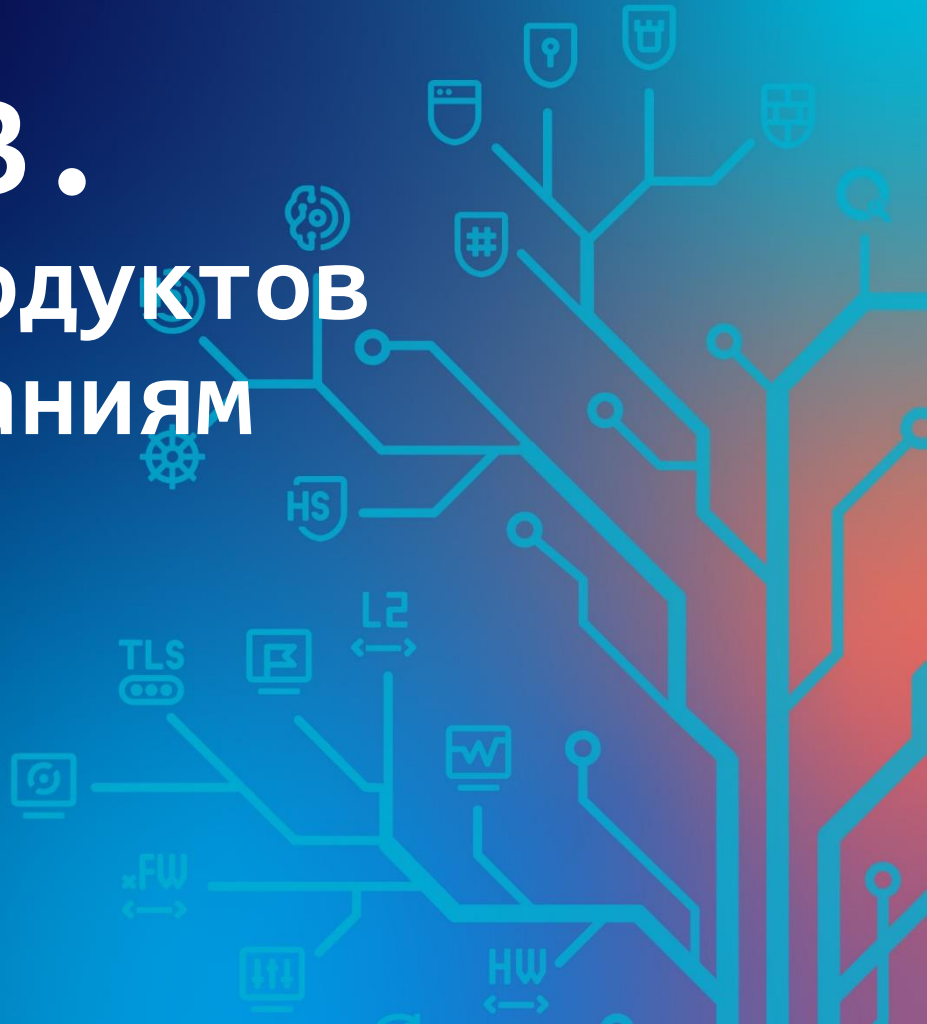


Новые версии продуктов по новым требованиям



Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3



ViPNet IDS NS

Обязательный
компонент



ViPNet TIAS

Не обязательные компоненты



ViPNet IDS MC



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.0003.01B100

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 NS1000, ViPNet IDS NS10000, ViPNet IDS NS100000, 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 учетом изъятия об изъятии № 6 ФРКЕ.00211.FB.6.2023,

соответствует требованиям ФСБ России к средствам обнаружения компьютерных атак класса В и может использоваться для обнаружения и автоматического реагирования на 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 учетом изъятия об изъятии № 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 № 149/2/12-1074А от 31 августа 2023 г.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01B100

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).

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01B100

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» (Постехомиссия России, 1999) - по 4 уровню контроля и техническим условиям ФРКЕ.00167-01 97 01 ТУ при выполнении указанных по эксплуатации, приведенных в формуляре ФРКЕ.00167-01 30 01.

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

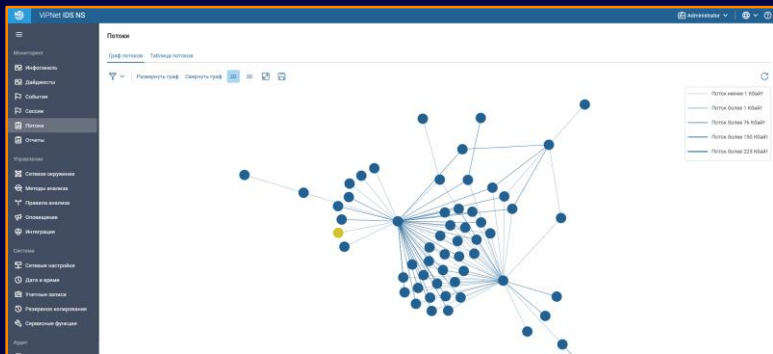


ViPNet IDS MC: 1.9.0-1.10.0



ViPNet TIAS: 3.10 – новая прошивка

VIPNet IDS NS 3.10

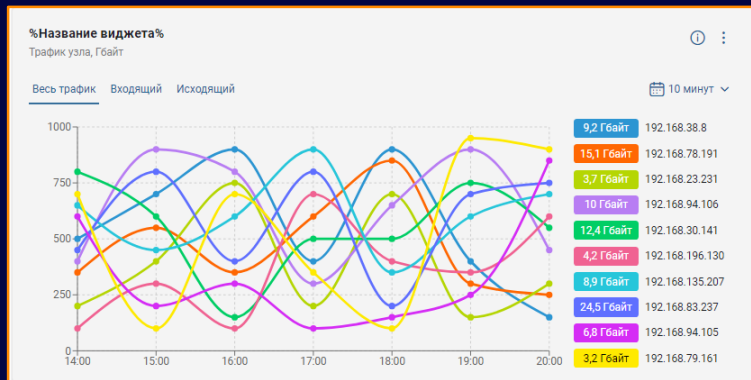


Математическая модель анализа трафика на узлах

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

The screenshot displays the VIPNet TIAS 3.10 web interface. The left sidebar contains navigation links: Мониторинг, Инциденты (highlighted), События, Соповые, Угрозы, Отчеты, Управление, Экспертные данные, Инфраструктура, Оценки, Интеракция, Стор данных, Системы, Учетные записи, Сервисные функции, Аудит, and Журнал аудита. The main content area is divided into two sections. The top section, 'Инциденты', shows a table of incidents with columns for status, user, registration date, priority, score, and quantity. The bottom section, 'Связанные события', shows a table of related events with columns for date, severity, rule, type, agent ID, and IP address. The right sidebar contains a 'Классификатором выявлено предположение на подозрительное...' section, a 'Предшественствующие (1)' section, a 'Дочерние (6)' section, and a 'Дублирующие' section.

Инциденты

Статус	Пользователь	Дата и время регистрац...	Приоритет	Оценка у...	Количество в...	Количество с...	Пораженные	Имя агента	Методы реаг...
☐ Не обработан		24.07.2025 22:10:24	6	1	0	8	2.200.1.4		Подозритель...
☐ Не обработан		25.07.2025 02:10:43	6	1	0	6	2.200.1.2		Подозритель...
☐ Не обработан		24.07.2025 09:31:21	7	1	0	8	37.110.48.9		Подозритель...
☐ Не обработан		24.07.2025 21:22:51	6	1	0	5	37.110.48.9		Подозритель...
☐ Не обработан		24.07.2025 20:04:39	5	1	0	6	2.200.1.9		Подозритель...
☐ Не обработан		24.07.2025 17:49:05	6	1	0	10	37.110.48.5		Подозритель...
☐ Не обработан		24.07.2025 17:15:47	6	1	0	8	37.110.48.7		Подозритель...

Связанные события

Дата и время	Уровень важности	Правило	Тип сенсора	ID агента	IP-адрес
24.07.2025 17:47:44	Низкий	SNMP public access udp 98	IDS NS		
24.07.2025 17:47:43	Низкий	classifier signature 97	IDS NS		
24.07.2025 17:47:40	Очень низкий	ET INFO Session Traversal Utilities for NAT (STUN Binding Request) 94	IDS NS		
24.07.2025 17:47:05	Очень низкий	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (C) 59	IDS NS		
24.07.2025 17:46:58	Низкий	SNMP public access udp 52	IDS NS		
24.07.2025 17:46:49	Очень низкий	ET INFO Session Traversal Utilities for NAT (STUN Binding Request) 43	IDS NS		
24.07.2025 17:46:41	Очень низкий	ET INFO Self Signed Certificate Retrieved 35	IDS NS		
24.07.2025 17:46:36	Низкий	AM INFO Self Signed Certificate Retrieved 30	IDS NS		
24.07.2025 17:46:10	Очень низкий	ET CHAT Skype VOIP Checking Version (Startup) 4	IDS NS		
24.07.2025 17:45:41	Очень низкий	ET INFO Session Traversal Utilities for NAT (STUN Binding Request) 975	IDS NS		

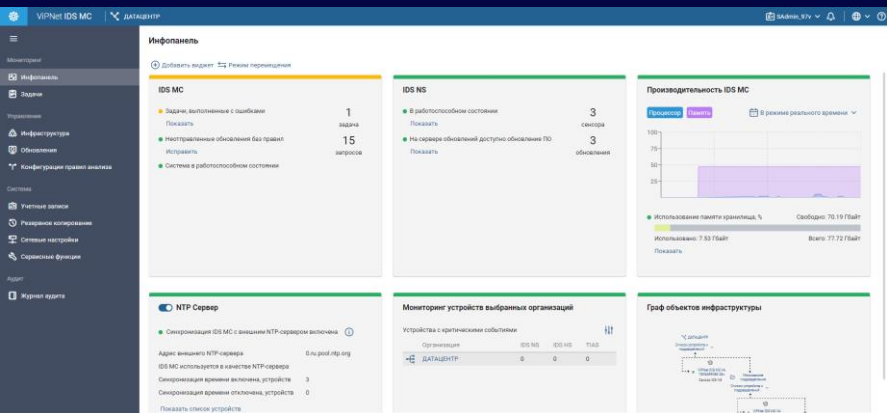
Новая модель машинного обучения

позволяет выявлять подозрительные цепочки событий связанные с работой вредоносного ПО

Создание инцидентов вручную

создать карточку инцидента на основе зарегистрированных событий

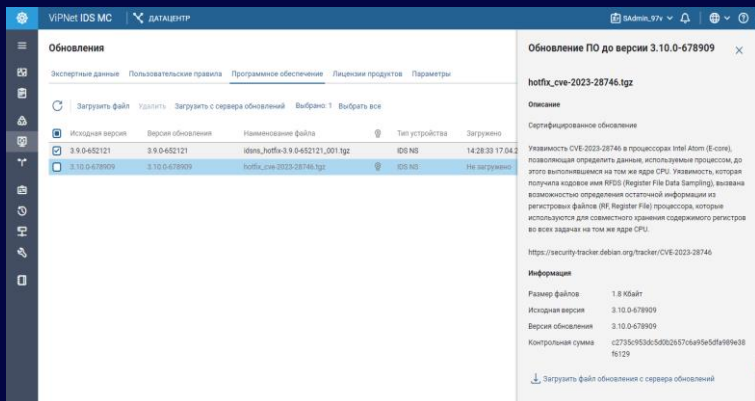
ViPNet IDS MC 1.10



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

ViPNet Update Server



Обновления для ViPNet IDS NS

Базы правил

Базы Malware detection

SCADA

Обновления ПО

Поиск обновления



С любой датой создания



Любая версия ПО



Файл обновления	Версия	Дата создания	Размер	Совместимые версии ПО	Электронная подпись	Бюллетень	Описание
hotfix_002_ids.tgz	3.9.0-652121	28.08.2024	4.77 Мбайт	3.9.0-652121	hotfix_002_ids.tgz.sig		Описание

Распространение сертифицированных патчей через сервер обновлений

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.

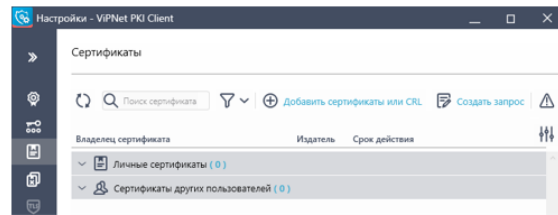
Инструкция по проверке ЭП пакета обновления ПО

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

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 SSDeer в Malware detection



База GeoIP от Минцифры

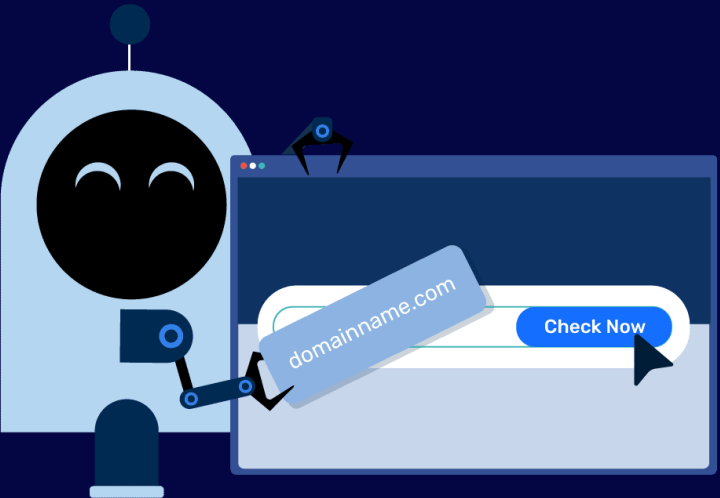
в состав базы правил входит база геопозиционных данных от Минцифры России



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

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.

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



Разные форматы правил

- Узловые правила для Linux/Windows
- 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

Экспертные данные

Правила фильтрации событий | Метаконфигурация анализа событий | Сетевые и узловые правила | Модель машинного обучения | Отчеты сканеров уязвимостей | Обновление экспертных данных

Выбрано 1 | Сбросить | Действие с событиями | Отключить |

8 правил

☐	Название	Состояние	Срок действия	Действие с событиями	Параметры фильтрации	Организация	Дата изменения	Изменено пользователем	Ревизия
☐	Закрытая уязвимость	☐	Всегда	✓ Анализировать	Метаконфигурация: Эксплуатация уязвимости CVE-2007-0015, Эксплуата...	ПАО "Сургутнефтегаз"	05.11.2025 11:15:00	Administrator	2
☐	Маловероятные инциденты выявленные...	☐	С 09.11.2025 00:00	✓ Анализировать	Уверенность ML-модели: 1-20%	ПАО "НК "Роснефть"	05.11.2025 11:17:40	Administrator	2
☐	Фильтр на установку администраторских пра...	☐	Всегда	✓ Анализировать	Метаконфигурация: Повышение привилегий для сервиса Syncfusion Dash...	ПАО "НК "Роснефть"	05.11.2025 11:09:54	Administrator	2
☐	Фильтр на узлы тестировщиков	☐	Всегда	✗ Исключить из анализа	Правило на сенсоре: ET TROJAN Rootkit TDSS/Alureon Checkin 2 IP-адрес источника: 10.10.0.7 - 10.10.1.0	ПАО "Сургутнефтегаз"	05.11.2025 11:05:40	Administrator	2
☐	Исключение для узла администратора	☐	Всегда	✓ Анализировать	IP-адрес источника: 1.1.1.1	ПАО "Сургутнефтегаз"	05.11.2025 11:12:30	Administrator	2
☒	Временный фильтр на события от Web-сервера	☐	С 10.11.2025 00:00	✓ Анализировать	Правило на сенсоре: ET WEB_SPECIFIC_APPS cmsWorks lib.module.p...	ПАО "Сургутнефтегаз"	05.11.2025 11:07:48	Administrator	3
☐	Фильтр на удалённое подключение с...	☐	Всегда	✗ Исключить из анализа	Правило на сенсоре: ET POLICY ToDesk Remote Access Control Tool, ...	ПАО "Сургутнефтегаз"	05.11.2025 11:12:00	Administrator	3
☐	Фильтр на включение VPN	☐	Всегда	✓ Анализировать	Правило на сенсоре: Попытка установки связи с сервером удаленн...	ПАО "Сургутнефтегаз"	05.11.2025 11:13:39	Administrator	3

Гибкая настройка фильтров

Создание правила фильтрации событий

Общие

☒ Правило включено

* Организация

ПАО "НК "Роснефть"

* Название

Описание

Срок действия

ДД.ММ.ГГГГ ЧЧ:ММ - ДД.ММ.ГГГГ ЧЧ:ММ

Применение

* Действие с отфильтрованными событиями

- ☒ Анализировать и присваивать обнаруженным инцидентам статус "Обработан автоматически" (рекомендуется) ?
- ☐ Исключить из анализа

* Параметры фильтрации

Сохранить

Отмена

Создание правила фильтрации событий

* Параметры фильтрации

* Метаправило

Эксплуатация уязвимости CVE-2007-0015 X

Эксплуатация уязвимости CVE-2009-0441 X

Эксплуатация уязвимости CVE-2008-2649 X

Эксплуатация уязвимости CVE-2008-0068 X

Эксплуатация уязвимости CVE-2008-6347 X

Поиск по названию метаправила или идентификатору правила на сенсоре ▾

И

* IP-адрес получателя

192.168.112.1-192.168.112.24 X

Введите значение и нажмите Enter

Отделяйте IP-адреса знаками ";" или ":", используйте знак "/" для маски подсети и знак "*" для диапазона IP-адресов.

Добавить параметр ▾

Сохранить

Отмена

Создание правила фильтрации событий

Объект инфраструктуры

Правило на сенсоре

Метаправило

IP-адрес источника

Порт источника

IP-адрес получателя

Порт получателя

IP-адрес агента

Имя агента

MAC-адрес источника

MAC-адрес получателя

MAC-адрес агента

Протокол

Идентификатор VLAN

Интерфейс захвата

Уверенность ML-модели

ВРЕМЯ ВОЗНИКНОВЕНИЯ СОБЫТИЯ

День недели

Период в течении дня

Добавить параметр ▾

Сохранить

Отмена

Взаимодействие с НКЦКИ

Классификатором выявлено предположение на подозрительное событие

● Средний уровень важности

Инцидент Связанные инциденты Взаимодействие с НКЦКИ

Уведомление об инциденте

Статус	Черновик
Зарегистрировано	05.11.2025 08:36:35
Обновлено	05.11.2025 08:36:35

[Редактировать уведомление](#)

Обмен файлами

Обмен файлами станет доступным после отправки и регистрации уведомления в НКЦКИ.

Чат

Обмен сообщениями станет доступным после отправки и регистрации уведомления в НКЦКИ.

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

Новые фичи



Шаблоны настроек IDS NS

Создание и применение шаблонов с настройками сенсоров



Управление методами анализа на сенсорах

- индивидуальная настройка
- групповая (через шаблон)



Синхронизация правил

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



Повышение информативности уведомлений

- агрегация однотипных
- пользовательские настройки



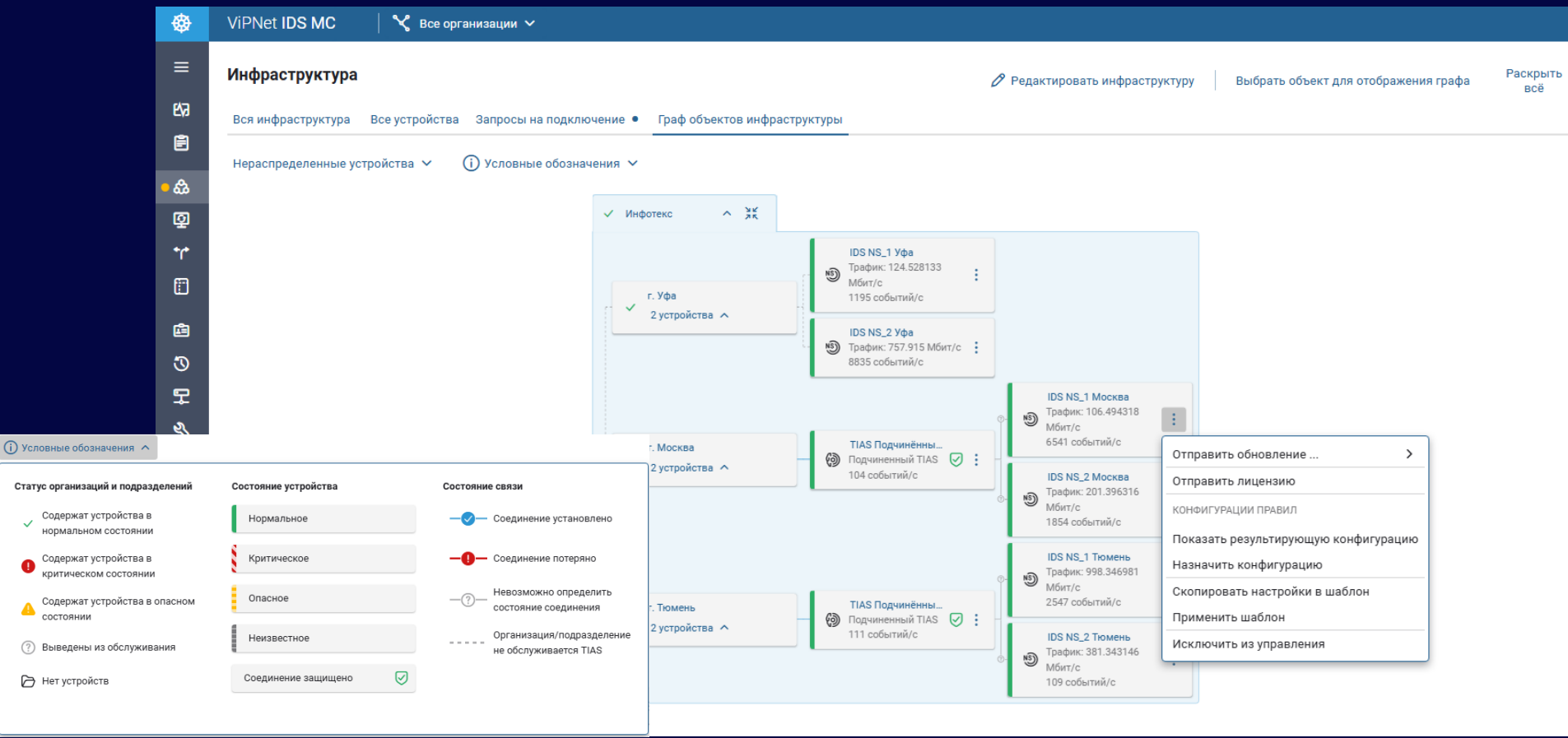
Управление конфигурациями

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



Управление конфигурациями правил модуля IPS HW 5

* Через интеграцию с Prime



Редактирование инфраструктуры

ВипNet IDS MC | Все организации

ADMIN | 4 | 84%

Редактирование инфраструктуры

Поиск

Условные обозначения

Доступные устройства

Название	Тип
IDS NS Отдел кл	Сенсор IDS NS
IDS NS Отдел ст	Сенсор IDS NS
IDS NS Финансо	Сенсор IDS NS
IDS NS отдел пр	Сенсор IDS NS
IDS NS_1 Москв	Сенсор IDS NS
IDS NS_1 Тюмен	Сенсор IDS NS
IDS NS_1 Уфа	Сенсор IDS NS
IDS NS_2 Москв	Сенсор IDS NS
IDS NS_2 Тюмен	Сенсор IDS NS

Вся инфраструктура

Название	Владелец
ГАЗПРОМБАНК	IDS MC
IDS NS Отдел клиентского сервиса	IDS MC
IDS NS Финансовый отдел	IDS MC
IDS NS отдел продаж	IDS MC
IDS NS Отдел страхования	IDS MC
ТИАС Автономный - ГАЗПРОМБАНК	IDS MC
Инфотекс	IDS MC
ТИАС Автономный - Инфотекс	IDS MC
ТИАС Головной - Инфотекс	IDS MC
г. Уфа	IDS MC

Тип устройства

- ☒ IDS NS
- ☒ IDS HS
- ☒ TIAS
- ☒ xFirewall
- ☒ EPP

Общее состояние

В любом состоянии

Состояние лицензии

Любое

Возможности

Любые

Версия ПО

Любая

☐ Только нераспределенные устройства и организации

☐ Только с неактуальными экспертными данными

☐ Только с неактуальными базами Malware detection

☐ Только подчиненные TIAS без подключения к головному

Найти

Закрыть

Инфотекс

- г. Уфа
- г. Москва
- г. Тюмень

ТИАС Автономный - Инфотекс

ТИАС Подчиненный - Инфотекс

IDS NS_1 Москва

IDS NS_2 Москва

ТИАС Подчиненный - Инфотекс

ТИАС Подчиненный - Инфотекс

ТИАС Головной - Инфотекс

IDS NS_1 Уфа

IDS NS_2 Уфа

IDS NS_1 Тюмень

IDS NS_2 Тюмень

Новые виджеты

Инфопанель

Добавить виджет Режим перемещения

- ☐ Работа в режиме NTP-сервера
- ☐ Мониторинг устройств выбранных организаций
- ☐ Граф объектов инфраструктуры
- ☒ Производительность IDS MC

ГРАФИКИ НАГРУЗКИ IDS NS

Выборка IDS NS по событиям в секунду

Выборка IDS NS по потерям пакетов

Потери пакетов в IDS NS

Количество событий в IDS NS

Трафик в IDS NS

ГРАФИКИ НАГРУЗКИ TIAS

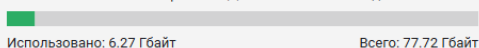
Выборка TIAS по количеству событий в секунду

Количество отправленных событий от всех IDS NS и полученных в TIAS

Количество событий, полученных в TIAS от всех подключенных устройств



Использование памяти хранилища, % Свободно: 71.45 Гбайт



Показать

IDS NS

В работоспособном состоянии

10

сенсоров

Показать

TIAS

В работоспособном состоянии

5

серверов

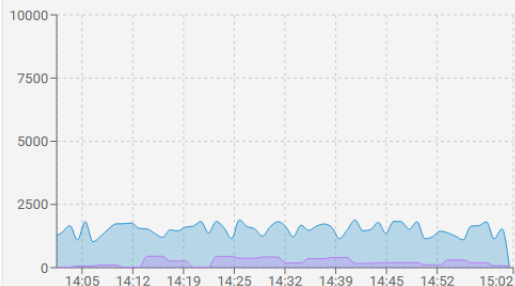
Показать

TIAS Инфотекс

Событий/с

1 час

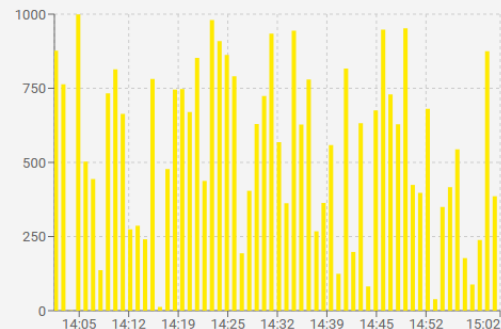
Отправлено NS Получено на TIAS



Трафик IDS Инфотекс Москва

Мбит/с

1 час



”

«Будущее уже наступило.
Просто оно ещё
неравномерно распределено

Уильям Гибсон

ВОПРОСЫ

Подписывайтесь
на наши соцсети,
там много интересного



infotecs

Спасибо за внимание!