

# Подключение НОВОГО сегмента сети на мониторинг за 30 минут

Светлана Старовойт  
Менеджер продуктов

техно infotecs  
2022 Фест

ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Немного теории

# Решение ViPNet TDR



## ViPNet IDS MC

- Управлять инфраструктурой сенсоров
- Осуществлять мониторинг состояния сенсоров



## ViPNet TIAS

- Анализировать события ИБ от сетевых и хостовых сенсоров и выявлять инциденты ИБ



## ViPNet IDS NS

- Выявлять события ИБ в сетевом трафике



## ViPNet IDS HS

- Выявлять события ИБ и аномалии поведения на конечных узлах

# Система управления ViPNet IDS MC

The screenshot displays the ViPNet IDS MC web interface. The top navigation bar includes 'Управление', 'Мониторинг', 'Устройства', and 'Обновления'. The main content area is divided into two panels:

- Зарегистрированные устройства (Registered Devices):** A table listing devices with columns for 'Наименование' (Name), 'Описание' (Description), 'Платформа' (Platform), and 'Версия ПО' (Software Version).

Наименование	Описание	Платформа	Версия ПО
ALLEREY	192.168.42.20	ViPNet IDS NS VA	3.5.0-509983
CLOMOT	192.168.42.21	ViPNet IDS NS VA	3.5.0-509983
...	...	ViPNet IDS HS	1.4.0.55183
...	...	ViPNet IDS HS	1.4.0.55183
...	...	ViPNet IDS NS VA	3.5.0-507252
...	...	ViPNet IDS NS VA	3.5.0-510915
- Мониторинг (Monitoring):** A summary of system health and tasks.

Состояние	Задача	Счетчик
Опасное состояние	Резервное копирование не выполнялось	14 дней
Предупреждение	Задачи, выполненные с ошибками	23 задачи
Информация	Незасланные обновления ПО	2 обновления
Информация	Незасланные обновления баз правил	12 запросов
Информация	Незасланные обновления баз Malware detection	2 запроса
Успех	Система в работоспособном состоянии	

- Управление пользователями и инфраструктурой решения TDR
- Разворачивание и инициализация устройств
- Настройка параметров работы устройств
- Управление обновлениями БРП, Malware, ЭД
- Управление лицензиями устройств
- Управление обновлениями ПО
- Мониторинг состояния устройств TDR

# Ролевой доступ в ViPNet IDS MC

Управление функциями IDS MC

Управление устройствами

Главный администратор

Главный администратор устройства

Главный администратор для  
локального доступа

Администратор устройства

Администратор безопасности

Пользователь устройства

Администратор

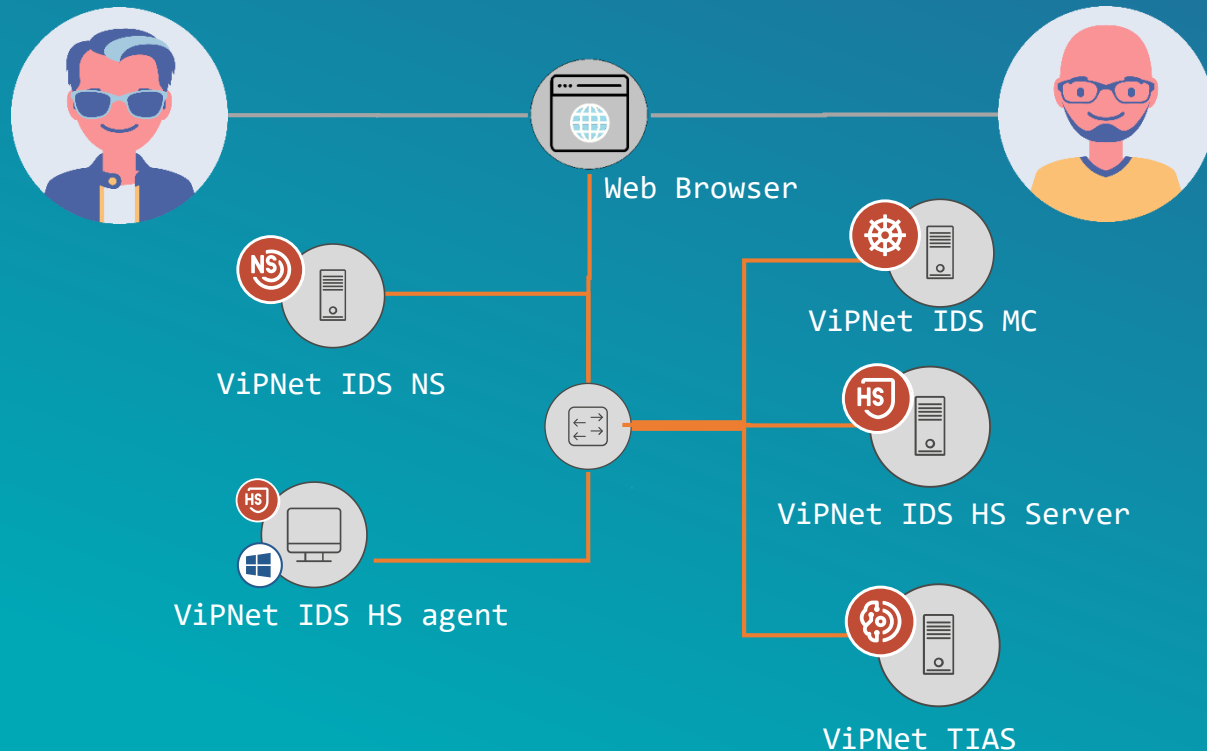
Аудитор

# Мастер-класс

# Описание стенда и сценария

Администратор филиала в г. Хабаровск

Администратор головного офиса



1. Подключение на обслуживание новой организации (контролируемого сегмента сети)
2. Добавление в организацию нового сенсора IDS NS
3. Подключение агента IDS HS
4. Настройка работы сенсоров из IDS MC
5. Настройка автоматических обновлений
6. Мониторинг состояния устройств

ТЕХНО infotecs  
2022 Фест

Спасибо за внимание!

---

Подписывайтесь на наши соцсети



[https://vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_news](https://t.me/infotecs_news)