ViPNet TIAS 3.6
Новые возможности

Светлана Старовойт

О чем этот вебинар?

Новое в версии ViPNet TIAS 3.6

- Иерархическая схема построения TIAS
- Мультиарендный режим доступа в TIAS
- Новые алгоритмы выявления инцидентов
- Гарантированная доставка событий по защищенному каналу

и другие возможности

Что такое ViPNet TIAS?

infotecs

ViPNet IDS NS

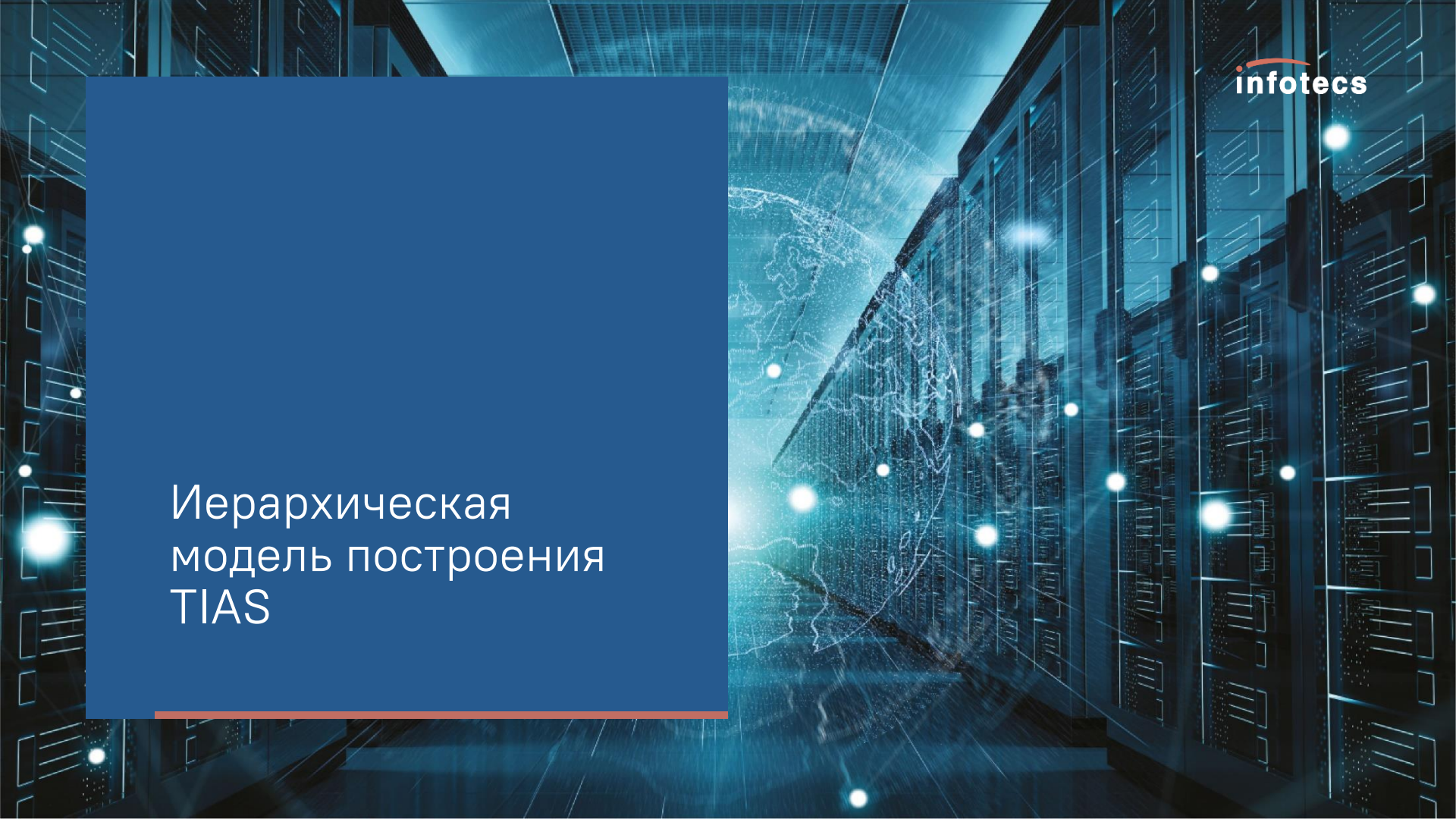
ViPNet IDS HS

События ИБ

TI Feeds

ViPNet TIAS

Инциденты ИБ



Иерархическая модель построения TIAS

Кому и зачем это нужно?

Режим подчиненного TIAS

infotecs

Весь функционал TIAS Standalone

\+ передача в головной TIAS:

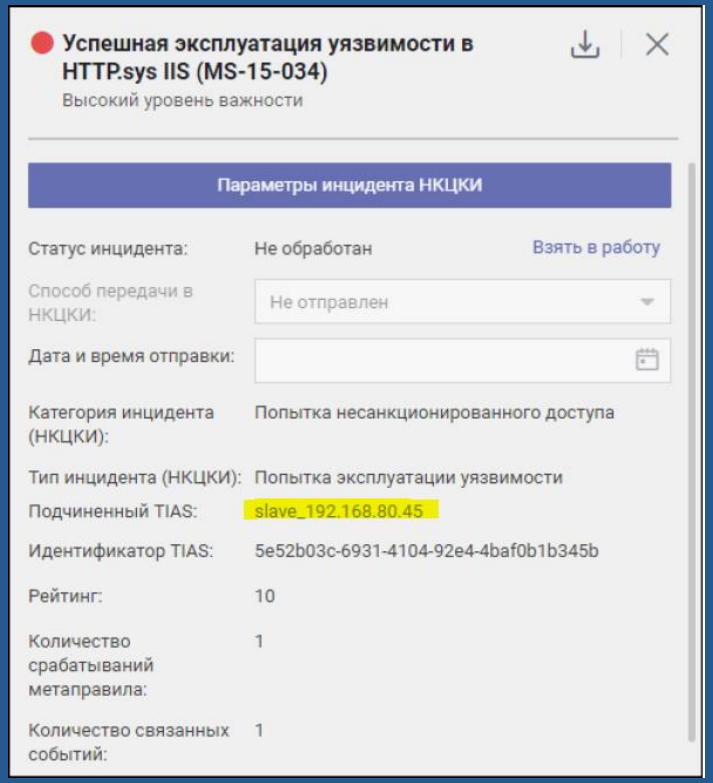
- инцидентов и связанных событий
- агрегированной информации о событиях для инфопанели

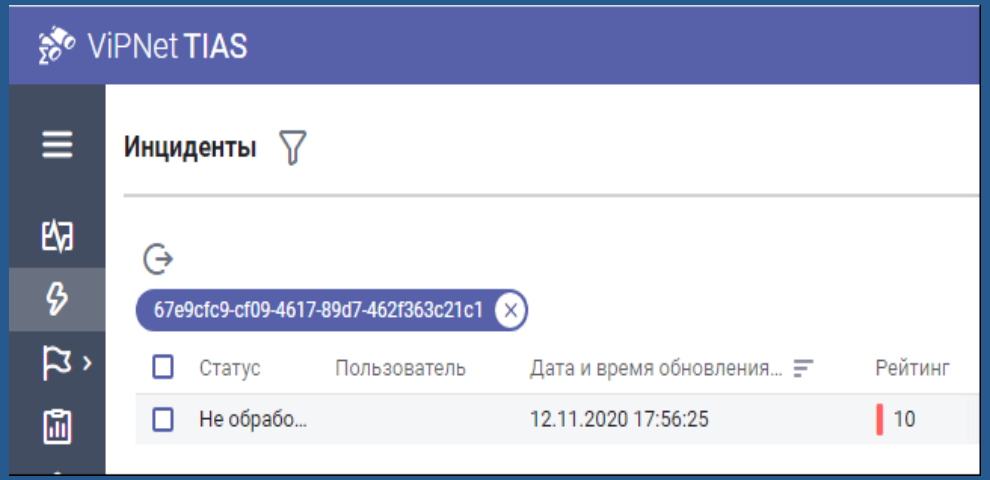
- ✓ Не требует специфической лицензии
- ✓ Режим работы и головной TIAS задается в IDS MC
- ✓ На любом варианте исполнения TIAS

Режим головного TIAS

- Сбор и хранение информации обо всех инцидентах
- Работа с инцидентами и связанными событиями
- Передача инцидентов в НКЦКИ (настраивается для каждой организации)
- Отображение онлайн дэшбордов по событиям
- Оповещение об инцидентах и передача инцидентов во внешние системы
- Отчеты

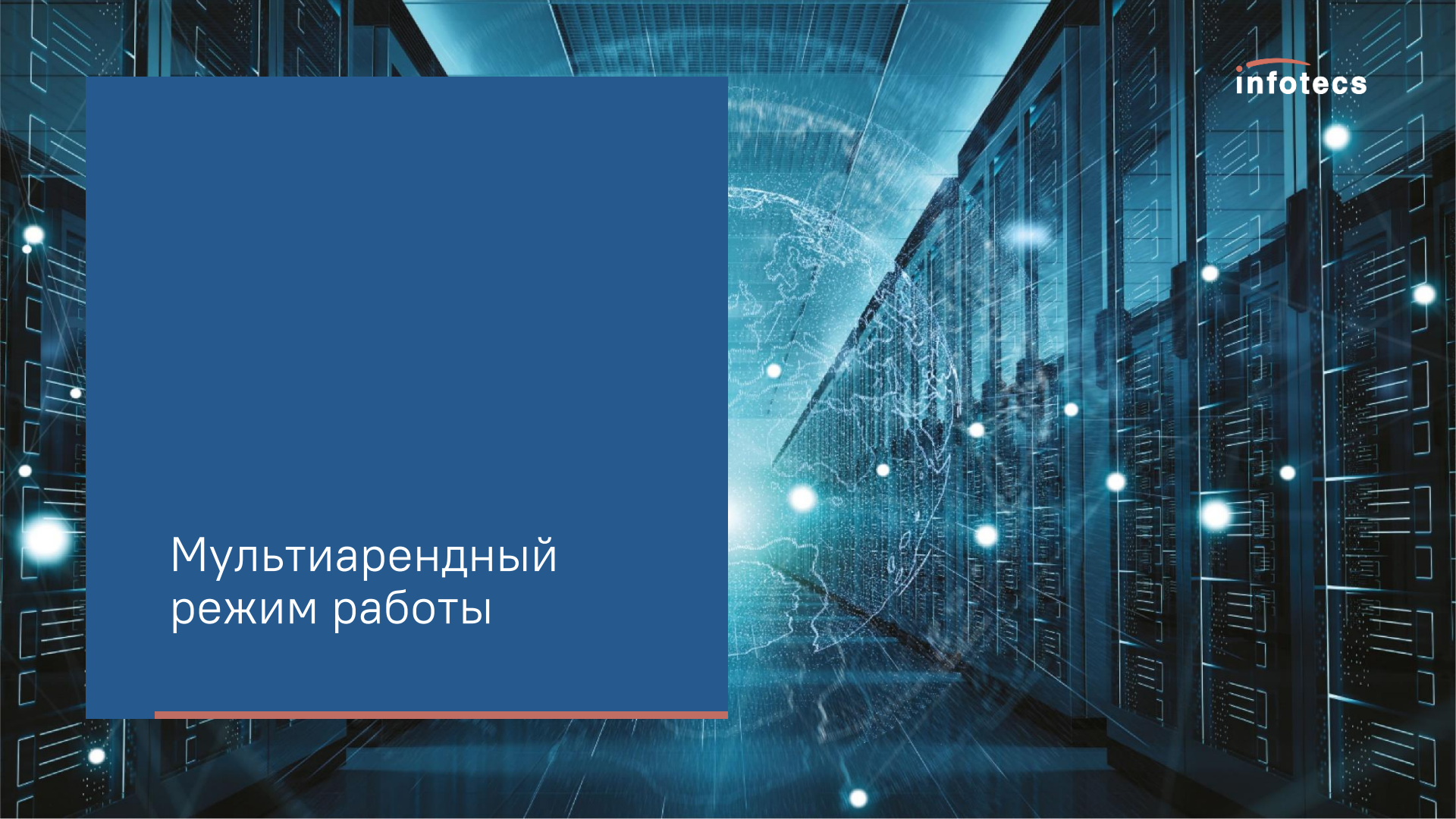
Доступ к Web UI подчиненных TIAS





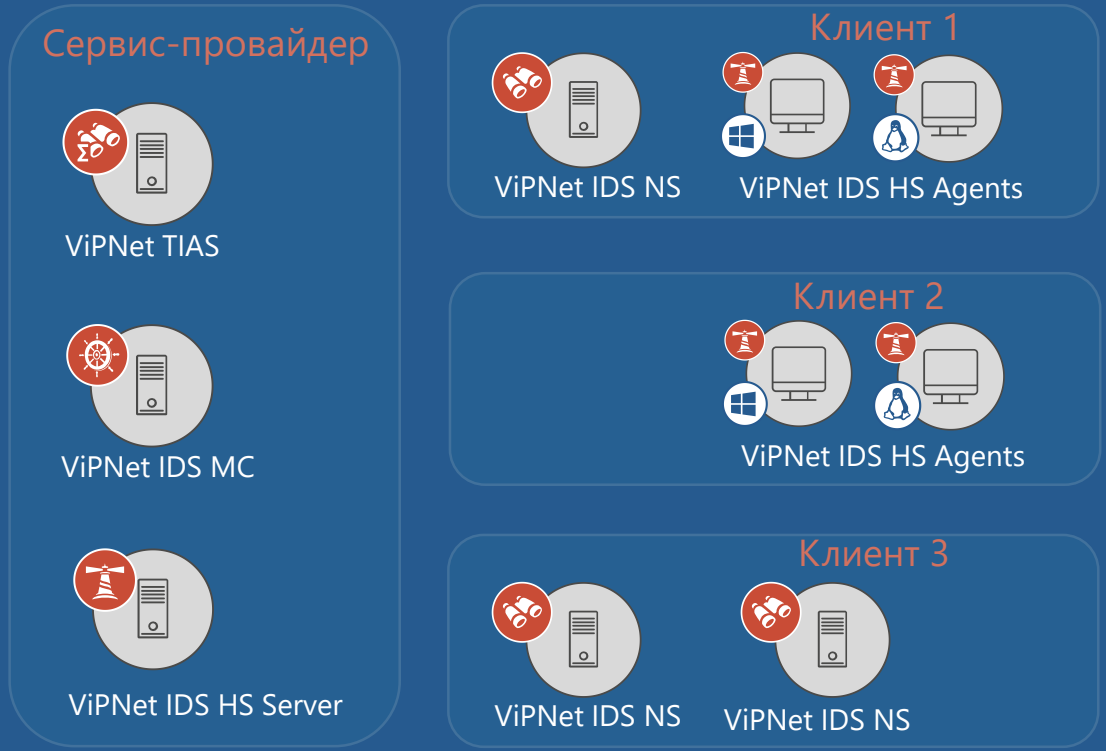
Режим головного TIAS

- Требуется специальная лицензия на головной TIAS
- Управление структурой и режим работы TIAS задается в IDS MC
- Работает на TIAS 2000 и TIAS 5000



Мультиарендный режим работы

Сервис на базе решения

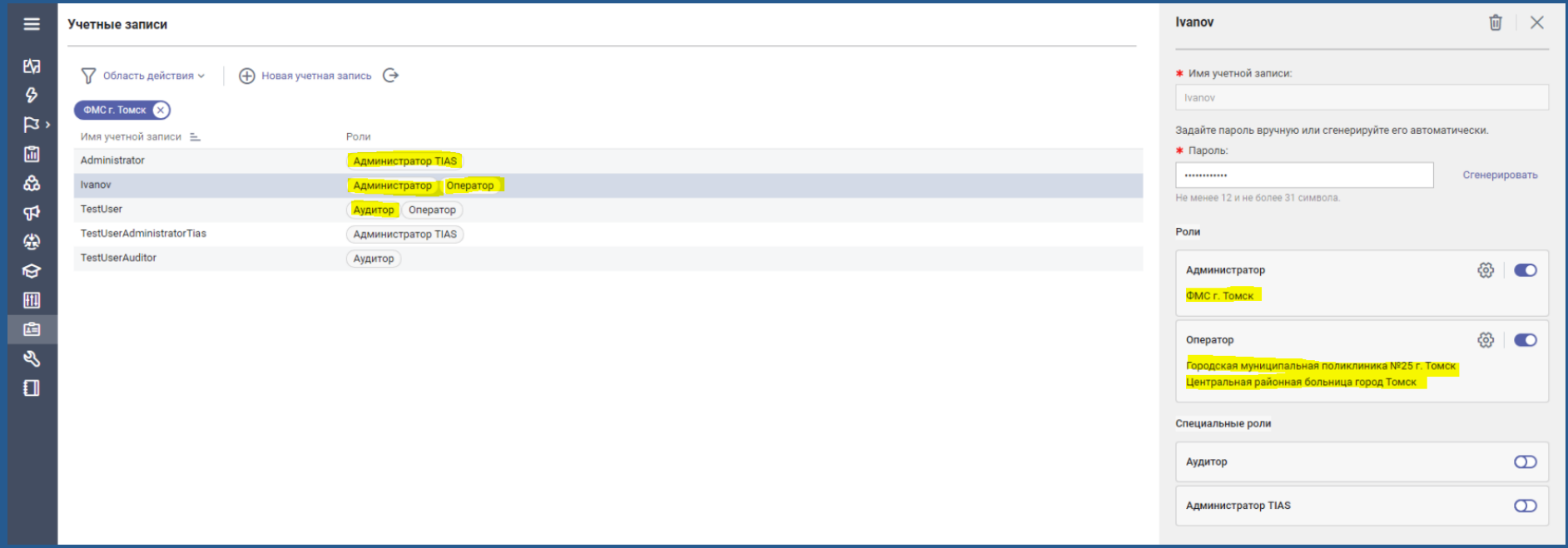


- мультиарендный доступ к IDS MC и TIAS
- мастер подключения организации
- активация и настройка сенсоров из IDS MC
- распределение и учет лицензий по организациям

Виды услуг

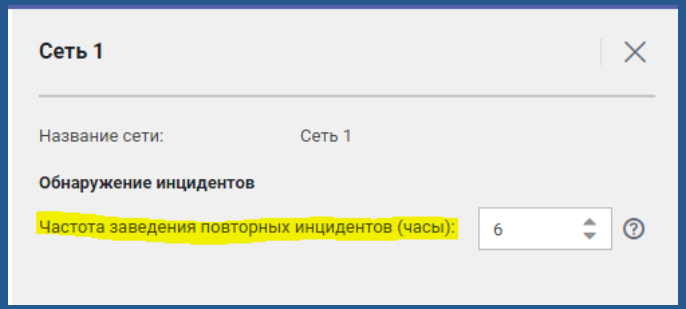
- Мониторинг угроз ИБ в сетевом трафике клиента и автоматическое выявление инцидентов на основе анализа трафика
  - оповещение по e-mail
  - в режиме 24x7
  - сетевой сенсор ViPNet IDS NS.
- Мониторинг угроз ИБ на рабочих станциях пользователей
  - оповещение по e-mail
  - в режиме 24x7
  - сенсоры ViPNet IDS HS agent.
- Проведение расследований по инцидентам и рекомендации по реагированию
  - квалифицированными аналитиками ИБ сервис-провайдера
  - с привлечением аналитиков Перспективного мониторинга
- Предоставление отчетов по выявленным угрозам и инцидентам
- Настройка и обслуживание сенсоров
- Доступ конечного клиента к web-консоли ViPNet TIAS

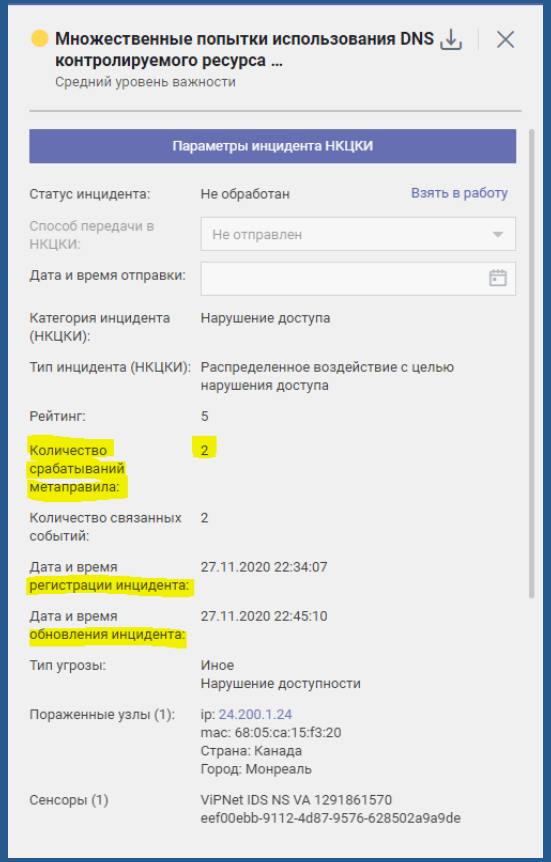
Разграничение доступа в TIAS



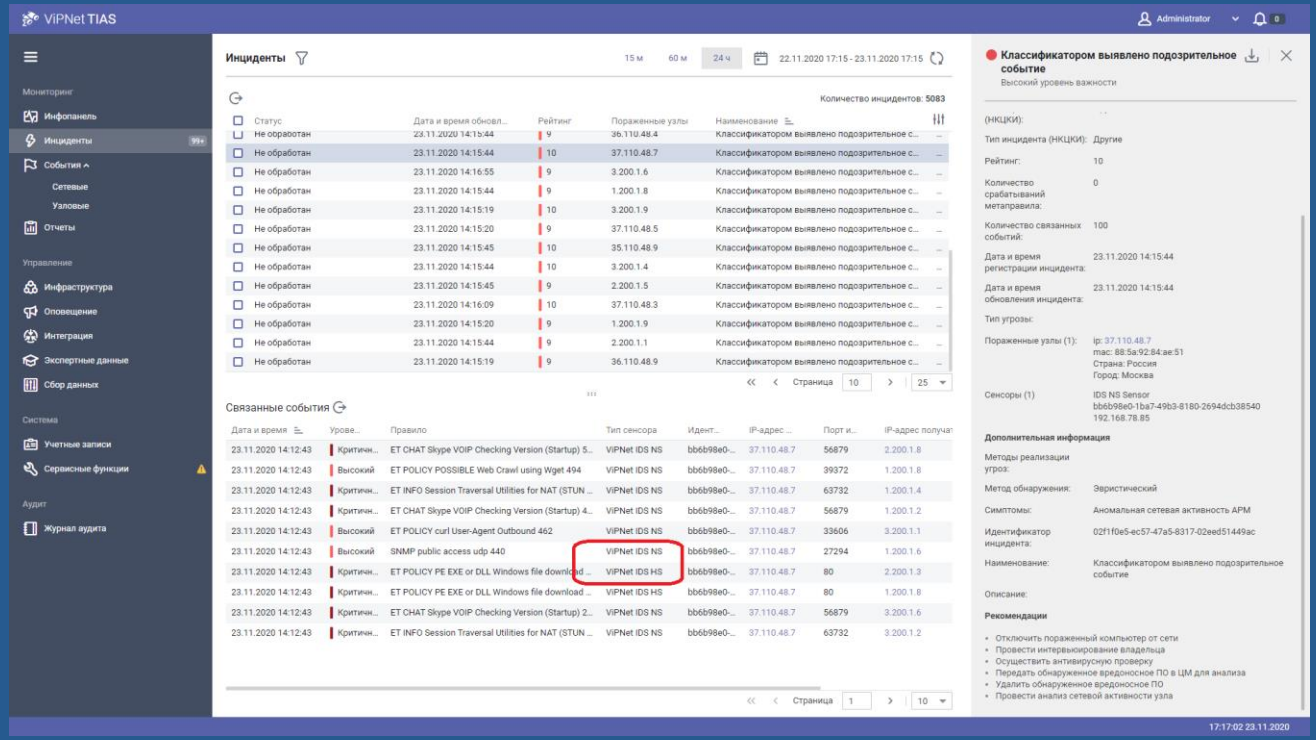
Новые алгоритмы выявления инцидентов

Агрегация инцидентов

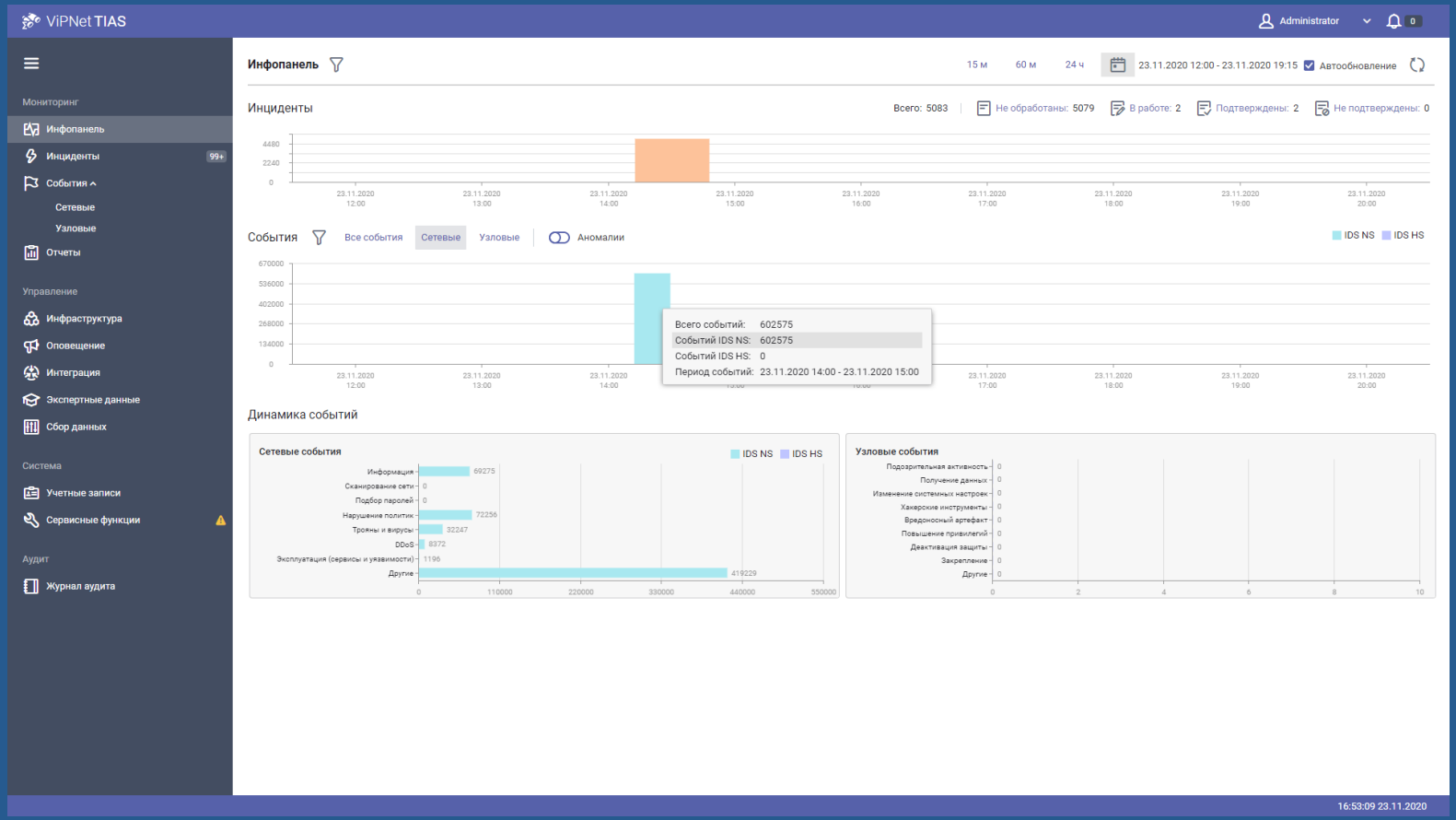


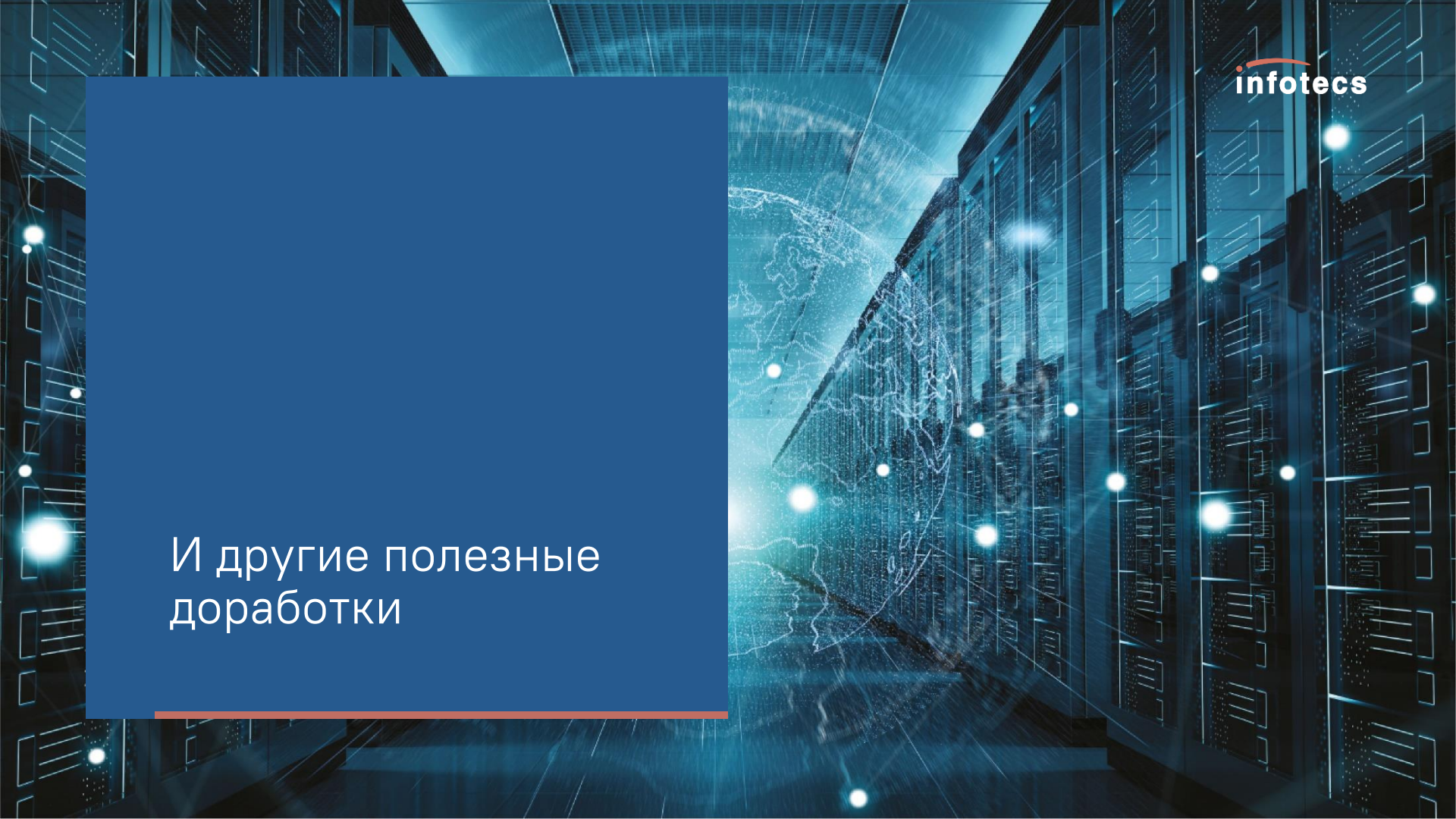


Корреляция событий с разных источников

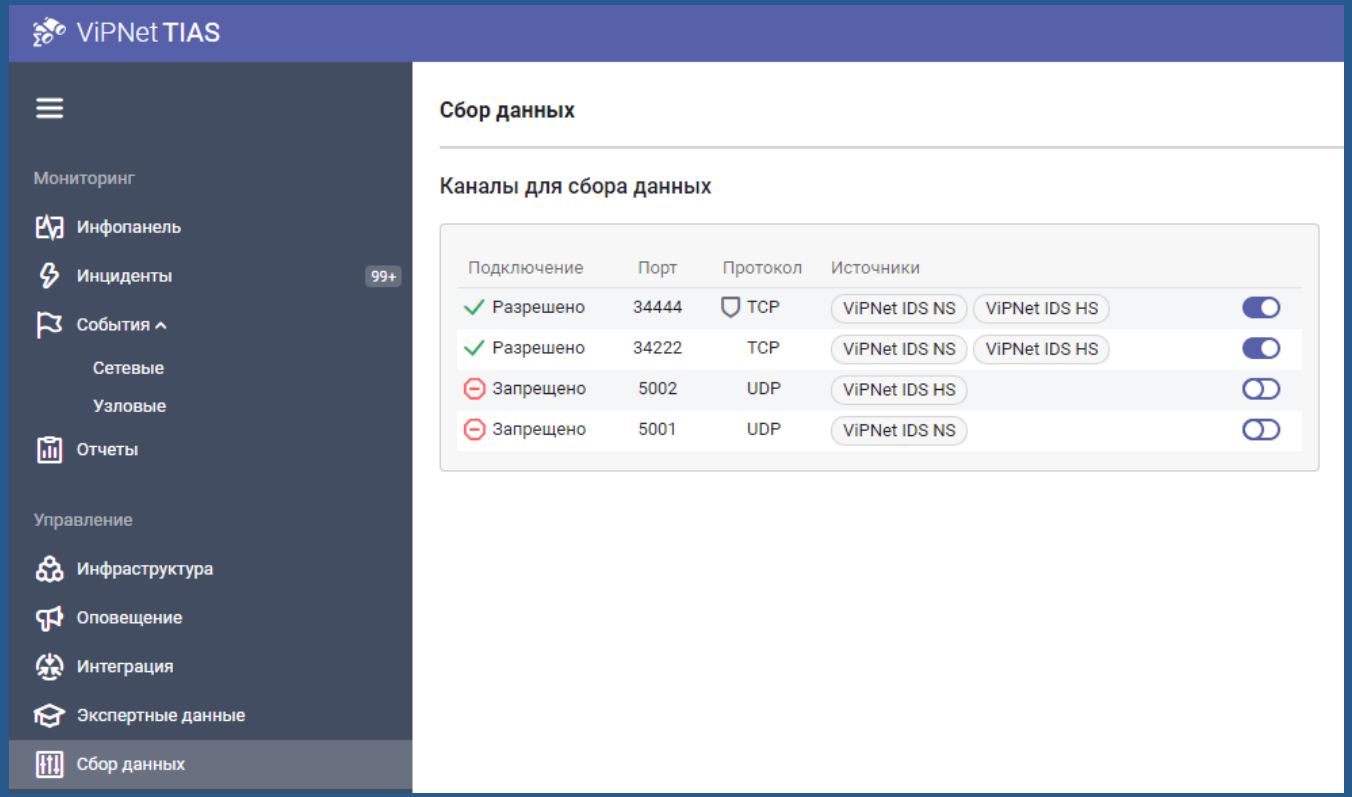


Общая инфопанель событий и инцидентов

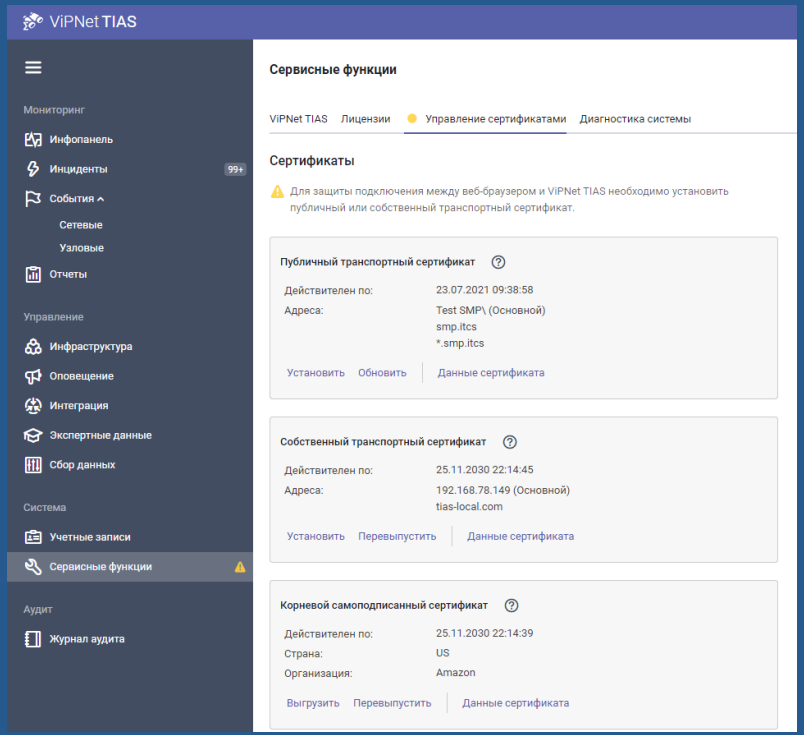


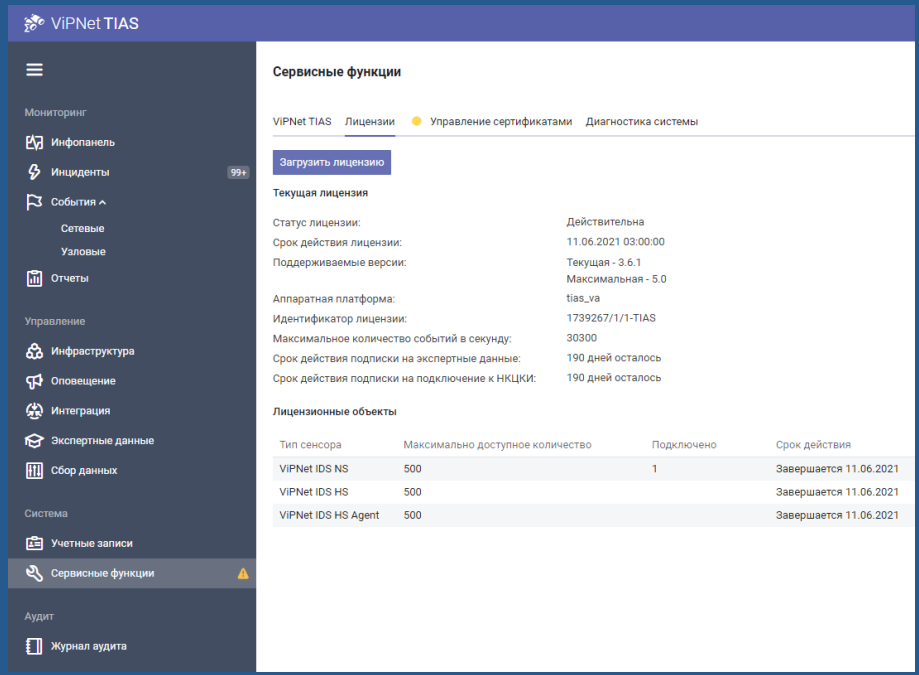

infotecs
И другие полезные доработки

Гарантированная доставка и защита канала передачи событий



Управление сертификатами и лицензией через Web GUI





Другие улучшения

- Загрузка и выгрузка данных по протоколу SFTP
- Установка часового пояса местоположения ViPNet TIAS
- Расширенный набор параметров мониторинга TIAS в ViPNet IDS MC.

Передача в ViPNet IDS MC следующих данных:

- Системное время
- Версия ПО и наименование исполнения ViPNet TIAS
- Дата окончания действия лицензии
- Дата и время установки и выпуска установленных экспертных данных
- Отчет для биллинга об узлах защищаемой сети в каждой обслуживаемой организации.

Основные отличия IDS NS 3 версии

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).

Сертификат выдан на основании технического заключения от 30.09.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 27.10.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

Д.Шевцов

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах информатизации разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

- Централизованное управление и мониторинг с помощью ViPNet IDS MC
- Новый модуль Malware detection
- Возможность анализа до 10 Гбит трафика
- Сертифицированная версия IDS NS VA
- Управление правилами с помощью профилей
- Синхронизация системного времени ViPNet IDS NS
- Возможность удаленного подключения к консоли по протоколу SSH
- Возможность настройки передаваемых в CEF параметров сообщений
- Обнаружение сетевых атак на протокол IPv6
- Расширение функционала по обнаружению атак типа ARP-spoofing

Что дальше?

- ViPNet xFW и EPP в качестве источников
- Выявление инцидентов с использованием репутационных списков адресов
- Обогащение информации об инцидентах данными от сканеров уязвимостей
- Ретроспективный анализ событий
- Новые алгоритмы машинного обучения

Ответы на вопросы!

Контакты

Светлана Старовойт

Старший менеджер
отдела развития продуктов

E-mail:
starovoytsg@infotecs.ru

infotecs

Спасибо
за внимание!