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах
- Регистрация атак и инцидентов
- Анализ событий ИБ
- Инвентаризация

Класс Б

- Анализ угроз ИБ
- Составление и актуализация перечня угроз
- Выявление уязвимостей
- Подготовка предложений по повышению уровня защищенности
- Составление перечня инцидентов

Класс В

- Ликвидация последствий
- Анализ результатов ликвидации последствий

Варианты подключения

Самостоятельное подключение

ГОССОПКА

Субъект
ГосСОПКА

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



Подключение через корпоративный центр

ГОССОПКА

Корпоративный центр
ГосСОПКА

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



Объект КИИ

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

Общие требования к средствам ГосСОПКА

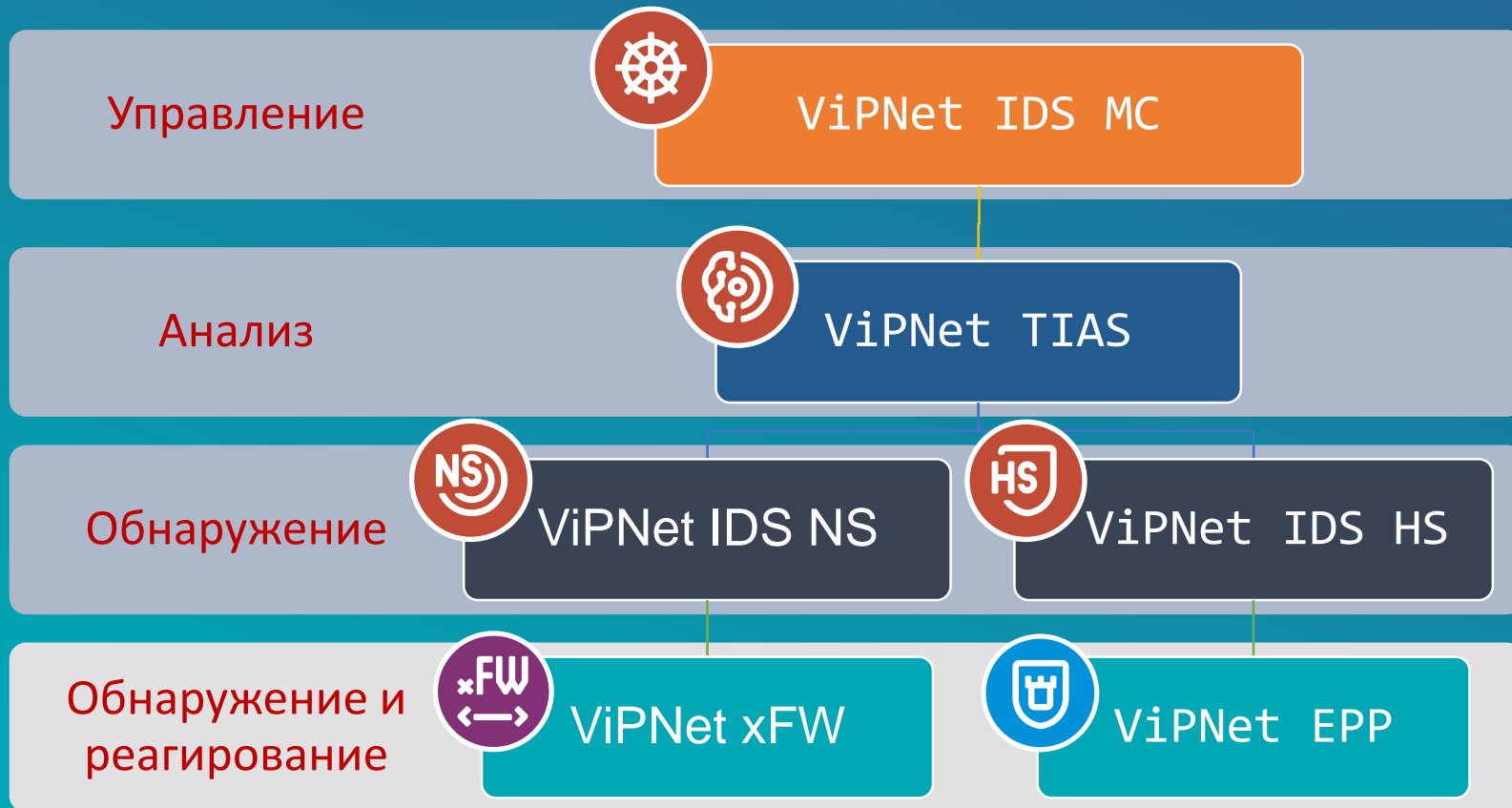


Средства ГосСОПКА должны соответствовать следующим требованиям:

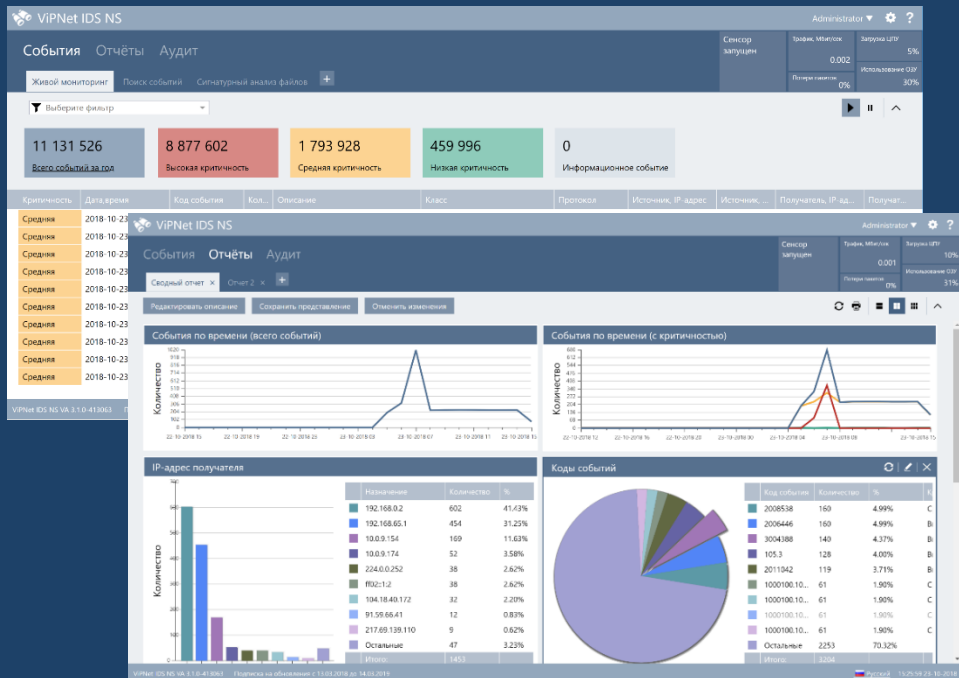
- Должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта КИИ или привлекаемыми работниками
- Должна быть исключена возможность несанкционированной передачи обрабатываемой информации
- Должны иметь возможность модернизации российскими организациями, 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

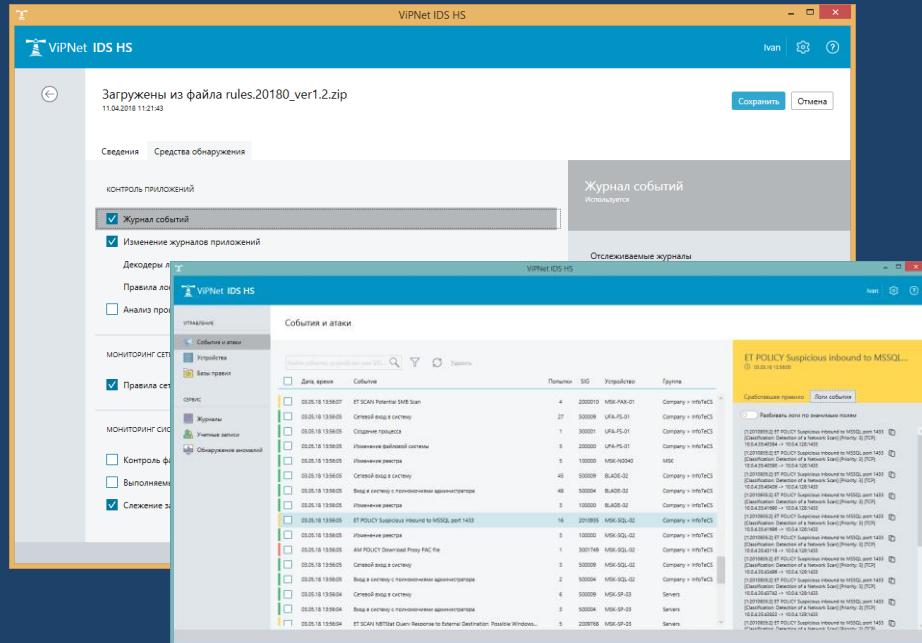


- Обнаруживать события ИБ в трафике
- Оповещать о событиях
- Хранить события
- Работать с событиями
- Управлять правилами и настройкой сигнатур





- **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





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

Мониторинг

Статус	Количество
VIPNet IDS MC (14 сенсоров)	14 сенсоров
VIPNet IDS MC (1 устройство)	1 устройство
VIPNet IDS MC (2 правила)	2 правила

Зарегистрированные устройства

Имя устройства	IP-адрес	Сеть	Порт	Время ТП	Статус устройства
Алгоритм	192.168.0.100	VIPNet-83.145.151	1.5.5.200003		Получены данные с устройства
Алгоритм	192.168.0.200	VIPNet-83.145.151	1.5.5.200003		Получены данные с устройства
Алгоритм	192.168.0.101	VIPNet-83.145.151	1.5.5.200103		Получены данные с устройства
Алгоритм	192.168.0.102	VIPNet-83.145.151	1.5.5.200103		Получены данные с устройства
Алгоритм	192.168.0.103	VIPNet-83.145.151	1.5.5.200103		Получены данные с устройства

CLOMOT
ID: 100-000-011

Свойства правила: 100-000-011-001

Время жизни: 4007

Модель устройства: X1010A0010

Описание: Личный компьютер на базе ОС Windows

Описание события: Дублирование IP 192.168.100.1

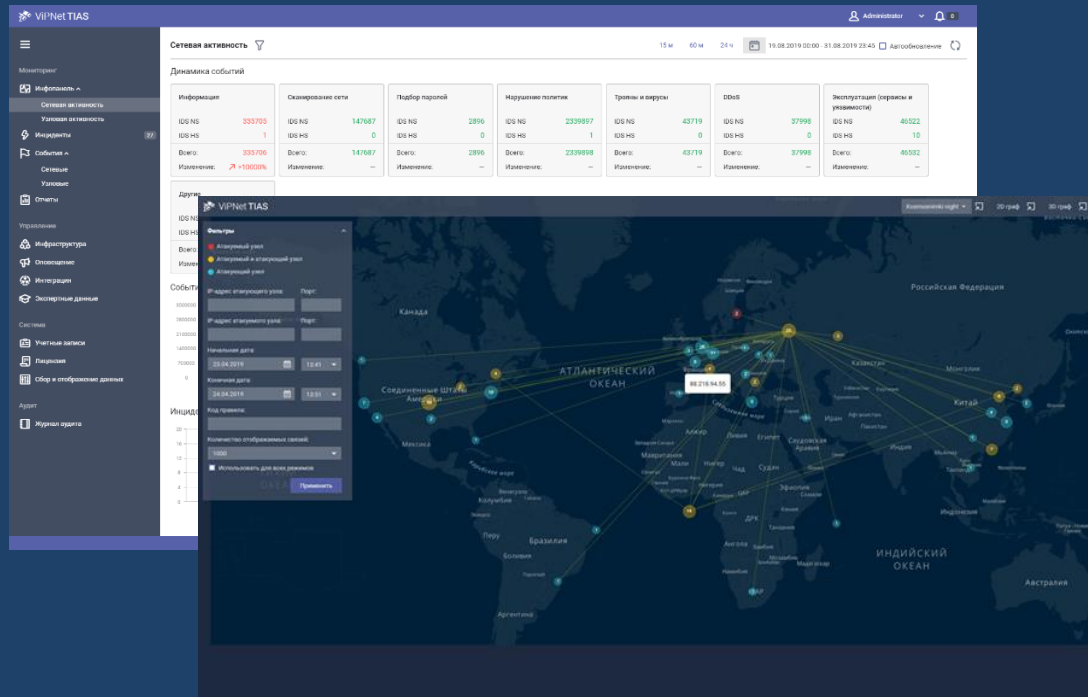
Область охвата: Все

Модель устройства: X1010A0010

Время жизни: 4007

Создано: 10/20/2011 11:45:00

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



The screenshot displays the VIPNet TIAS dashboard. The main section is titled 'Сетевая активность' (Network Activity) and shows a 'Динамика событий' (Event Dynamics) table. The table has columns for 'Информация' (Information), 'Сканирование сети' (Network Scanning), 'Выбор портов' (Port Selection), 'Массовые попытки' (Massive Attempts), 'Трениры и вбросы' (Trainers and Dumps), 'DDoS', and 'Эксплуатация (скрипты и уязвимости)' (Exploitation (scripts and vulnerabilities)).

Информация	Сканирование сети	Выбор портов	Массовые попытки	Трениры и вбросы	DDoS	Эксплуатация (скрипты и уязвимости)
IDS NG: 333709	IDS NG: 147687	IDS NG: 2896	IDS NG: 2329897	IDS NG: 43719	IDS NG: 37998	IDS NG: 46522
IDS MS: 1	IDS MS: 0	IDS MS: 0	IDS MS: 1	IDS MS: 0	IDS MS: 0	IDS MS: 10
Всего: 333709	Всего: 147687	Всего: 2896	Всего: 2329898	Всего: 43719	Всего: 37998	Всего: 46532
Изменения: ▲ +30020%	Изменения: --	Изменения: --	Изменения: --	Изменения: --	Изменения: --	Изменения: --

Below the table, there is a 'События' (Events) section with a search form and a 'Инциденты' (Incidents) section. A map of the Atlantic Ocean region is visible in the background, showing network connections between various countries and cities.



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

Прикладные протоколы (1)	Пользователей
Microsoft Exchange	Приложения
Пользователи (1)	Протоколы
Ivanov	Источники
	Назначения
	Расписания

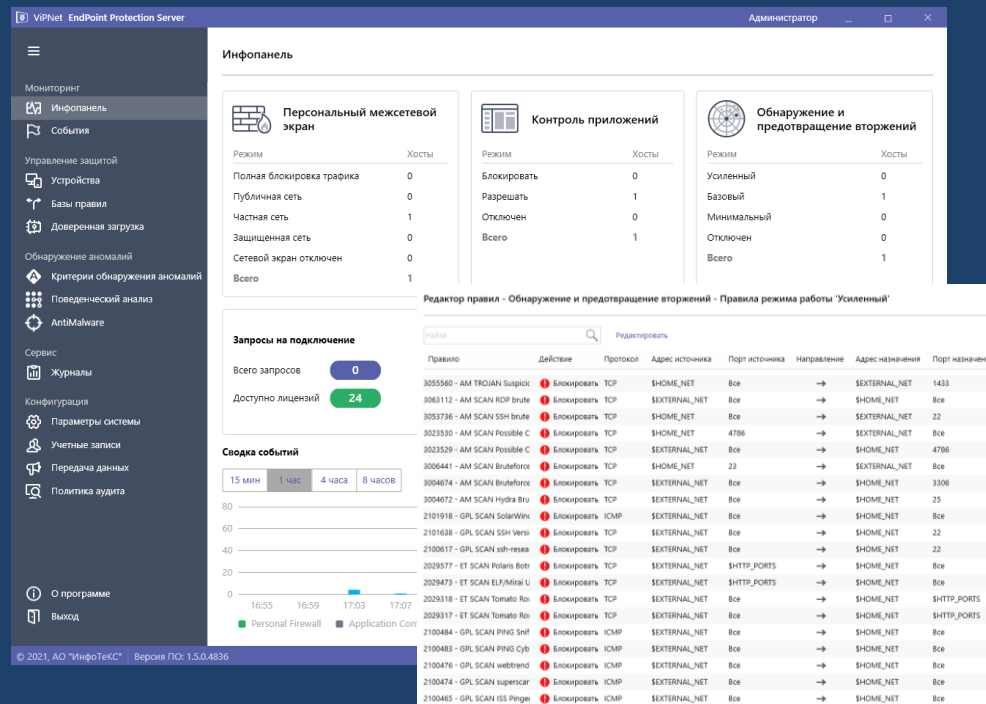
Сетевой фильтр применяется всегда для любого приложения, транспортного протокола, источника и назначения.

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 Межсетевой экрана
- списков ПО для Черного и Белого списка
- правил HIPS



Инфопанель

Персональный межсетевой экран

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

Контроль приложений

Режим	Хосты
Блокировать	0
Разрешать	1
Отключен	0
Всего	1

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

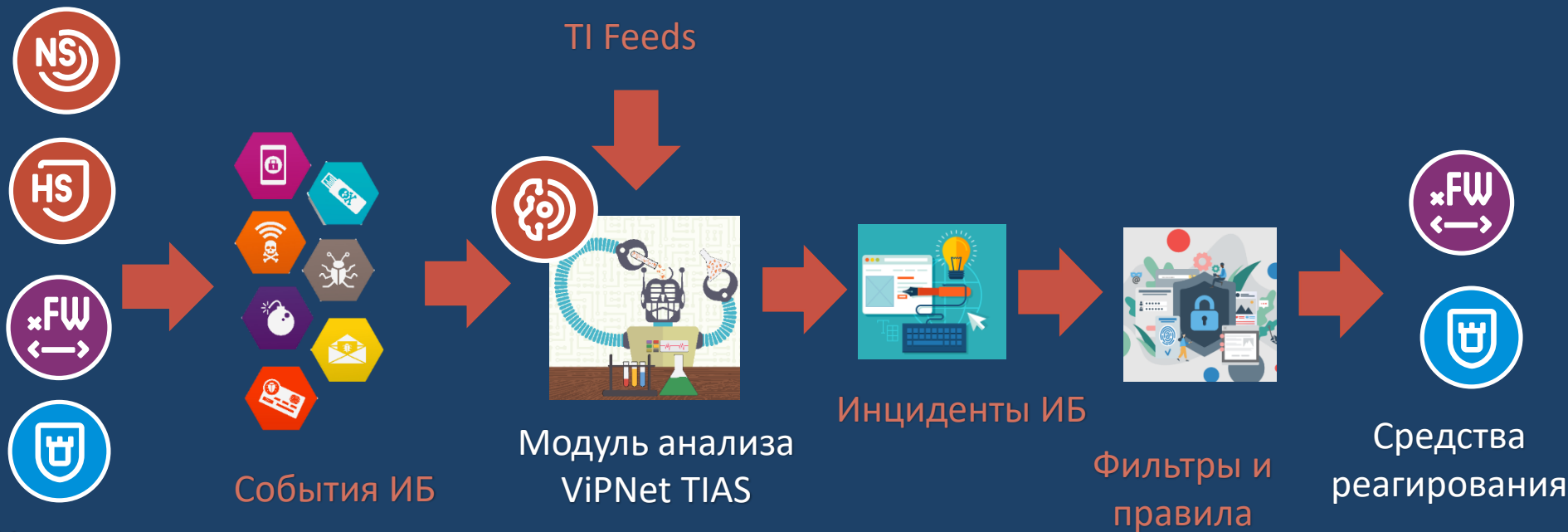
Сводка событий

15 мин | 1 час | 4 часа | 8 часов

Правило	Действие	Протокол	Адрес источника	Порт источника	Направление	Адрес назначения	Порт назначения
3055560 - AM TROJAN Suspici	Блокировать	TCP	SHOME_NET	Все	→	SEXTERNAL_NET	1433
3063112 - AM SCAN RDP brute	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
3053736 - AM SCAN SSH brute	Блокировать	TCP	SHOME_NET	Все	→	SEXTERNAL_NET	22
3023529 - AM SCAN Possible C	Блокировать	TCP	SHOME_NET	4796	→	SEXTERNAL_NET	8ce
3023529 - AM SCAN Possible C	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	4796
3006441 - AM SCAN BruteForce	Блокировать	TCP	SHOME_NET	23	→	SEXTERNAL_NET	8ce
3004674 - AM SCAN BruteForce	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	3306
3004674 - AM SCAN Hydra Bru	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	25
2101918 - GPL SCAN SolarWind	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
2101628 - GPL SCAN SSH versu	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	22
2102617 - GPL SCAN ssh-rescue	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	22
2029577 - ET SCAN Polarix Bot	Блокировать	TCP	SEXTERNAL_NET	\$HTTP_PORTS	→	SHOME_NET	8ce
2029473 - ET SCAN ELF/Mitlra U	Блокировать	TCP	SEXTERNAL_NET	\$HTTP_PORTS	→	SHOME_NET	8ce
2029318 - ET SCAN Tomato Roi	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	\$HTTP_PORTS
2029317 - ET SCAN Tomato Roi	Блокировать	TCP	SEXTERNAL_NET	Все	→	SHOME_NET	\$HTTP_PORTS
2100484 - GPL SCAN PING Srf	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
2100483 - GPL SCAN PING Srf	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
2100476 - GPL SCAN webtrend	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
2100474 - GPL SCAN supercar	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce
2100465 - GPL SCAN ISS Ping	Блокировать	ICMP	SEXTERNAL_NET	Все	→	SHOME_NET	8ce

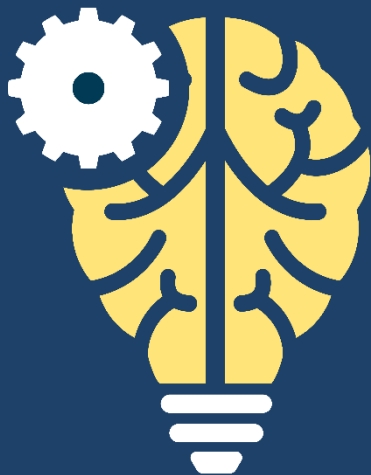
© 2021, АО "ИнфоТекс" Версия ПО: 1.5.0.4836

Как это работает?



Отличительные особенности

Machine Learning



- Математическая модель принятия решений
- Алгоритмы машинного обучения
- Обучение модели на реальных данных
- 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

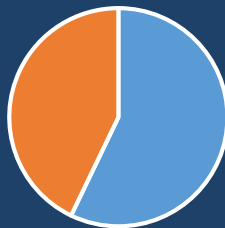
Обновление правил и экспертных данных

Правила IDS NS



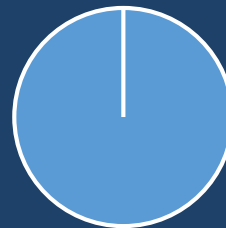
AM ET Всего: 27000

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

Производительность и потребность в ресурсах



ViPNet IDS NS



анализ трафика
до 10 Гбит/с



ViPNet TIAS



анализ до 10 000 событий/с
подключение до 200 IDS NS
подключение до 10 000 IDS HS Agents



ViPNet IDS HS Agent

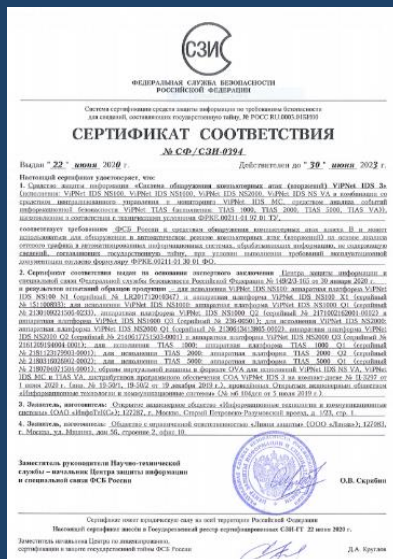
потребляет ~ 60 Мбайт
оперативной памяти

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





237 человек обучено на курсе
«Администрирование IDS и TIAS»



12 ВУЗов имеют лаборатории,
оснащенные VipNet IDS и TIAS

ТЕХНО infotecs
2022 ФЕСТ

Спасибо
за внимание!

Информационный
партнер



Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363