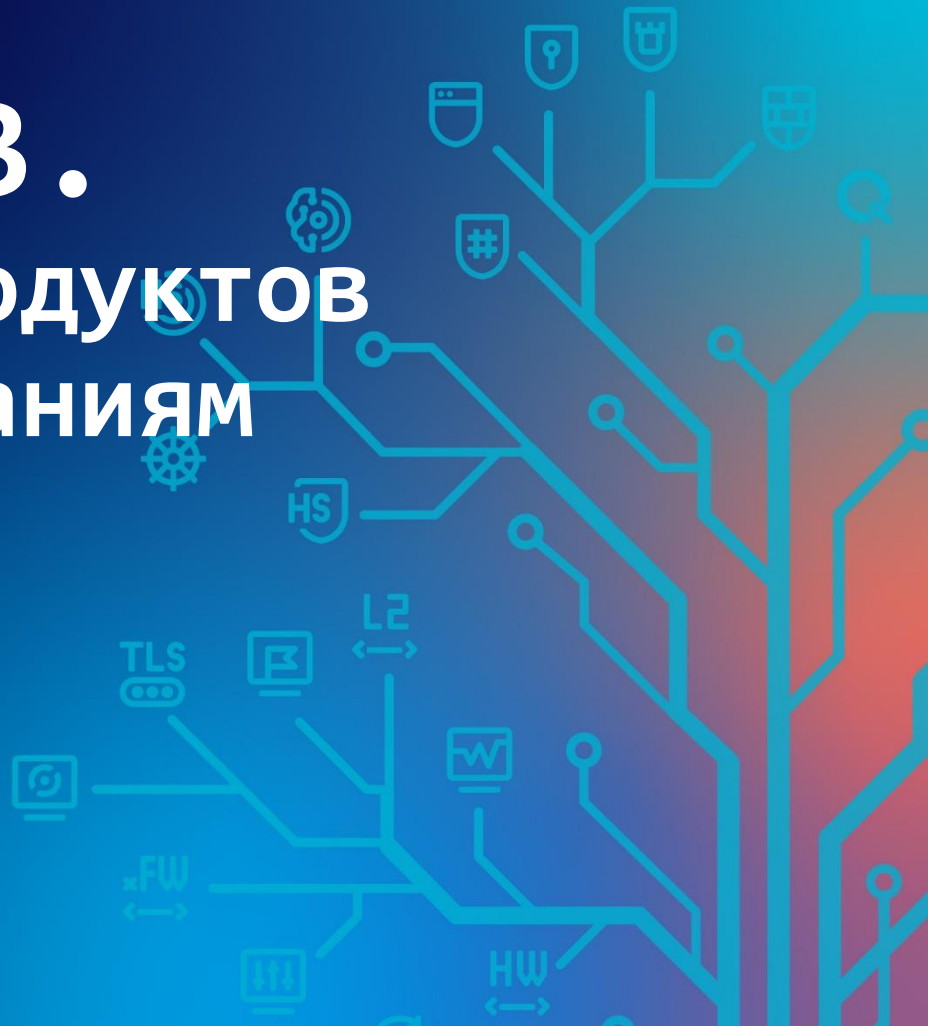
ViPNet IDS 3.
Новые версии продуктов по новым требованиям

Светлана Старовойт
Менеджер продуктов

infotecs



Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3

ViPNet IDS NS

ViPNet TIAS

ViPNet IDS MC

Обязательный компонент

Не обязательные компоненты

Система обнаружения вторжений уровня сети 4 класс

Требования доверия безопасности 4 уровня

Система обнаружения компьютерных атак класс В

Действующие сертификаты

Система обнаружения компьютерных атак класс В

Система обнаружения вторжений уровня сети 4 класс

Требования доверия безопасности 4 уровня

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, № РОСС RU.0003.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0656

Выдан "30" июня 2023 г. Действителен до "30" июня 2028 г.

Настоящий сертификат удостоверяет, что:

1. Средство защиты информации **«Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3»** (исполнения: ViPNet IDS NS100, ViPNet IDS NS1000, ViPNet IDS NS2000, ViPNet IDS NS10000, ViPNet IDS NS VA 100, ViPNet IDS NS VA 500, ViPNet IDS NS VA 1000, ViPNet IDS NS VA 2000, ViPNet IDS NS VA 5000 в комбинации со средством централизованного управления и мониторинга ViPNet IDS MC, средством анализа событий информационной безопасности ViPNet TIAS (исполнения: TIAS 1000, TIAS 2000, TIAS 5000, TIAS 10000, TIAS VA)), изготовленное в соответствии с техническими условиями ФРКЕ.00211-01 97 01 ТУ с учётом извещения об изменении № 6 ФРКЕ.00211.FB.6-2023,

соответствует требованиям ФСБ России к средствам обнаружения компьютерных атак класса В и может использоваться для обнаружения в автоматическом режиме компьютерных атак (вторжений) на основе анализа сетевого трафика в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, при условии выполнения требований эксплуатационной документации согласно формуляру ФРКЕ.00211-01 30 01 ФО с учётом извещения об изменении № 6 ФРКЕ.00211.FB.6-2023.

2. Сертификат соответствия выдан на основании экспертного заключения Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации № 149/2/1/2-1074А от 31 августа 2023 г.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4329

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 24 ноября 2020 г.

Выдан: 24 ноября 2020 г.
Действителен до: 24 ноября 2025 г.

Настоящий сертификат удостоверяет, что **система обнаружения компьютерных атак (вторжений) ViPNet IDS 3**, разработанная и производимая АО «ИнфоТеКС», является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Будет продлён

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4152

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 5 августа 2019 г.

Выдан: 5 августа 2019 г.
Действителен до: 5 августа 2024 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс ViPNet TIAS ФРКЕ.00167-02**, разработанный и производимый ОАО «ИнфоТеКС», является средством мониторинга событий безопасности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в руководящем документе «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля и техническим условиям ФРКЕ.00167-01 97 01 ТУ при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00167-01 30 01.

НЕ ДЕЙСТВИТЕЛЕН

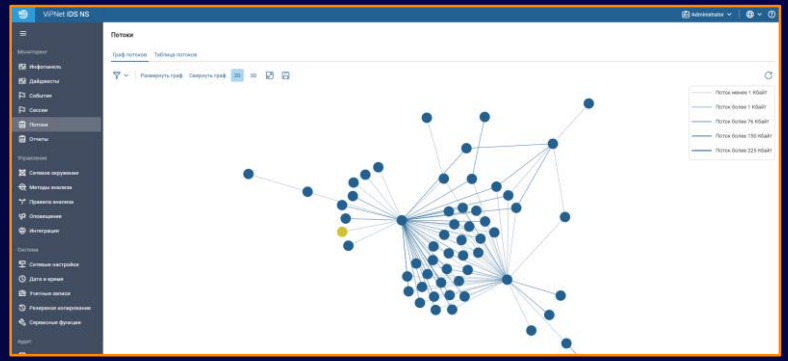
Сертифицированные версии

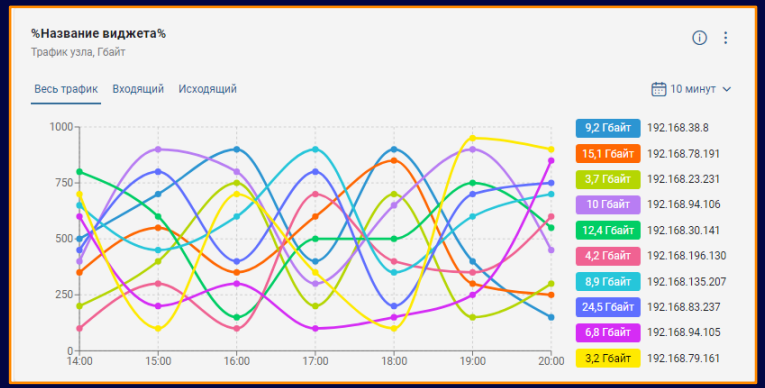
- ViPNet IDS NS 3.10
- ViPNet IDS MC 1.10
- ViPNet TIAS 3.10

Обновления:

- **ViPNet IDS NS:** 3.9.0 – 3.10.0
- **ViPNet IDS MC:** 1.9.0-1.10.0
- **ViPNet TIAS:** 3.10 – новая прошивка

ViPNet IDS NS 3.10





Математическая модель анализа трафика на узлах

анализ аномалий объема трафика с помощью нейросети

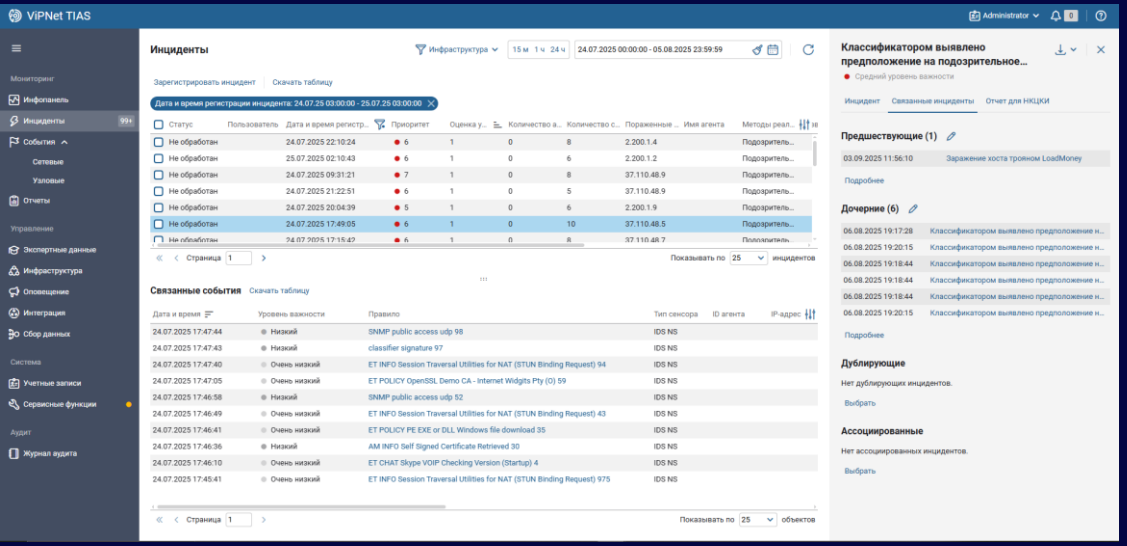
Информация о сетевых потоках

табличное и векторное представление

Запись образцов трафика

запись и передача в TIAS фрагментов сессии

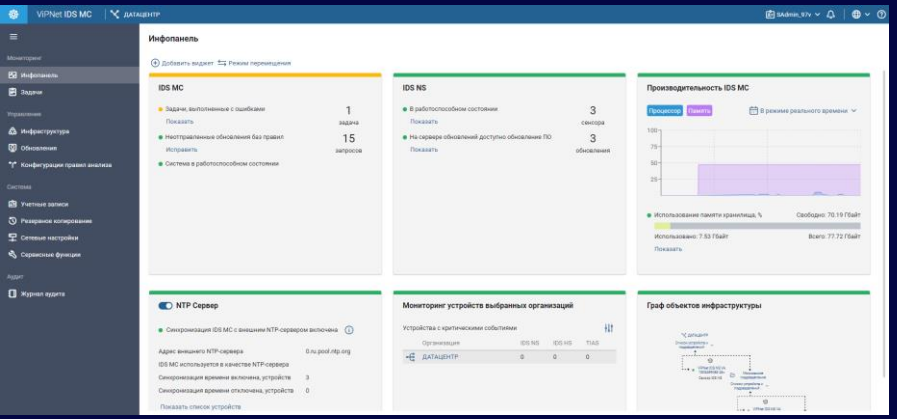
ViPNet TIAS 3.10

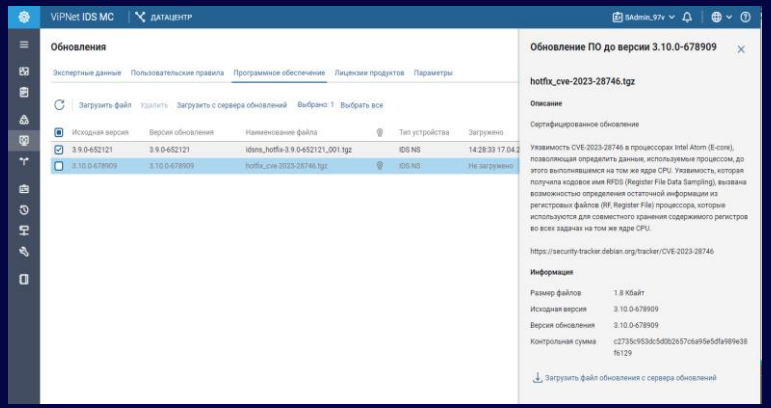


Новая модель машинного обучения
позволяет выявлять подозрительные цепочки событий связанные с работой вредоносного ПО

Создание инцидентов вручную
создать карточку инцидента на основе зарегистрированных событий

ViPNet IDS MC 1.10





Визуализация инфраструктуры
инфраструктура TDR в виде интерактивного графа

Расширенный мониторинг и настраиваемая инфопанель

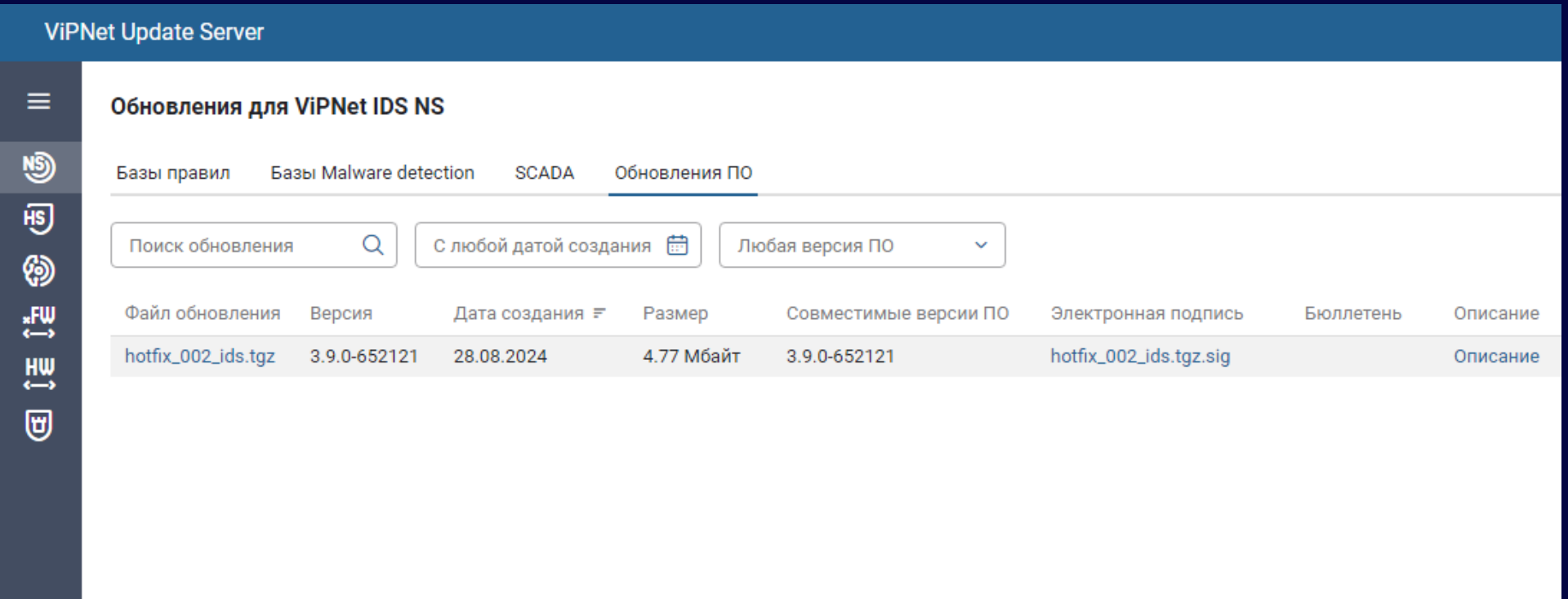
отследить потерю связи между сетевым сенсором IDS NS и TIAS

Получение патчей ПО с сервера обновлений

- получение уведомления
- проверка электронной подписи

Распространение патчей через сервер обновлений

infotecs



Распространение сертифицированных патчей через сервер обновлений

infotecs

Правила пользования для нового сертифицированного комплекта IDS 3:

Пакеты обновлений ПО публикуются на сервере обновлений изготовителя. Для обеспечения подлинности и целостности пакеты обновлений ПО подписываются открепленной ЭП. Также на сервере обновлений изготовителя для пакетов обновлений ПО публикуются бюллетени и краткое описание.

Уведомления о выпуске новых пакетов обновлений ПО на сервере обновлений можно настроить в ViPNet IDS MC.

Проверка подписи

Автоматическая проверка:
- средствами IDS MC

Проверка вручную:
- Любым средством проверки ЭП
- Рекомендуемый способ – ViPNet PKI Client

Приложение А.

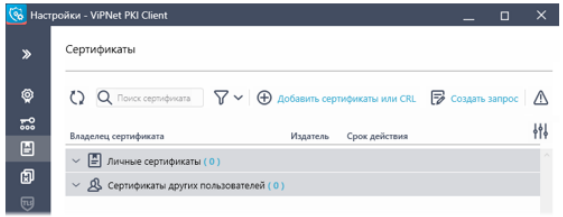
Инструкция по проверке ЭП пакета обновления ПО

Пакет обновления ПО представляет собой специальный архив. Для обеспечения подлинности и целостности архивы, распространяемые по сетям связи с помощью информационного ресурса изготовителя (сервер обновления), подписываются открепленной ЭП. Перед обновлением ПО необходимо проверить ЭП архива.

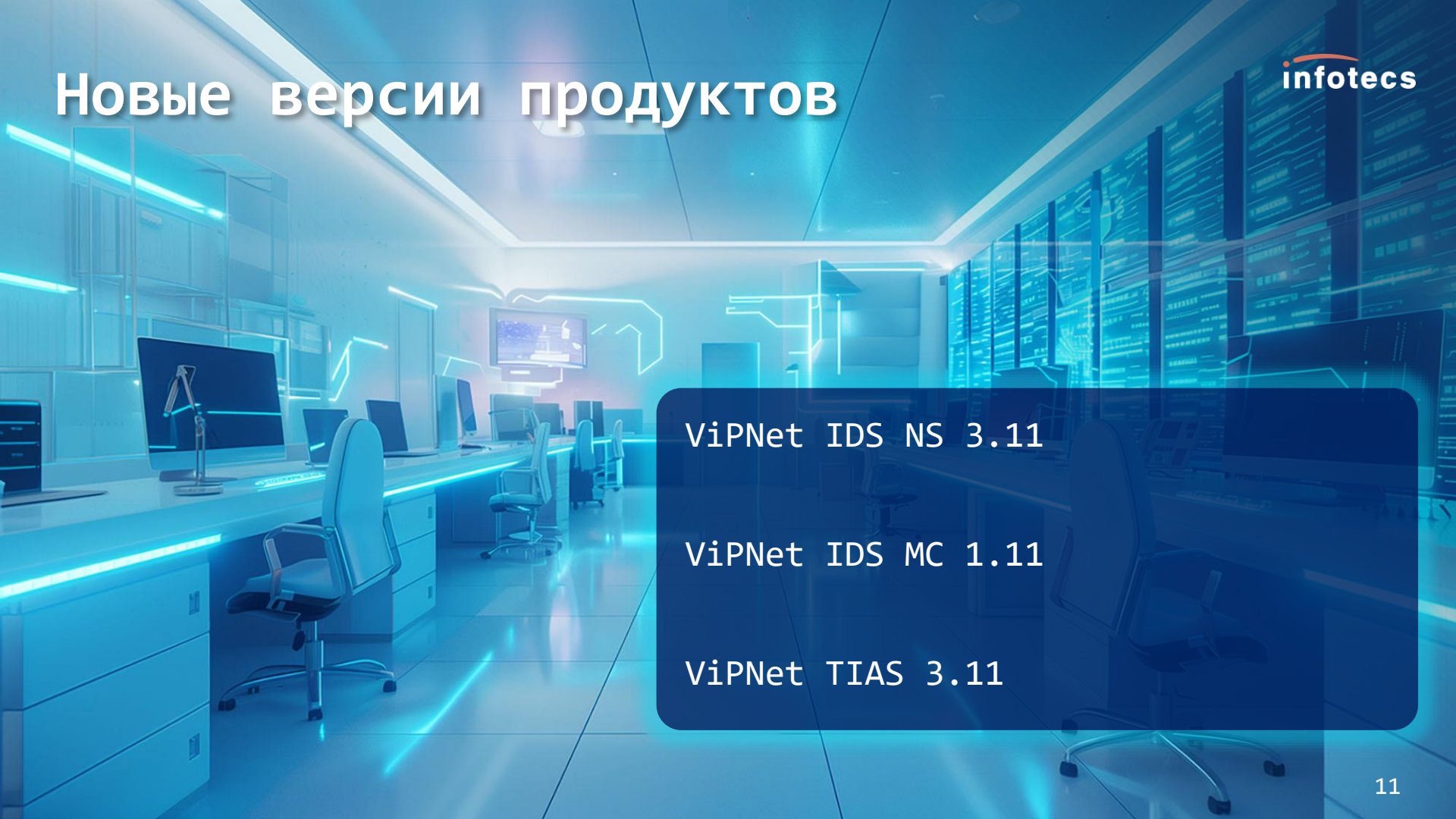
Проверка ЭП архива выполняется с помощью средства проверки ЭП, рекомендуется использовать ViPNet PKI Client. Скачать ViPNet PKI Client и документацию можно с сайта изготовителя https://infotecs.ru. Вместе с установочным файлом будет предоставлена демо-лицензия на 6 месяцев.

Порядок проверки ЭП пакета обновления ПО:

1. Запустить ViPNet PKI Client: в меню «Пуск» выбрать «ViPNet > ViPNet PKI Client».
2. На панели навигации перейти в раздел «Сертификаты» (см. рисунок 1) и выполнить одно из действий:
   - перетащить файл корневого сертификата центра сертификации АО «ИнфоТеКС» и файл со списком отозванных сертификатов (CRL) на панель просмотра;
   - нажать ⊕ «Добавить сертификат или CRL» и указать путь к файлу корневого сертификата центра сертификации АО «ИнфоТеКС» и файлу со списком отозванных сертификатов (CRL).



Новые версии продуктов



ViPNet IDS NS 3.11

ViPNet IDS MC 1.11

ViPNet TIAS 3.11

ViPNet IDS NS 3.11

Реализация новых требований

Версия соответствует требованиям ФСБ к СОА класса В

Ретроспективный анализ

Поиск новых IoC в сохраненных данных о потоках взаимодействия

Обновлена ролевая модель

- Добавлена новая роль Администратор системы
- Изменены названия других ролей

Доработаны функции безопасности

- блокировка учетных записей
- Уведомление о необходимости смены пароля
- Список доверенных адресов для подключения
- Настройка хранения записей журнала аудита

Новые фичи

Проверка IoC
Проверка наличия хэш-сумм вредоносного ПО в базе системных правил

Просмотр PCAP-файлов
просматривать детальную информацию о сетевом пакете из карточки события и карточки сессии

Выбор активных профилей правил при установке и обновлении базы правил

Использование алгоритма SSDeep в Malware detection

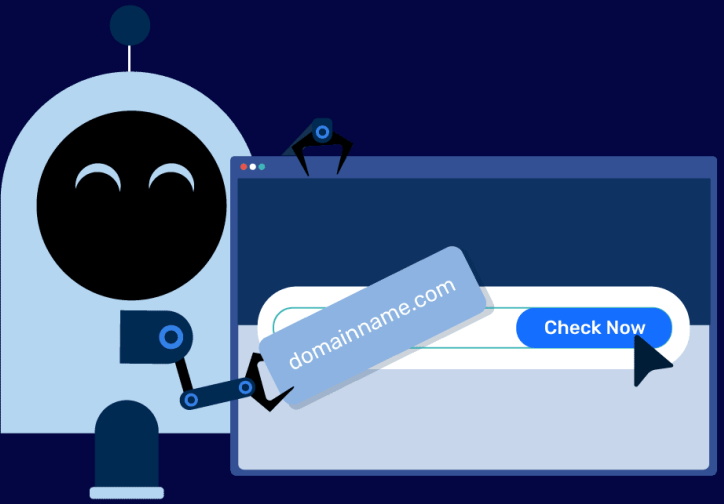
База GeoIP от Минцифры
в состав базы правил входит база геопозиционных данных от Минцифры России

Сброс настроек из консольного конфигуратора
сбросить до заводских настроек для восстановления работоспособности ПАК

infotecs

Новые модели машинного обучения

Обнаружение сгенерированных доменных имен



- Нейронная сеть
- Работает на данных о потоках
- Обучается на размеченном наборе данных + справочник доверенных доменных имён
- 46 миллионов доменов в сутки

Обнаружение фишинговых доменных имен

- Анализ DNS-запросов
- Обучение на списке доверенных и фишинговых имён
- Исключения на основании пользовательского белого списка
- Определение процента схожести

Обнаружение вредоносного ПО в TLS-трафике

- База известных хэш-сумм JA3 входит в состав базы правил
- Метод поддерживает протоколы следующих версий:
  - TLS — 1.0-1.3.
  - SSL — 3.0.

Обнаружение вредоносного ПО в TLS-трафике

- База известных хэш-сумм JA3 входит в состав базы правил
- Метод поддерживает протоколы следующих версий:
  - TLS — 1.0-1.3.
  - SSL — 3.0.

ViPNet TIAS 3.11

Реализация новых требований

Версия соответствует требованиям ФСБ к СОА класса Г (событийные СОА)

Ретроспективный анализ

Поиск инцидентов в сохраненных событиях по новым экспертным данным

Обновлена ролевая модель

- Добавлена новая роль Администратор системы
- Изменены названия других ролей

Доработаны функции безопасности

- блокировка учетных записей
- Уведомление о необходимости смены пароля
- Список доверенных адресов для подключения
- Настройка хранения записей журнала аудита
- Создание регулярных отчётов

Новые фичи

infotecs

Разные форматы правил

- Узловые правила для Linux/Windiws
- Сетевые правила Suricata

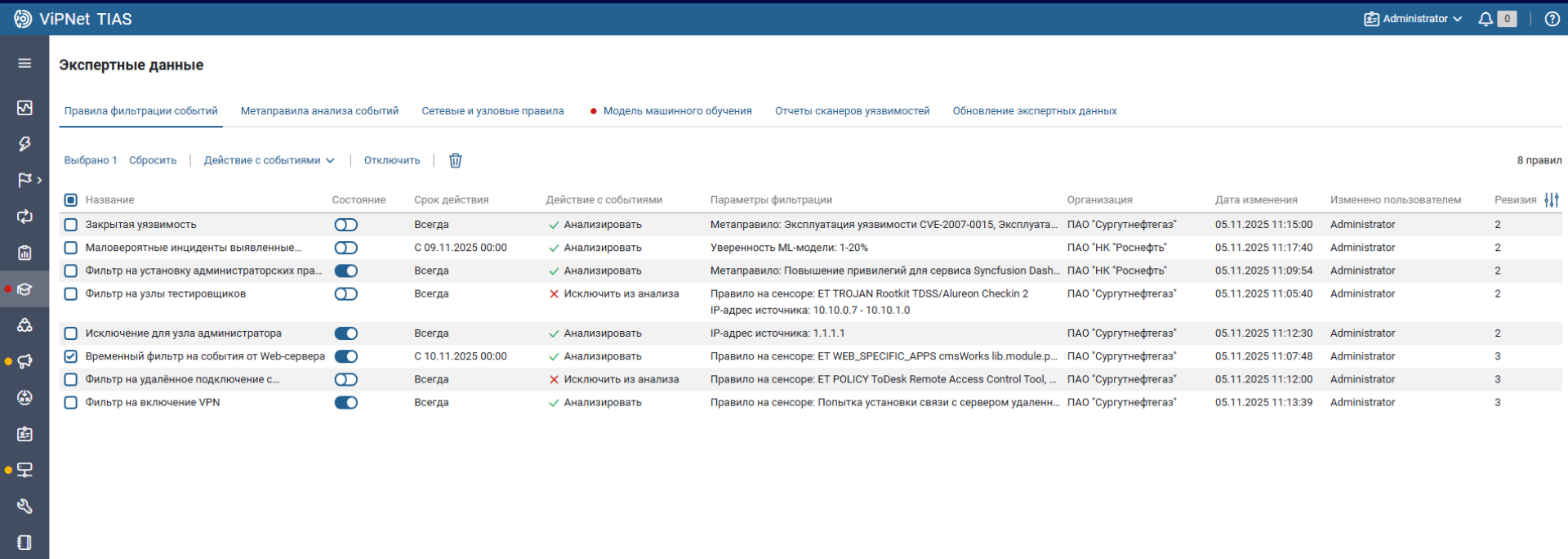
Анализ событий от моделей IDS NS

- Отдельный тип правил для ML-событий
- Добавление ML-событий в последовательности и наборы событий

Автоматическое получение пользовательских правил из IDS MC

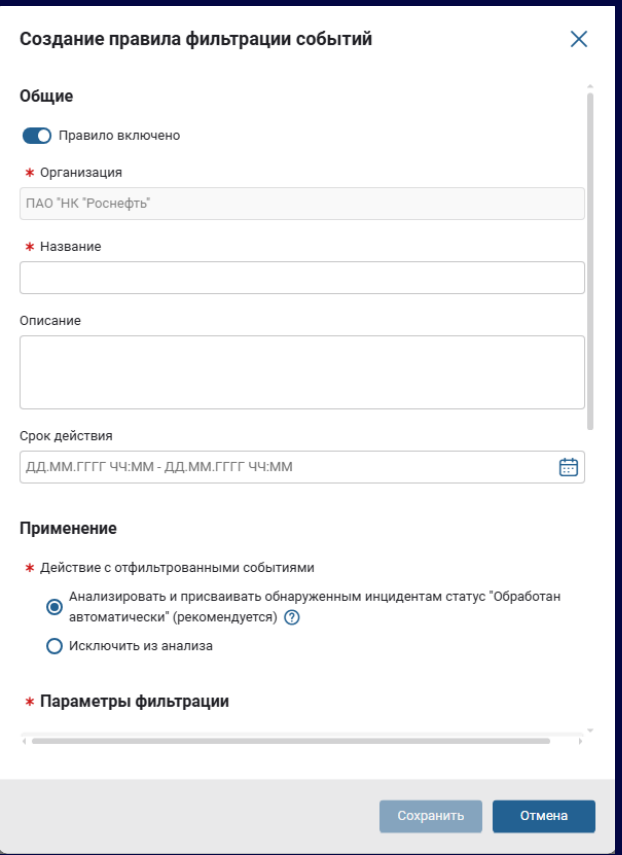
База GeoIP от Минцифры

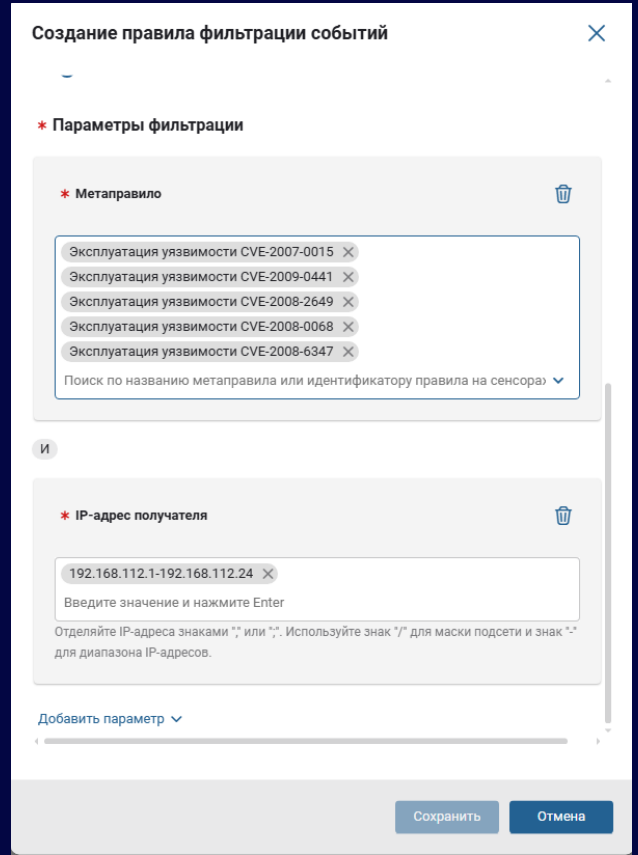
Фильтрация событий в модуле анализа

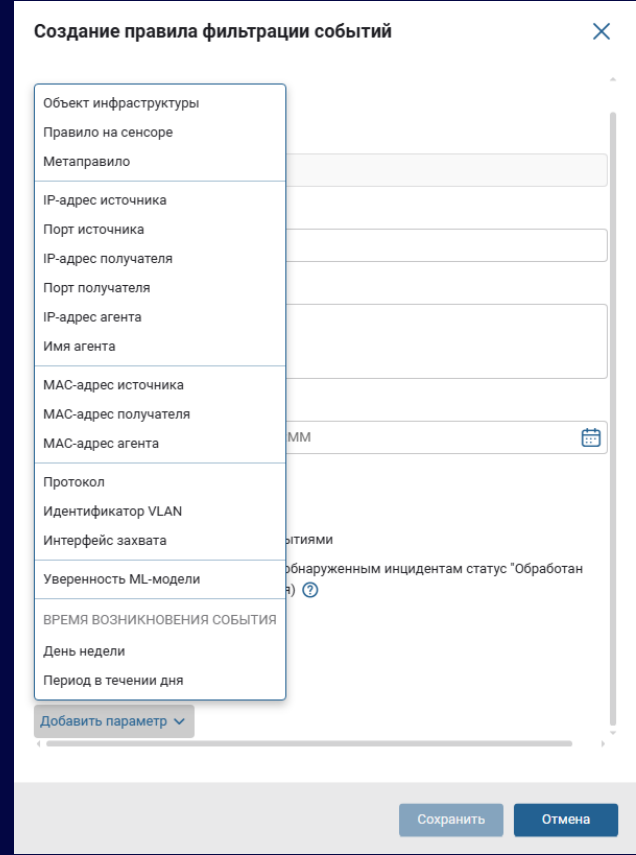


Гибкая настройка фильтров

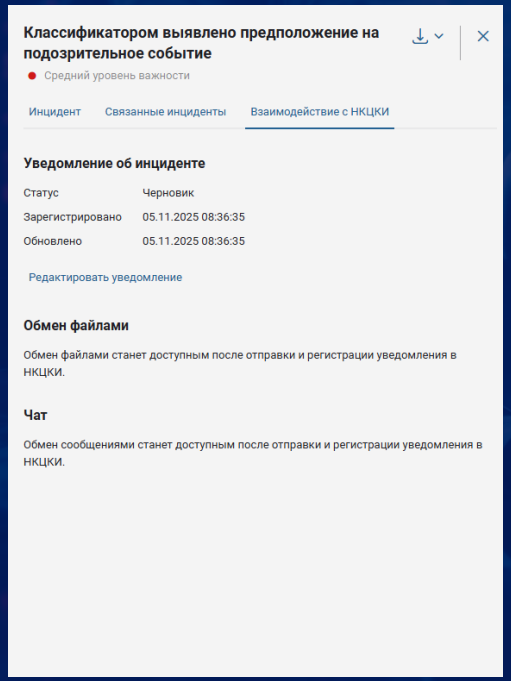
infotecs







Взаимодействие с НКЦКИ



- Взаимодействие с личным кабинетом НКЦКИ по API
- Получение подтверждения и идентификатора зарегистрированного уведомления об инциденте
- Обмен сообщениями
- Передача дополнительных файлов

ViPNet IDS MC 1.11

Новые фичи

Шаблоны настроек IDS NS

Создание и применение шаблонов с настройками сенсоров

Повышение информативности уведомлений

- агрегация однотипных
- пользовательские настройки

Управление методами анализа на сенсорах

- индивидуальная настройка
- групповая (через шаблон)

Управление конфигурациями

- создать конфигурацию с нуля
- на основе ранее созданной конфигурации.
- на основе результирующей конфигурации.
- на основе локальной конфигурации сенсора

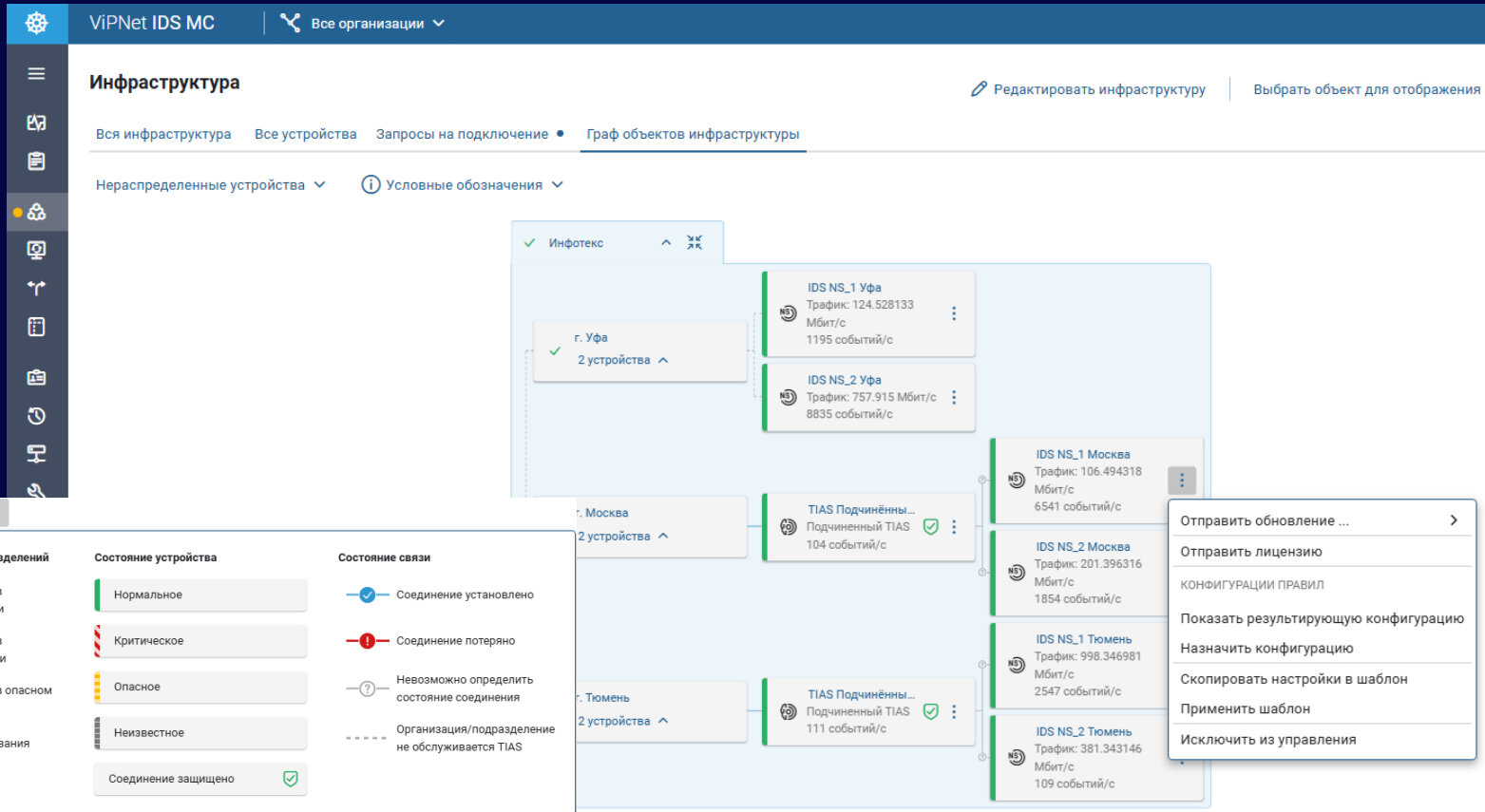
Синхронизация правил

автоматическая синхронизация пользовательских правил между IDS NS 3.11, IDS MC 1.11 и TIAS 3.11

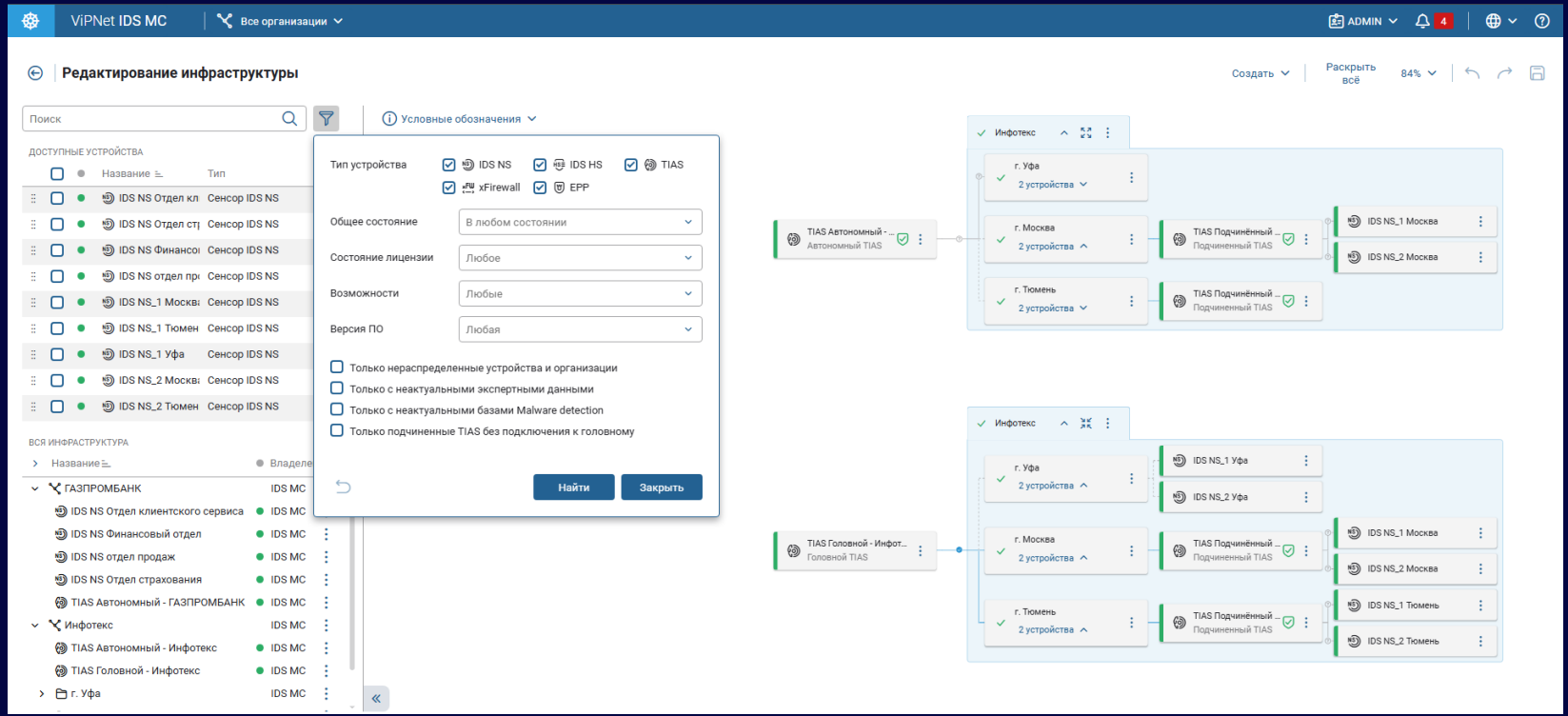
Управление конфигурациями правил модуля IPS HW 5

* Через интеграцию с Prime

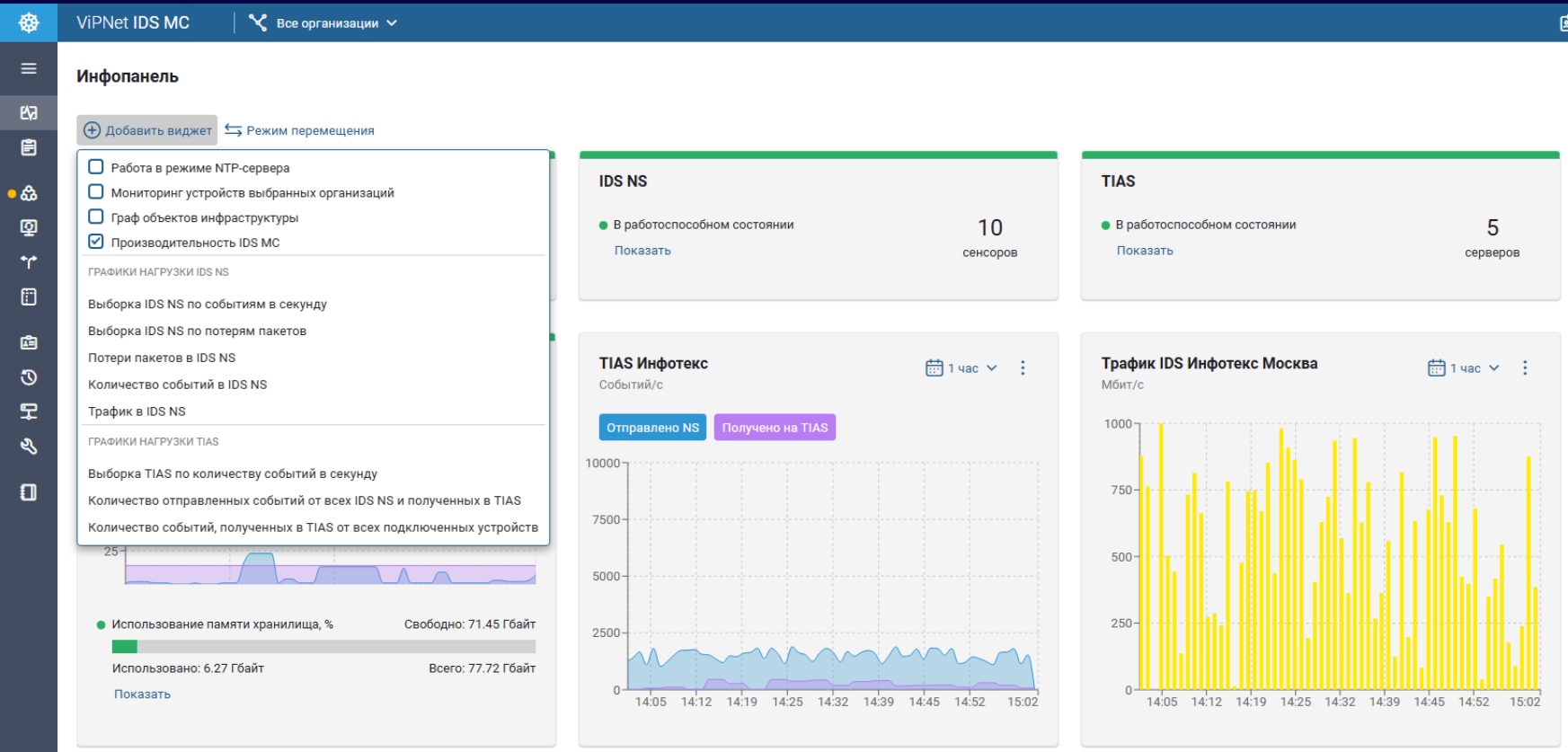
Граф объектов инфраструктуры



Редактирование инфраструктуры



Новые виджеты



«Будущее уже наступило. Просто оно ещё неравномерно распределено

Уильям Гибсон

ВОПРОСЫ

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Спасибо за внимание!