

# Подключение нового сегмента сети на мониторинг за 30 минут

Светлана Старовойт  
Руководитель продуктового направления



техно infotecs  
2023 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 management interface. The top section, titled "Зарегистрированные устройства" (Registered devices), shows a list of devices with columns for Name, Description, Platform, and Version. Two devices are listed: ALLEREY and CLOMOT, both running VIPNet IDS NS VA 3.5.0-509983. The bottom section, titled "Мониторинг" (Monitoring), shows the overall status of the system as "Опасное состояние" (Dangerous state) and lists several alerts:

Alert	Count
Резервное копирование не выполнялось (Backup not performed)	14 дней (days)
Задачи, выполненные с ошибками (Tasks completed with errors)	23 задачи (tasks)
Неразосланные обновления ПО (Unsent software updates)	2 обновления (updates)
Неразосланные обновления баз правил (Unsent rule base updates)	12 запросов (requests)
Неразосланные обновления баз Malware detection (Unsent Malware detection base updates)	2 запроса (requests)
Система в работоспособном состоянии (System in operational state)	

- 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

Главный администратор

Главный администратор  
для локального доступа

Администратор безопасности

Администратор

Аудитор

## Управление устройствами

Главный администратор устройства

Администратор устройства

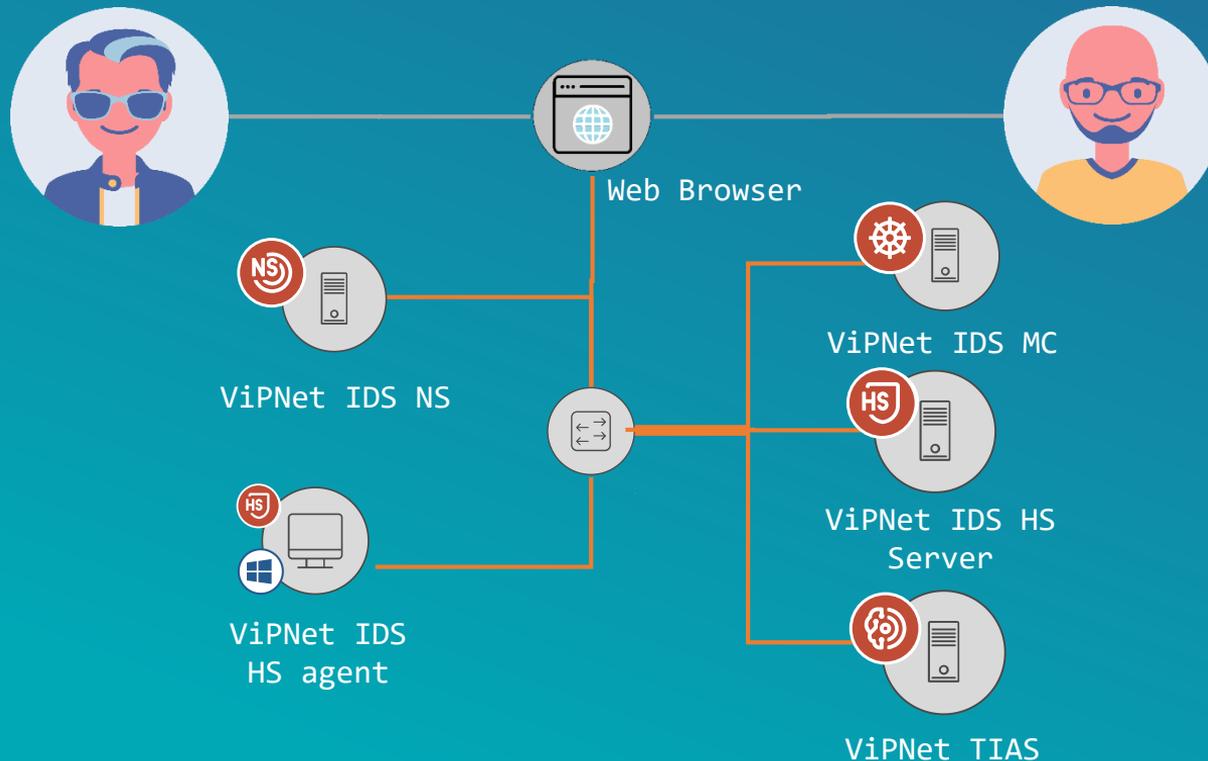
Пользователь устройства

# Мастер-класс

# Описание стенда и сценария

Администратор филиала в г. Мурманск

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



Спасибо за внимание!

---

Подписывайтесь на наши соцсети



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



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)