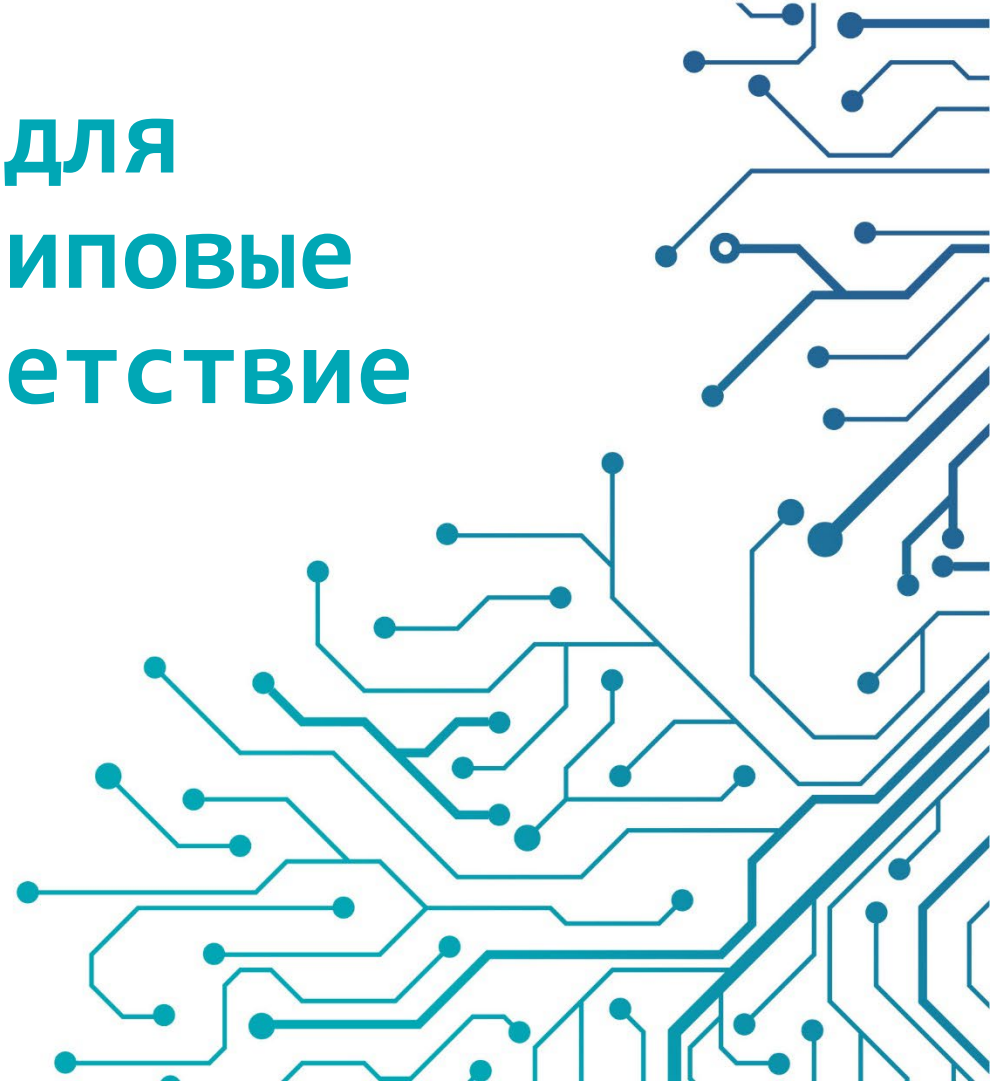
Решения ViPNet для объектов КИИ: типовые сценарии, соответствие требованиям

Селифанов Валентин
Заместитель руководителя
обособленного подразделения

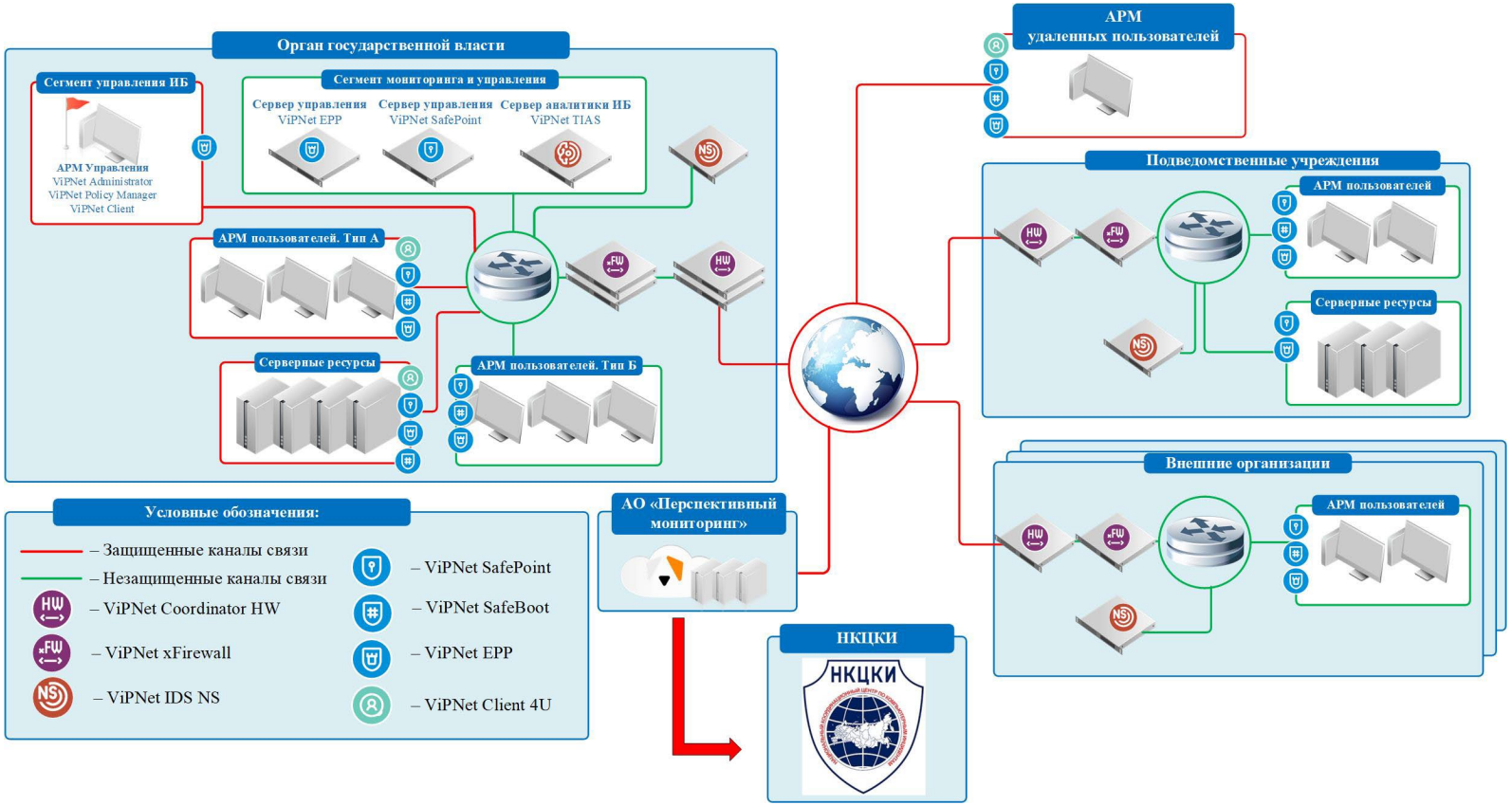
infotecs



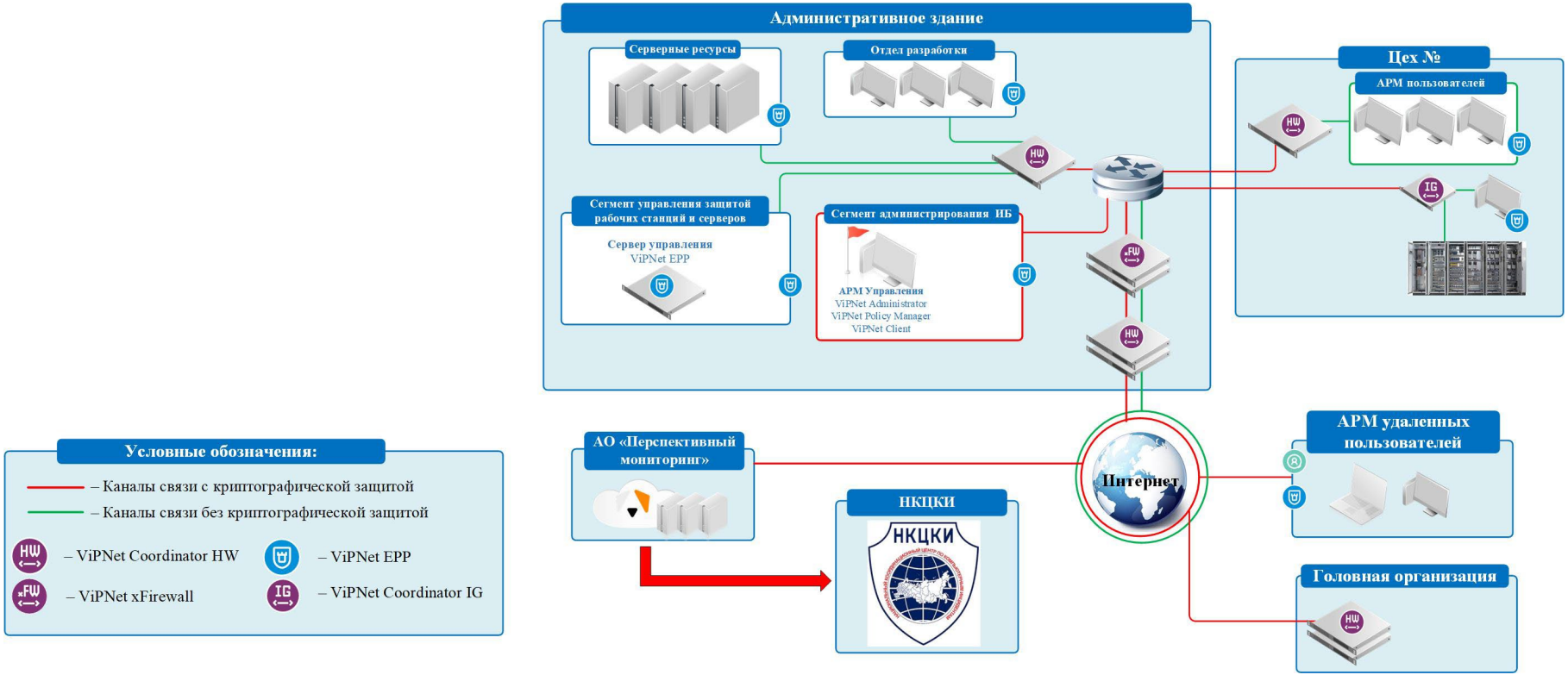
infotecs

Сценарии и соответствие требованиям

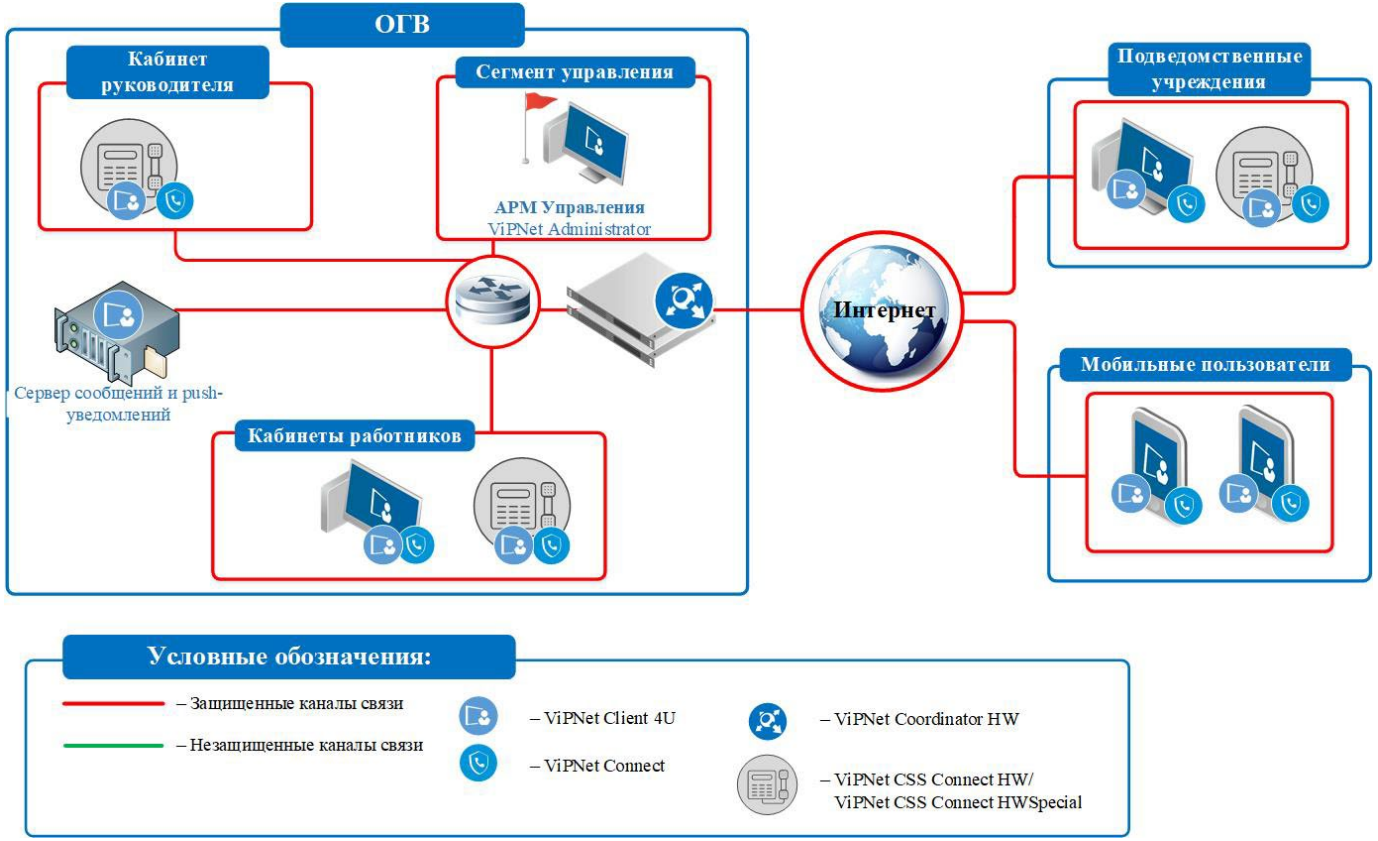
Защита распределенных систем



Защита оборонных предприятий



Защита коммуникаций

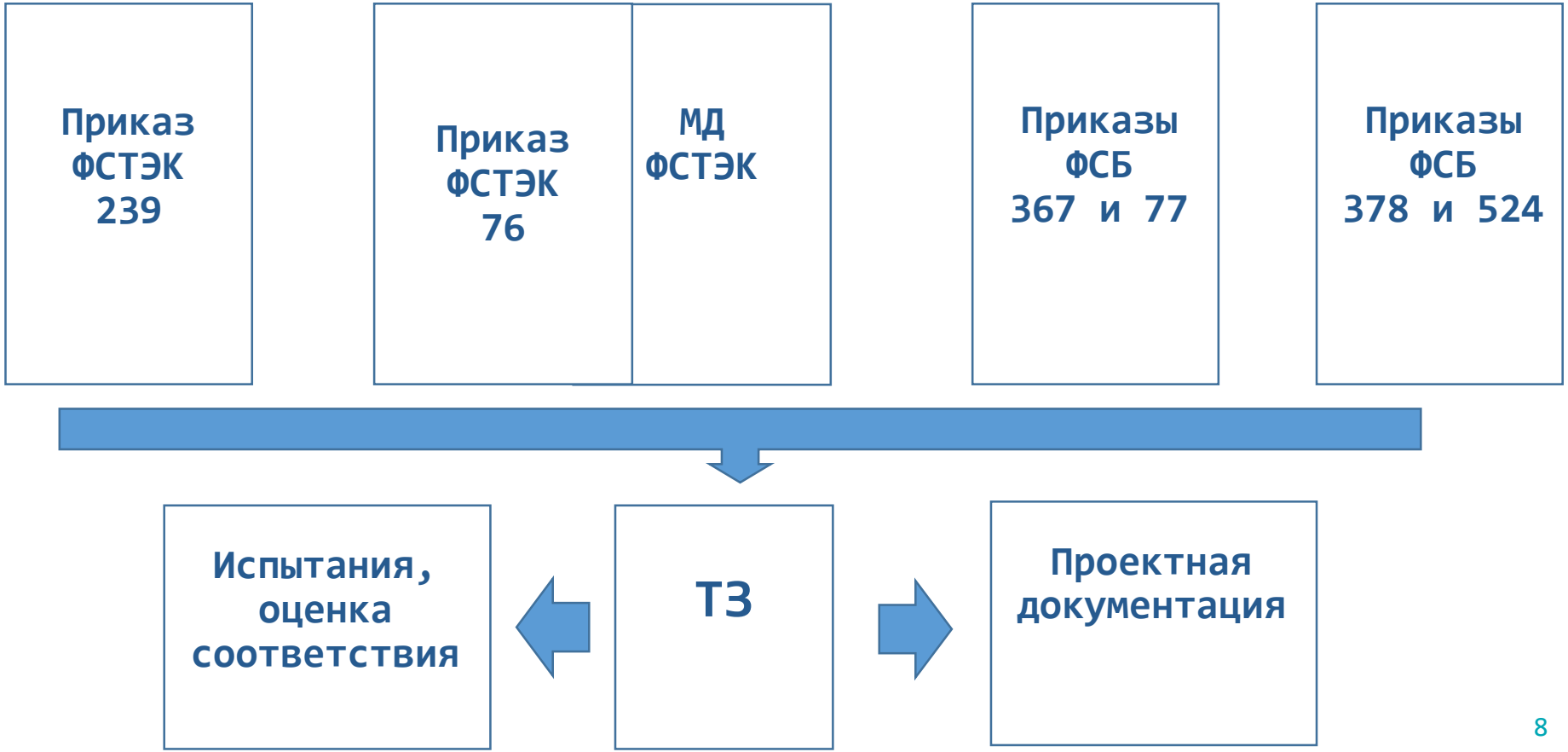


Требования к системе защиты

Техническое задание

- цель и задачи обеспечения безопасности
- категорию значимости ЗО КИИ
- перечень НПА, МД и НС, которым должен соответствовать объект
- перечень объектов защиты
- требования к организационным и техническим мерам, применяемым для обеспечения безопасности ЗО КИИ
- стадии (этапы работ) создания подсистемы безопасности ЗО КИИ
- требования к применяемым программным и программно-аппаратным средствам, в том числе СЗИ
- требования к защите средств и систем, обеспечивающих функционирование ЗО КИИ
- требования к информационному взаимодействию ЗО КИИ с иными О КИИ, а также иными ИС, АСУ или ИТКС
- требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта

Требования к системе защиты



Требования к системе защиты

ТЗ

СЗИ не ниже 4 класса защиты, а также СВТ не ниже 5 класса

+

Уровень доверия 4

Выбор средств защиты

Проектирование подсистемы безопасности значимого объекта

- **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- **определяются и обосновываются организационные и технические меры**, подлежащие реализации в рамках подсистемы безопасности значимого объекта;
- **определяются виды и типы средств защиты информации**, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
- **осуществляется выбор средств защиты информации** и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
- **разрабатывается архитектура подсистемы безопасности** значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
- **определяются требования к параметрам настройки** программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
- **определяются меры по обеспечению безопасности** при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

Макетирование

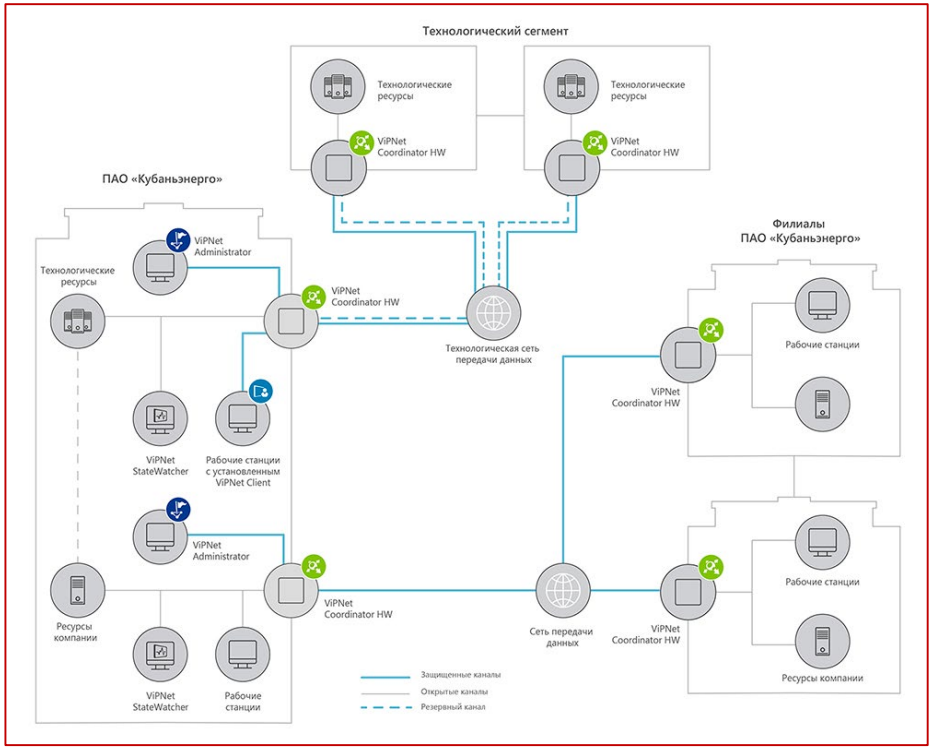
> В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды.

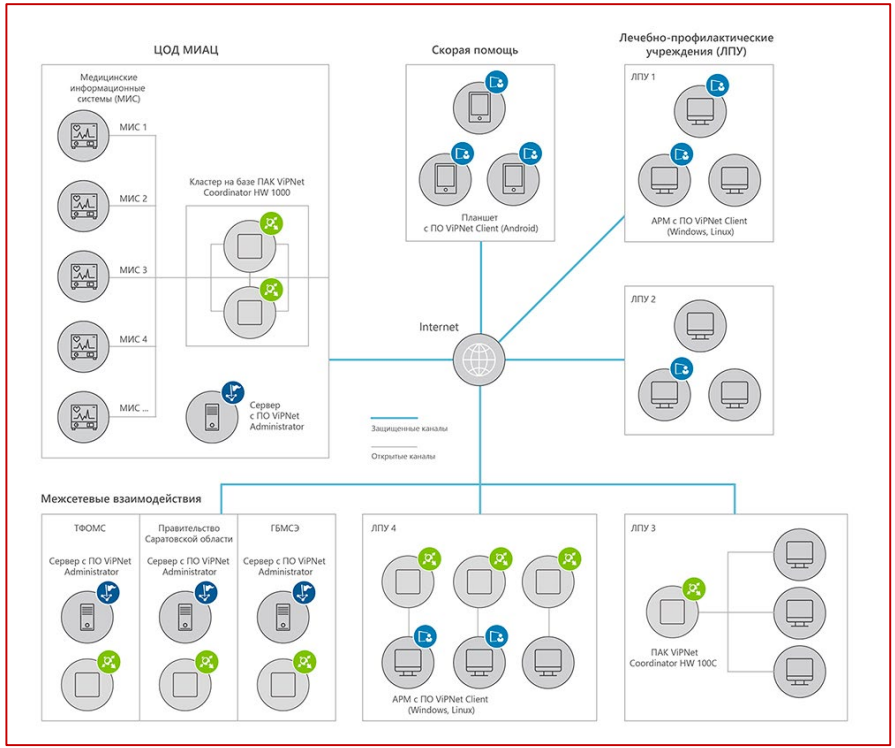
Пилотный проект

infotecs

Схемы решений и реализованные проекты

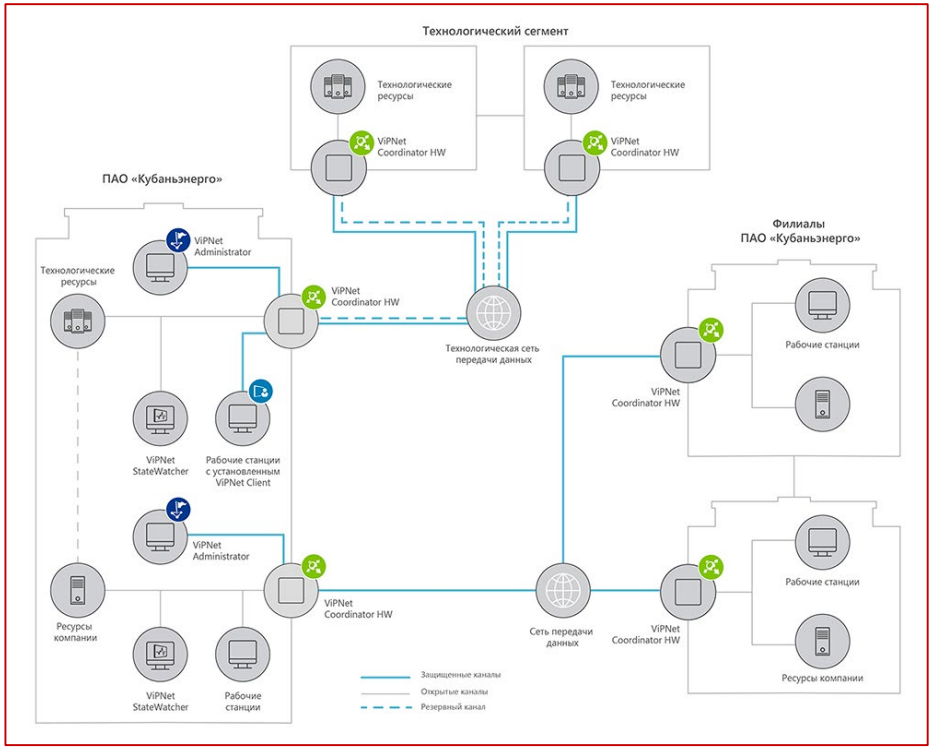
Защита распределенных систем

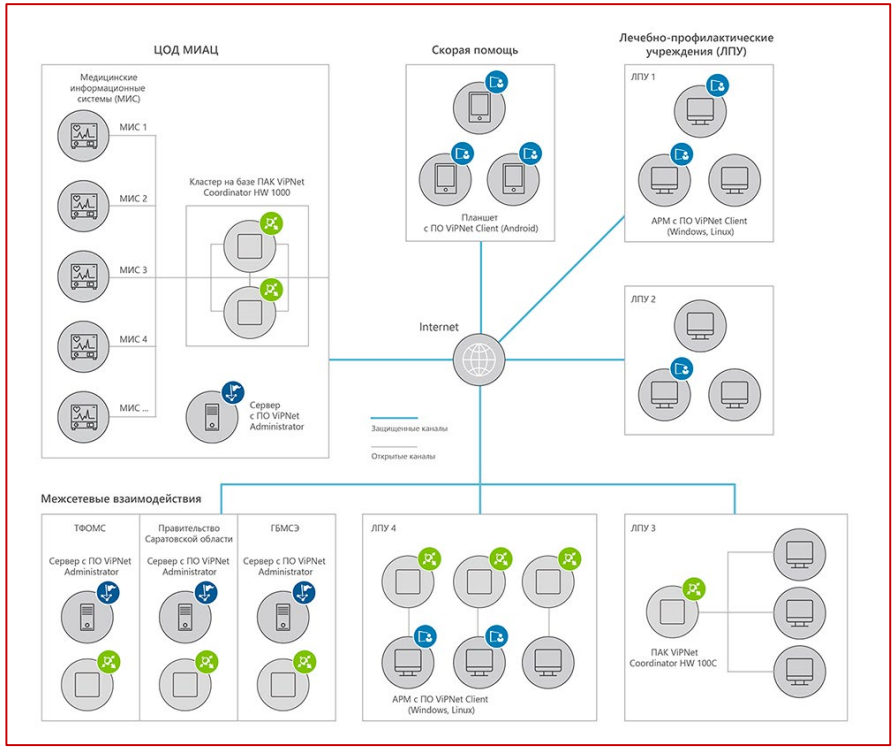




Истории успеха https://infotecs.ru/stories/?PAGEN_1=3

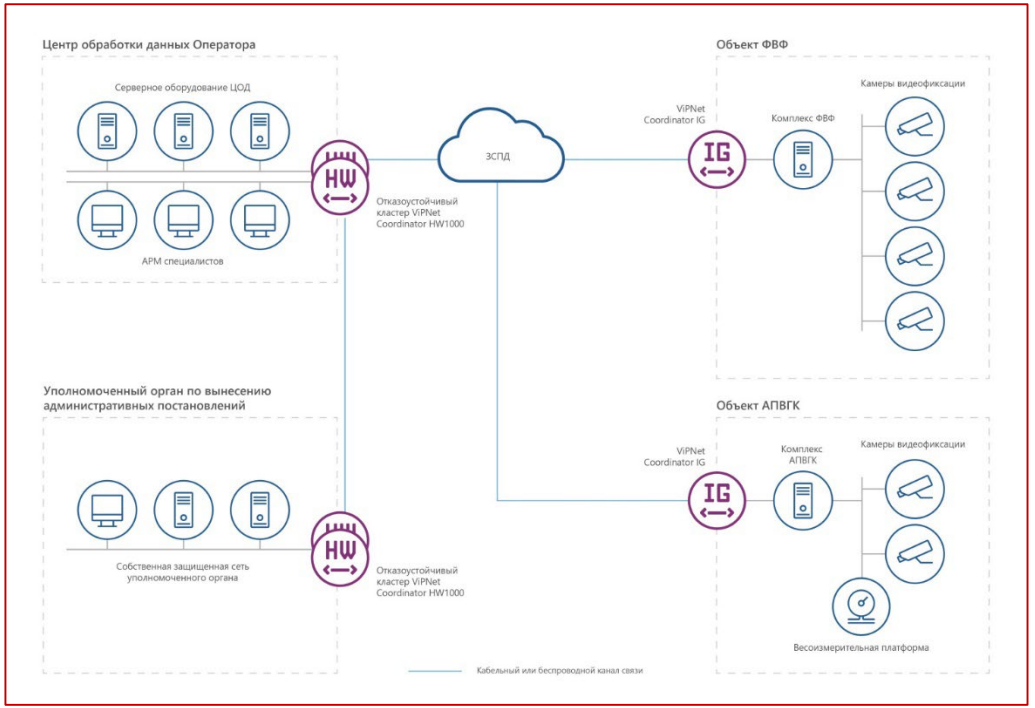
Защита распределенных систем

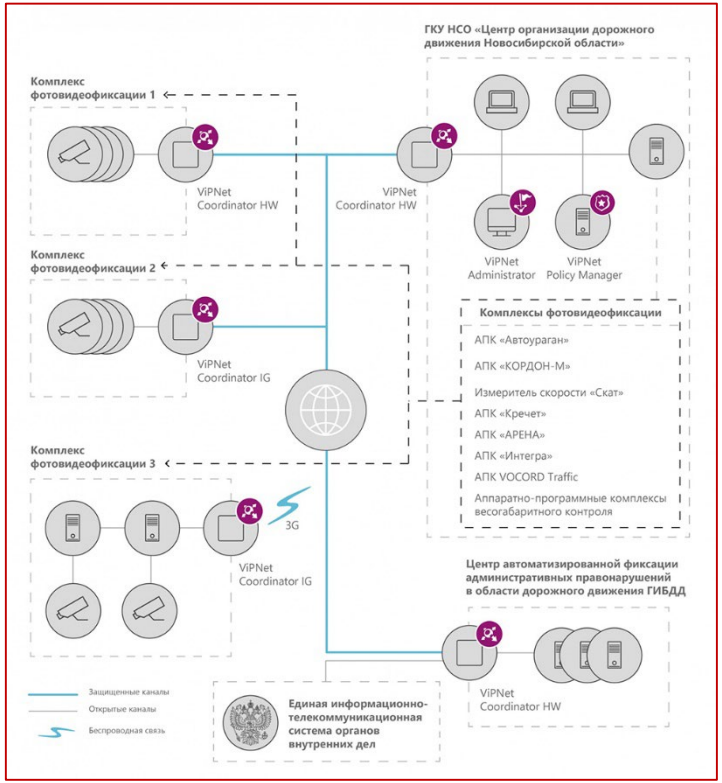




Истории успеха https://infotecs.ru/stories/?PAGEN_1=3

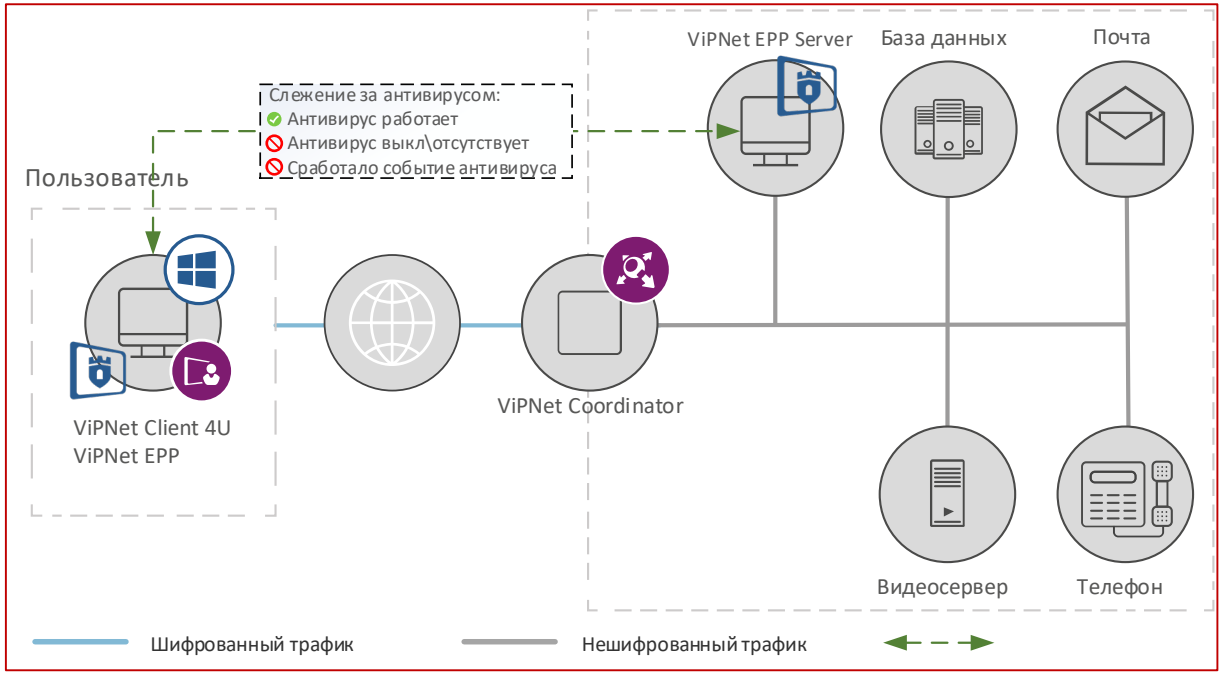
Фотовидеофиксация



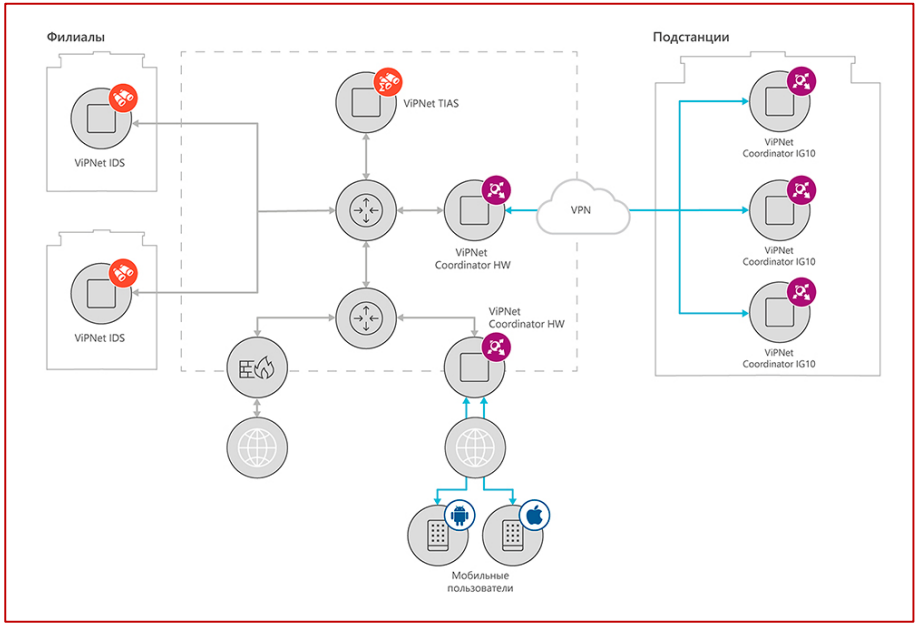


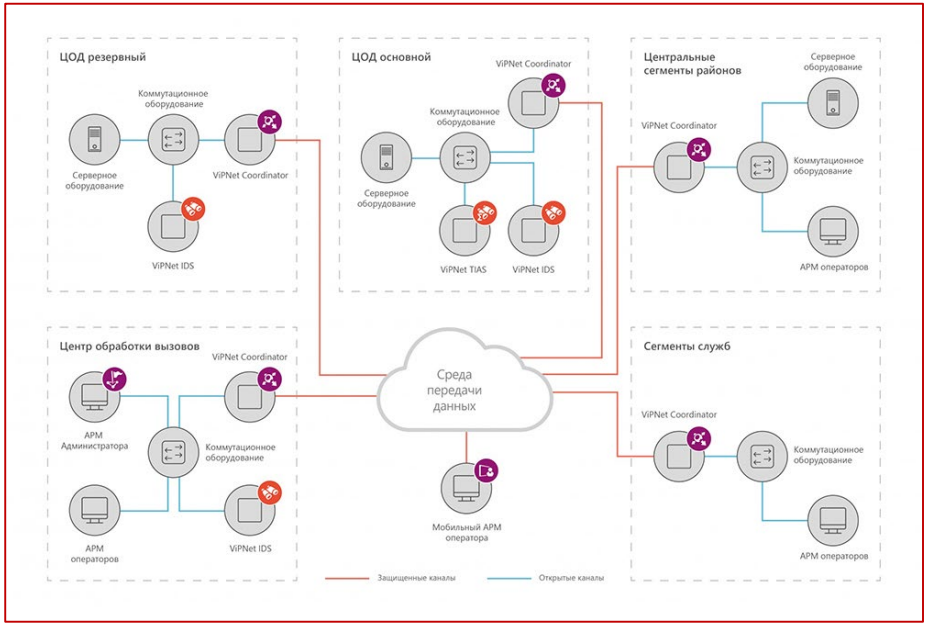
Истории успеха https://infotecs.ru/stories/?PAGEN_1=3

Создание микропериметра с помощью ViPNet EPP



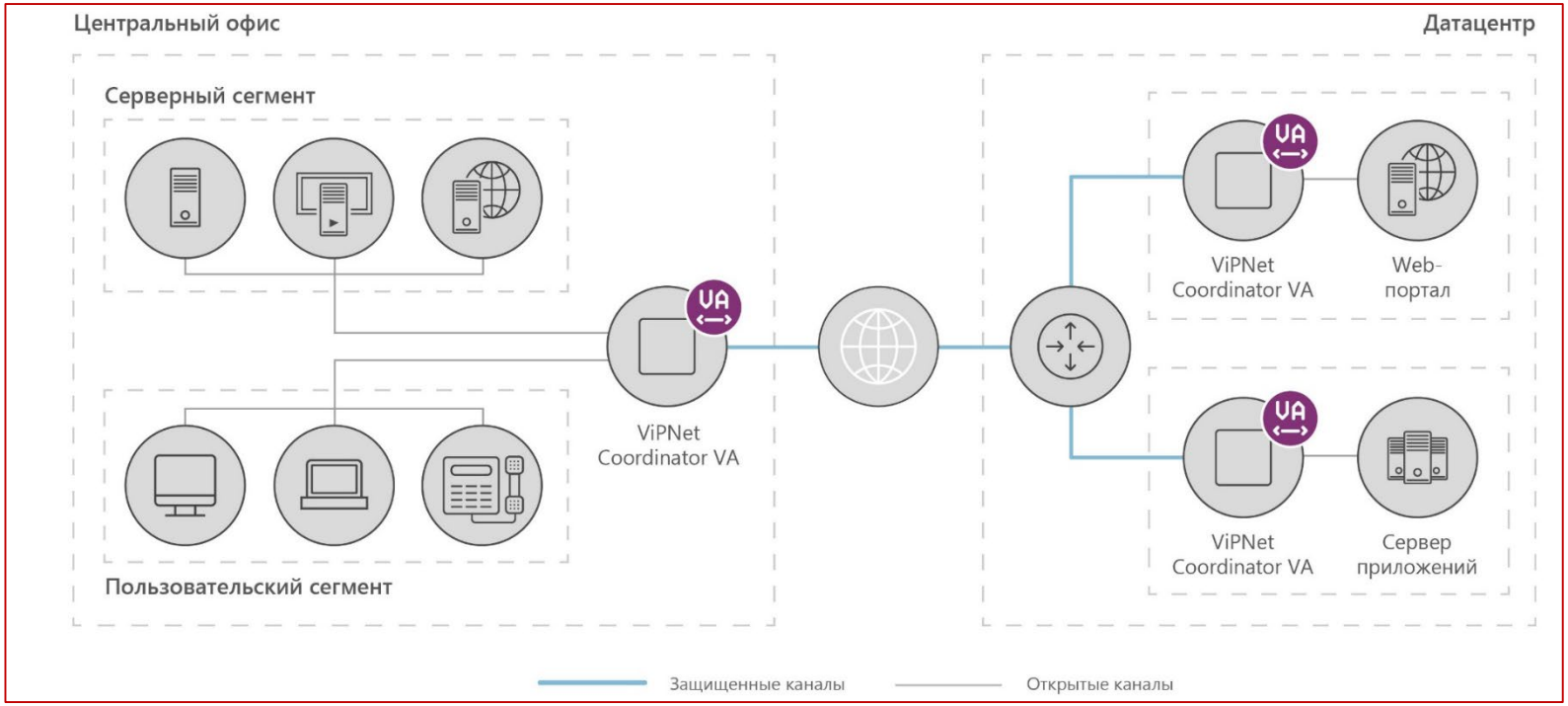
Обнаружение вторжений и угроз





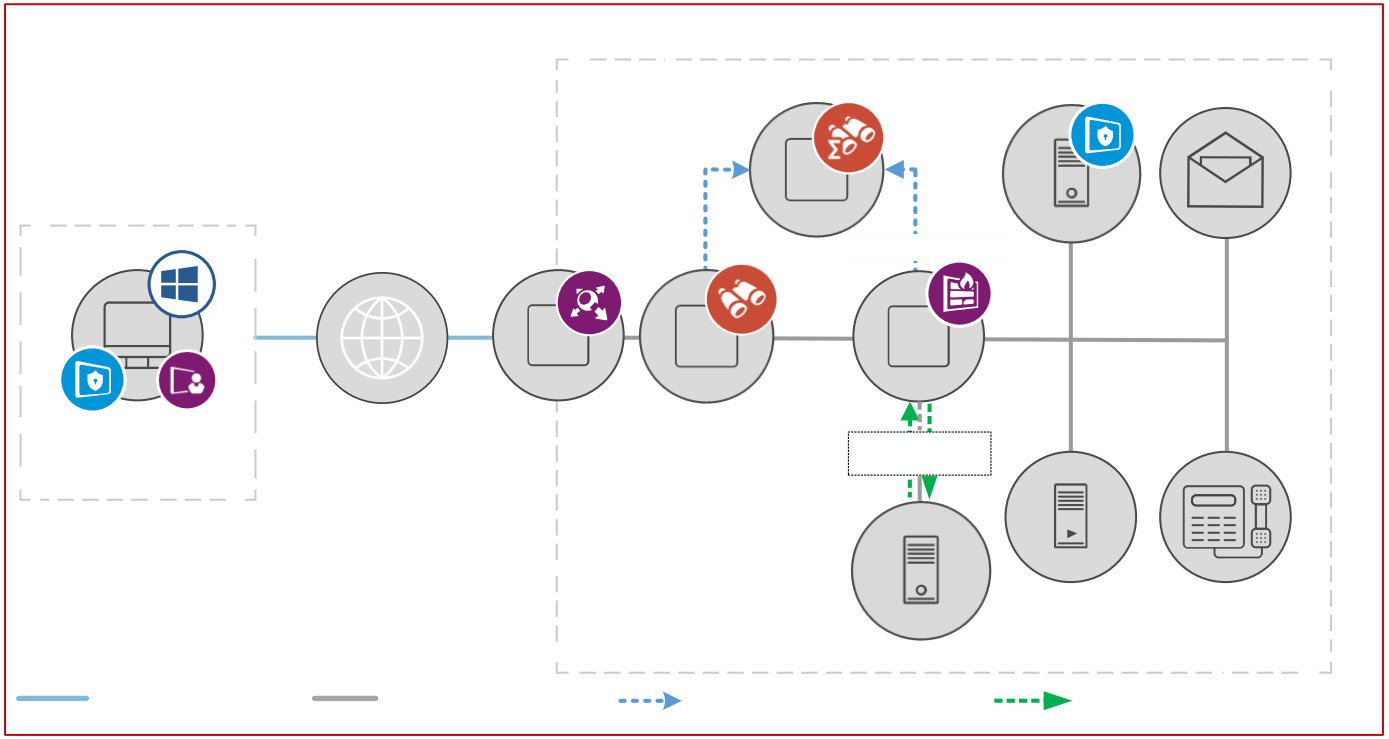
Истории успеха https://infotecs.ru/stories/?PAGEN_1=3

Сегментация сетей и безопасность частного облака

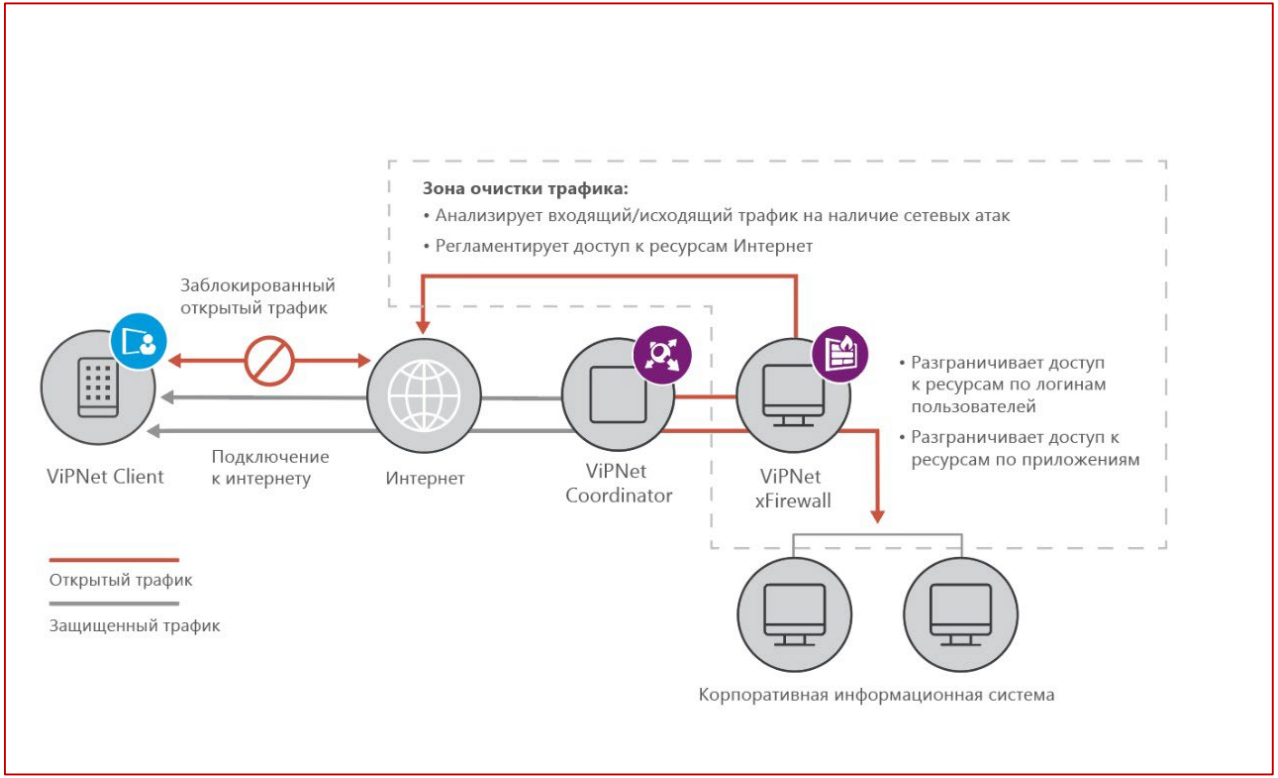


Истории успеха https://infotecs.ru/stories/?PAGEN_1=3

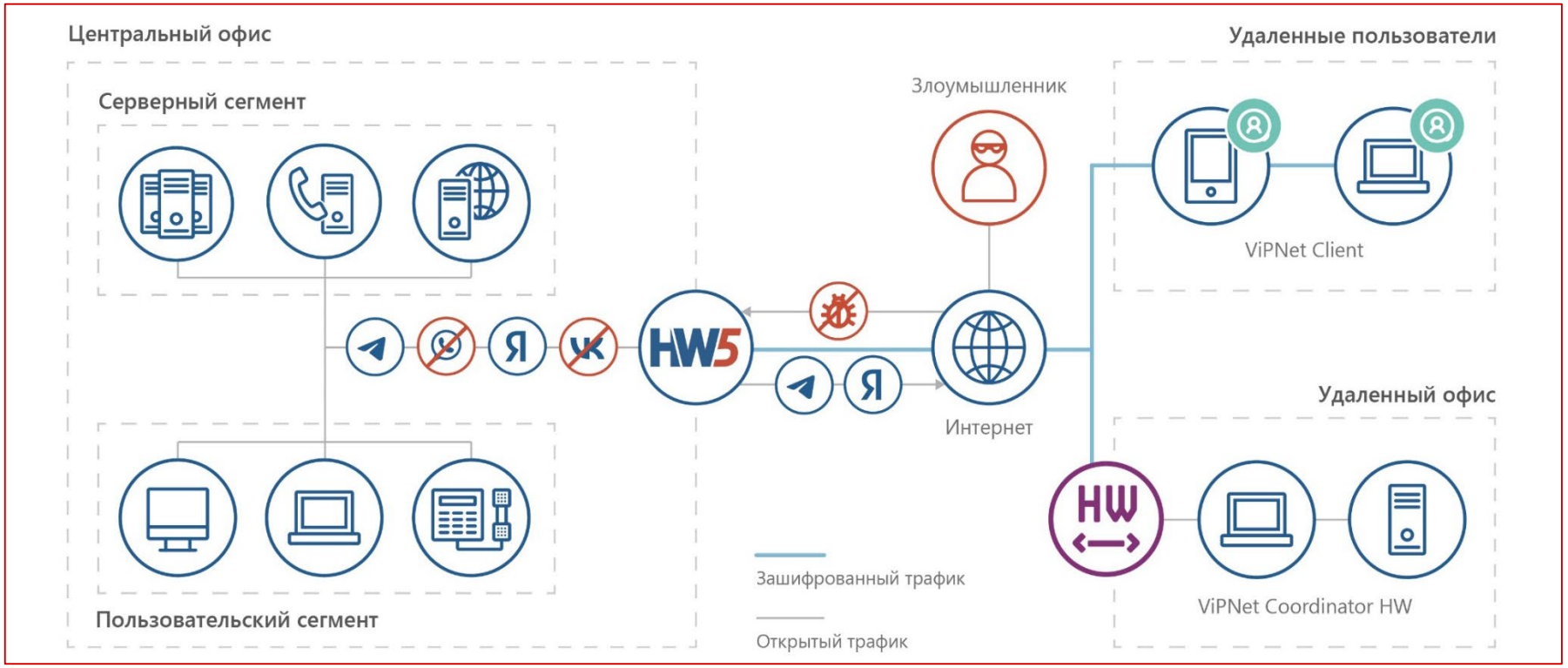
ZTA=VPN+xFirewall+SafePoint+TDR



Безопасный доступ в Internet = ViPNet VPN + xFirewall



Типовая схема применения HW 5



Дополнительная информация

Спасибо за внимание!

Селифанов Валентин
Valentin.Selifanov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363