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

Светлана Старовойт

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 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. 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. 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 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

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	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. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
27.	Средства защиты каналов передачи данных	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. Должны иметь сертификаты соответствия ФСБ России
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

ТЕХНО infotecs 2024 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

ГОССОПКА

Субъект ГосСОПКА

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

НКЦКИ

Субъект КИИ

Подключение через корпоративный центр

ГОССОПКА

Корпоративный центр ГосСОПКА

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

с 13 ДЕКАБРЯ 2025: Пройти аккредитацию

Передача информации в ГосСОПКА

Центр ГосСОПКА

ГОССОПКА

НКЦКИ

Сайт Роскомнадзор

РОСКОМНАДЗОР

Субъекты КИИ и ФСТЭК

24 часа - инцидент

Операторы ПД

24 часа - инцидент
3 суток – уведомление о результатах

Общие требования к средствам ГосСОПКА

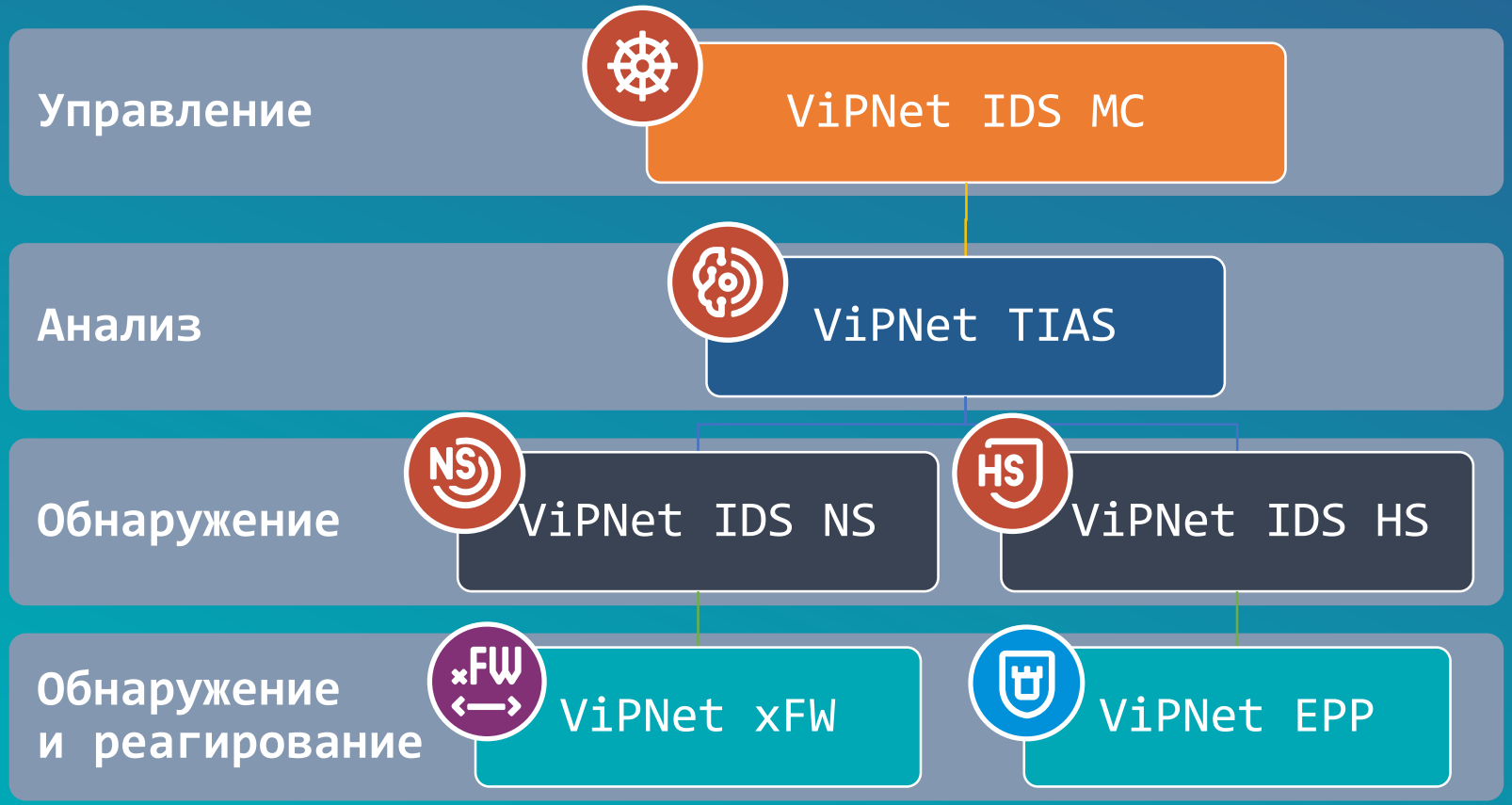
Средства ГосСОПКА должны соответствовать следующим требованиям:

- 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 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

Приказ № 196 от 6 мая 2019 года

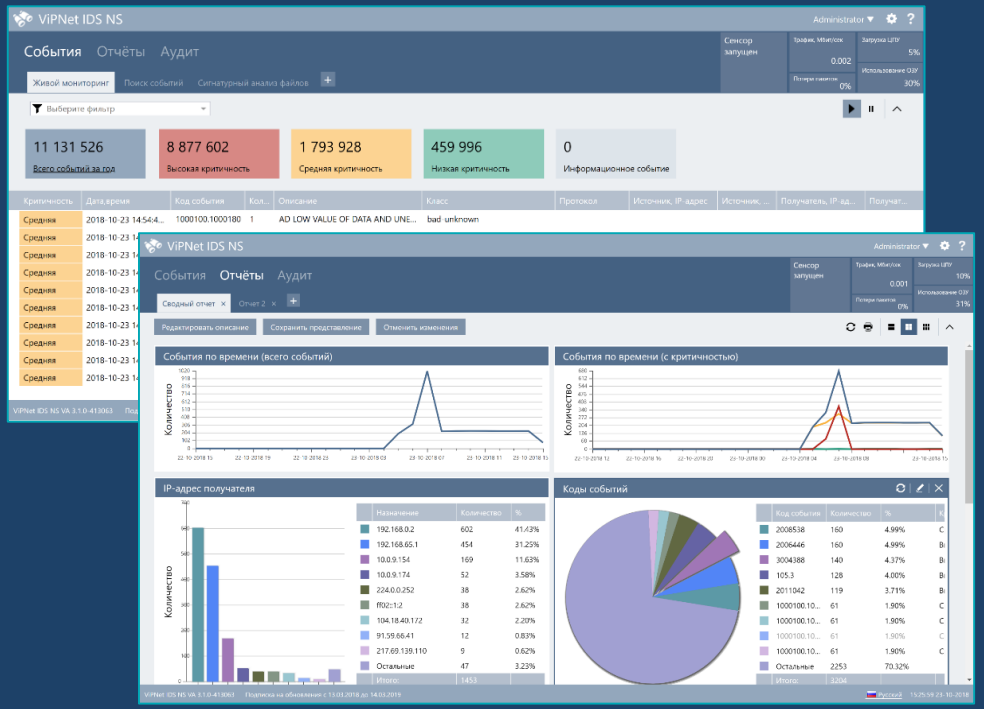
Решение ViPNet TDR

Решение ViPNet TDR



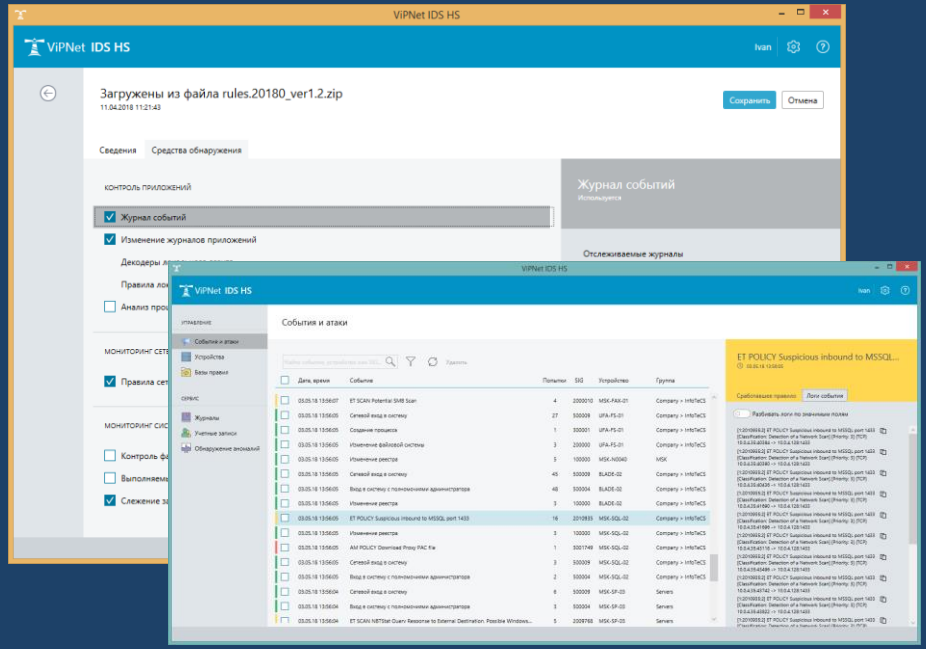
ViPNet IDS NS

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



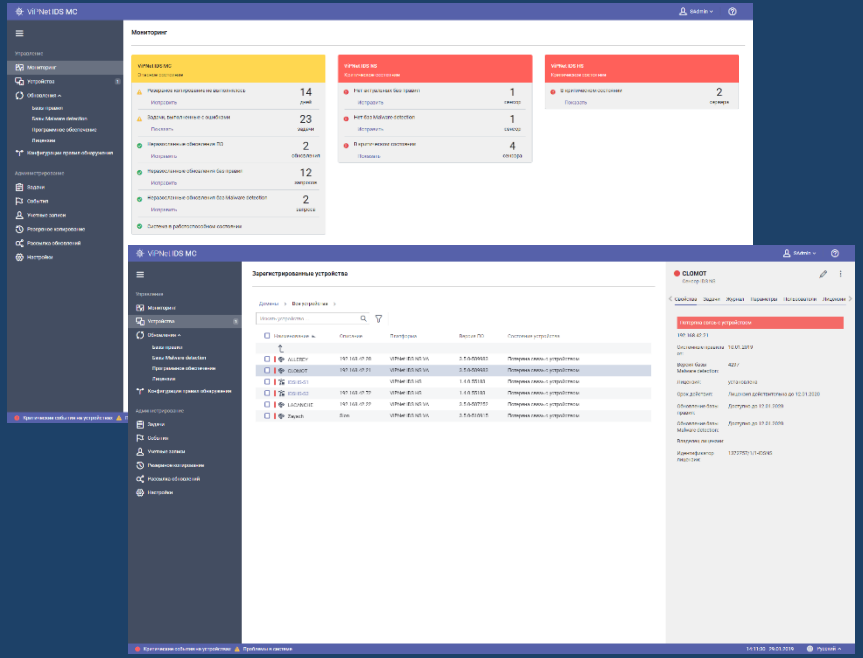
ViPNet IDS HS

- 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



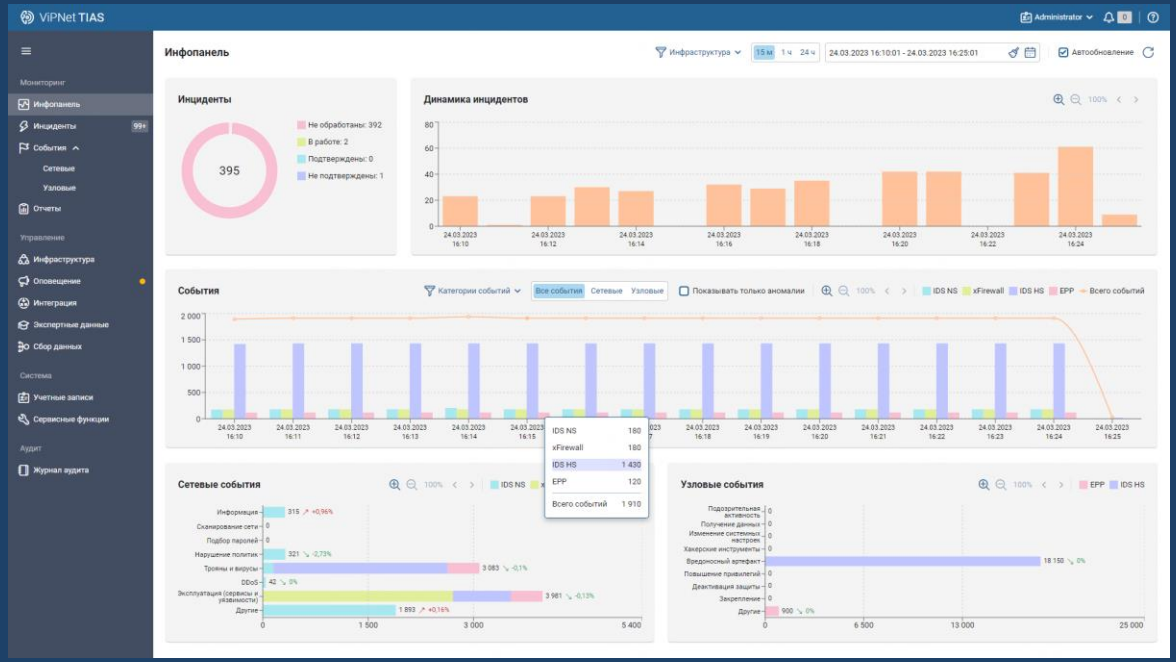
ViPNet IDS MC

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



ViPNet TIAS

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



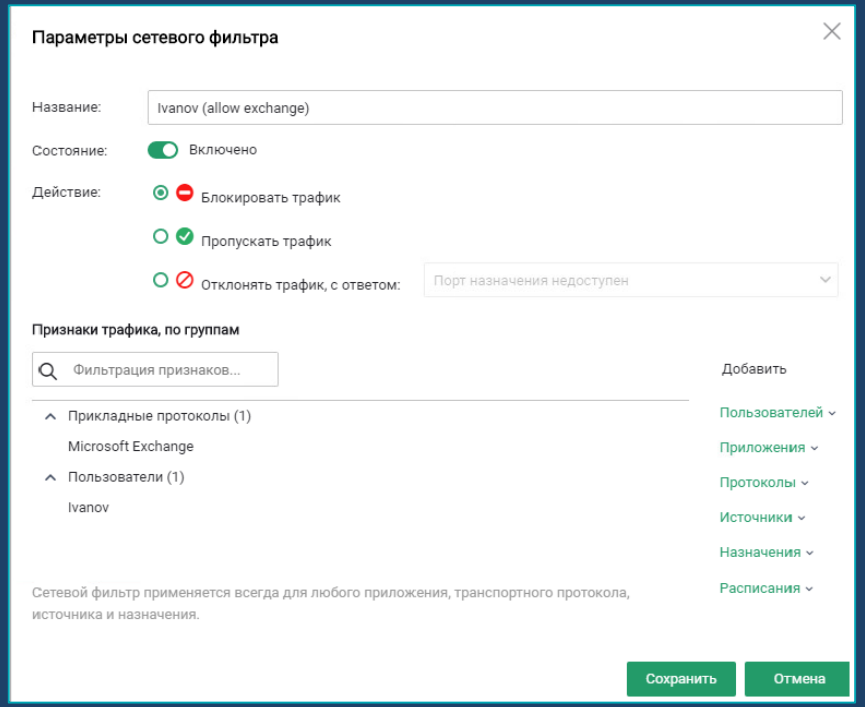
ViPNet xFirewall

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



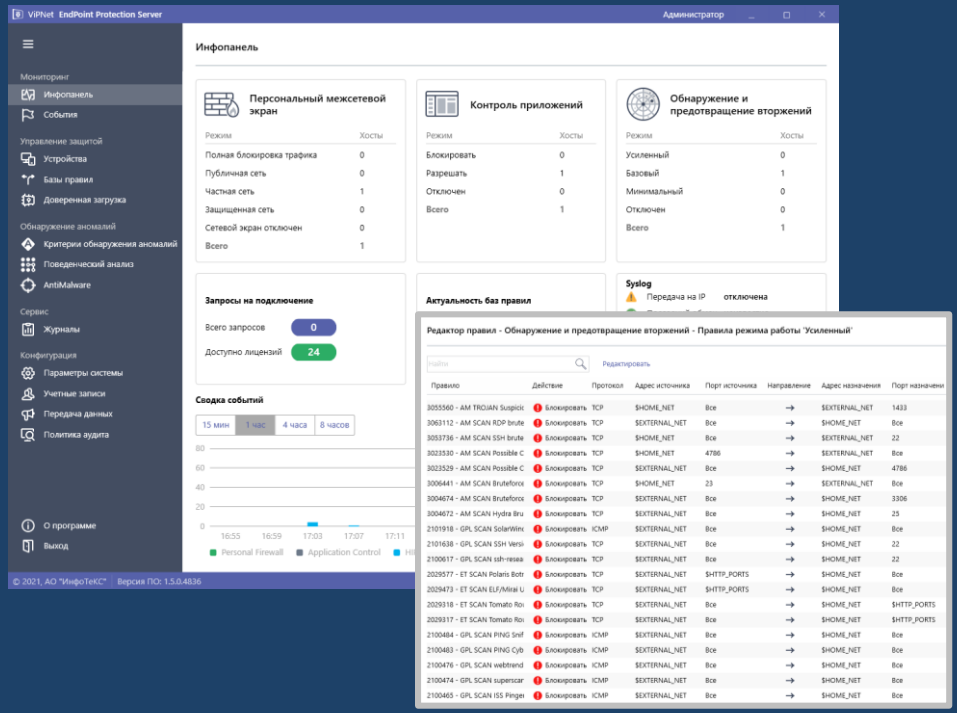
ViPNet EPP

Выявлять подозрительную активность на конечных рабочих станциях с помощью:

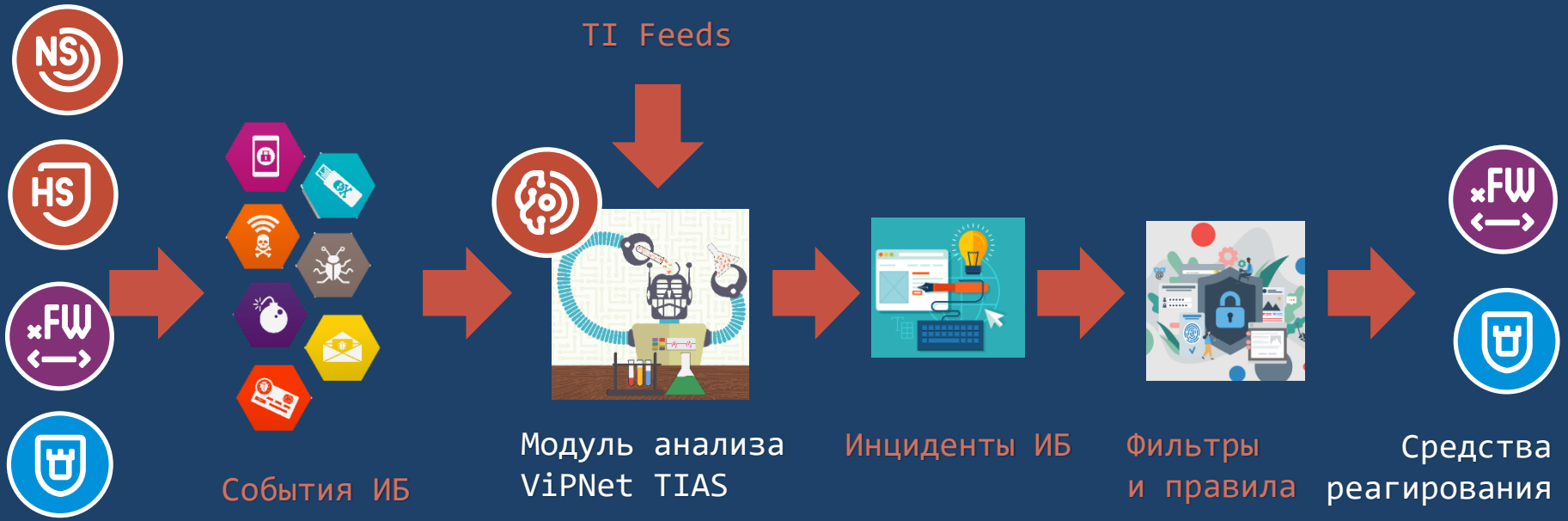
- правил системы обнаружения и предотвращения вторжений
- эвристического анализа Anti-Malware
- обнаружения аномального поведения системных утилит

Блокировать компьютерные атаки и подозрительные действия с помощью:

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

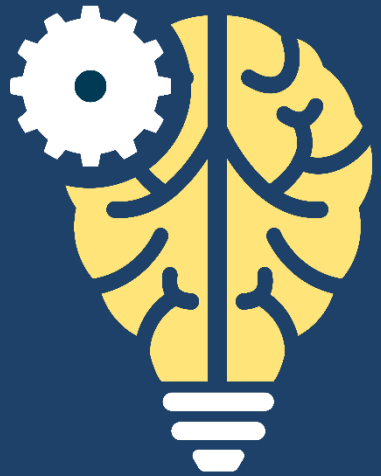


Как это работает?



Отличительные особенности

Machine Learning



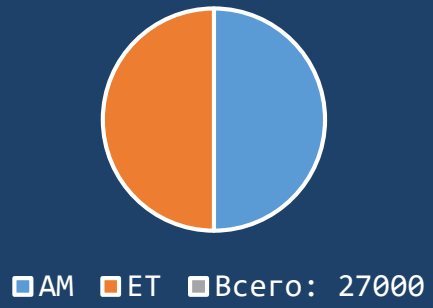
- Математическая модель принятия решений
- Алгоритмы машинного обучения
- Дообучение модели на данных пользователей
- Выявление атак нулевого дня

Threat Intelligence

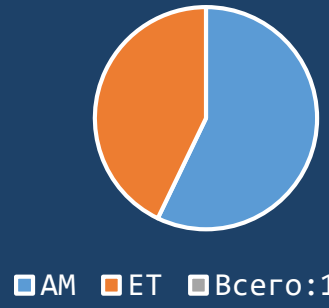
- Индикаторы атак и компрометации
- TTП – тактики, техники, процедуры
- Информационный обмен:
  - СОПКА
  - ФСТЭК
  - RU-CERT
- Опыт клиентов – верифицированная и обезличенная информация

Обновление правил и экспертных данных

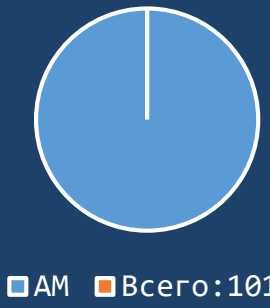
Правила IDS NS



Правила IDS HS

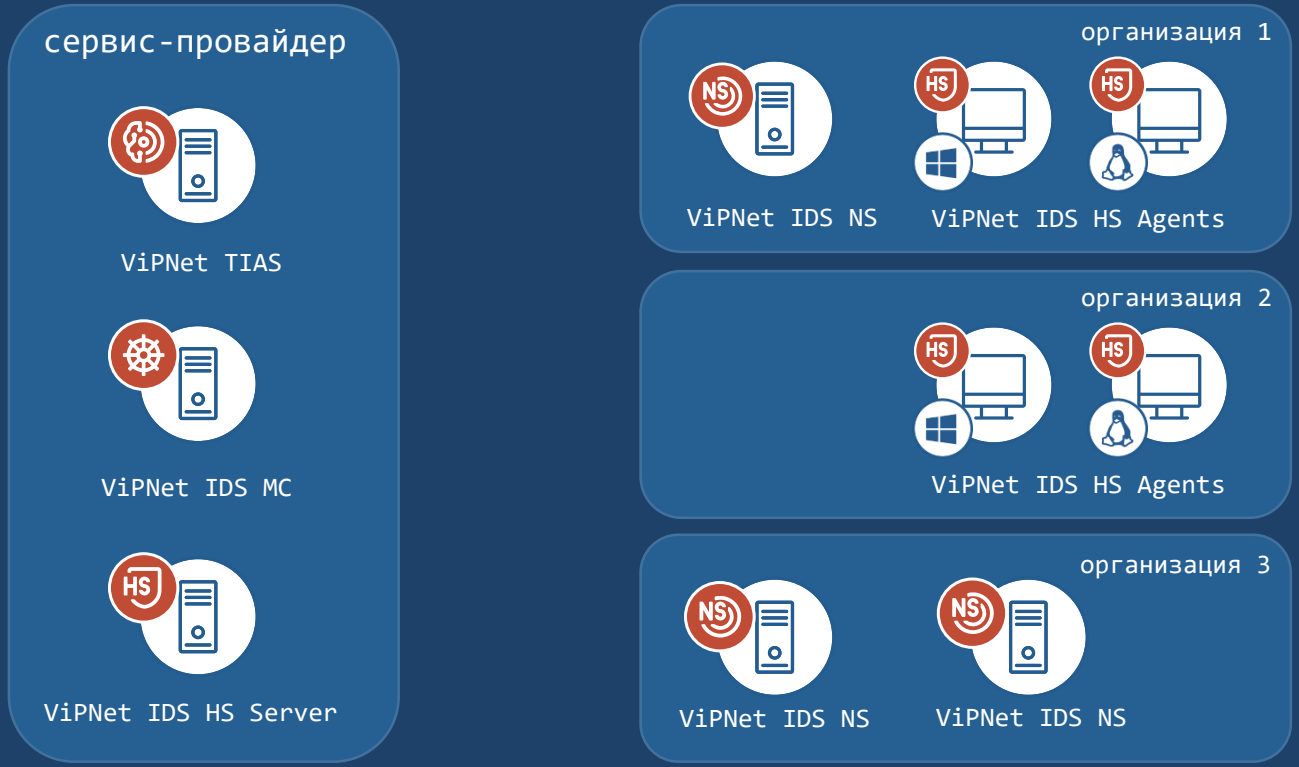


Правила TIAS



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

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

Учебный центр

450 человек обучено на курсе «Администрирование IDS и TIAS»

18 ВУЗов имеют лаборатории, оснащенные ViPNet IDS и TIAS

ТЕХНО 2024 infotecs ФЕСТ

Спасибо за внимание

Подписывайтесь на наши соцсети