infotecs

Как работать удаленно безопасно

Мы давно работаем удаленно







infotecs

Мир изменился

Давным-давно, примерно 3 недели назад…

- Чтение блогов
- VK, Одноклассники
- Twitter
- IM/WhatsApp
- Загрузка файлов (Dropbox, Яндекс.Диск)
- Потоковое видео (Youtube, Ivi)
- Потоковое аудио (Яндекс.Музыка)
- Качаем торренты
- Удаленный рабочий стол (TeamViewer, RDP)

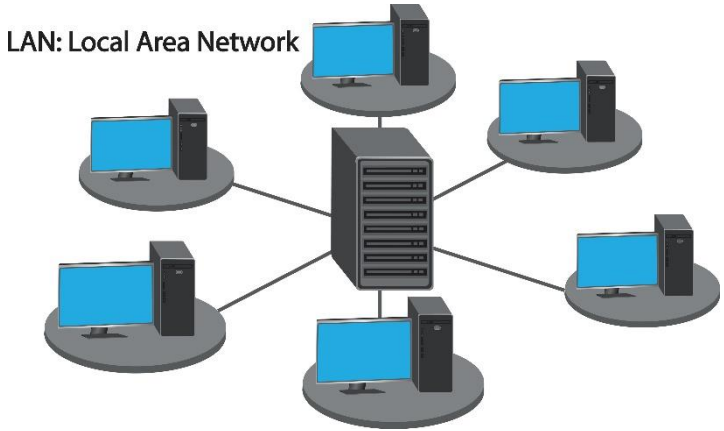


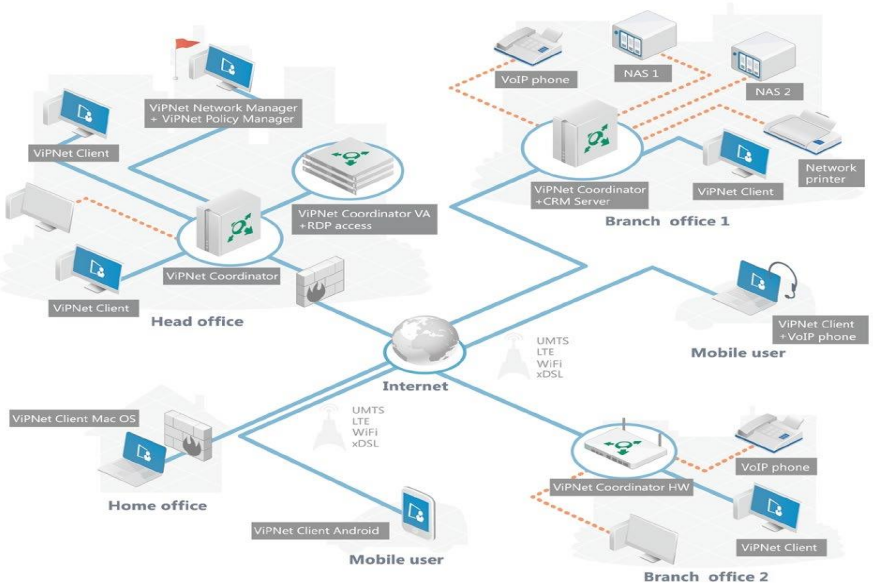
Мечты сбываются





Как поменять парадигму







Риски и Проблемы при удаленной работе

Риски

infotecs

Терминальные сервера и другие ресурсы

Механизмы аутентификации (логин - пароль)

Служебные подключения к поддерживающим сервисам

MITM

BYOD (политики, вредоносы)

Мобильный доступ

Не контролируемые работы в облаках

Работы с ЭП

Что будет, если риски сработают – Проблемы

infotecs

Обход затянутых гаек (shadow it, gmail, whatsapp и тп)

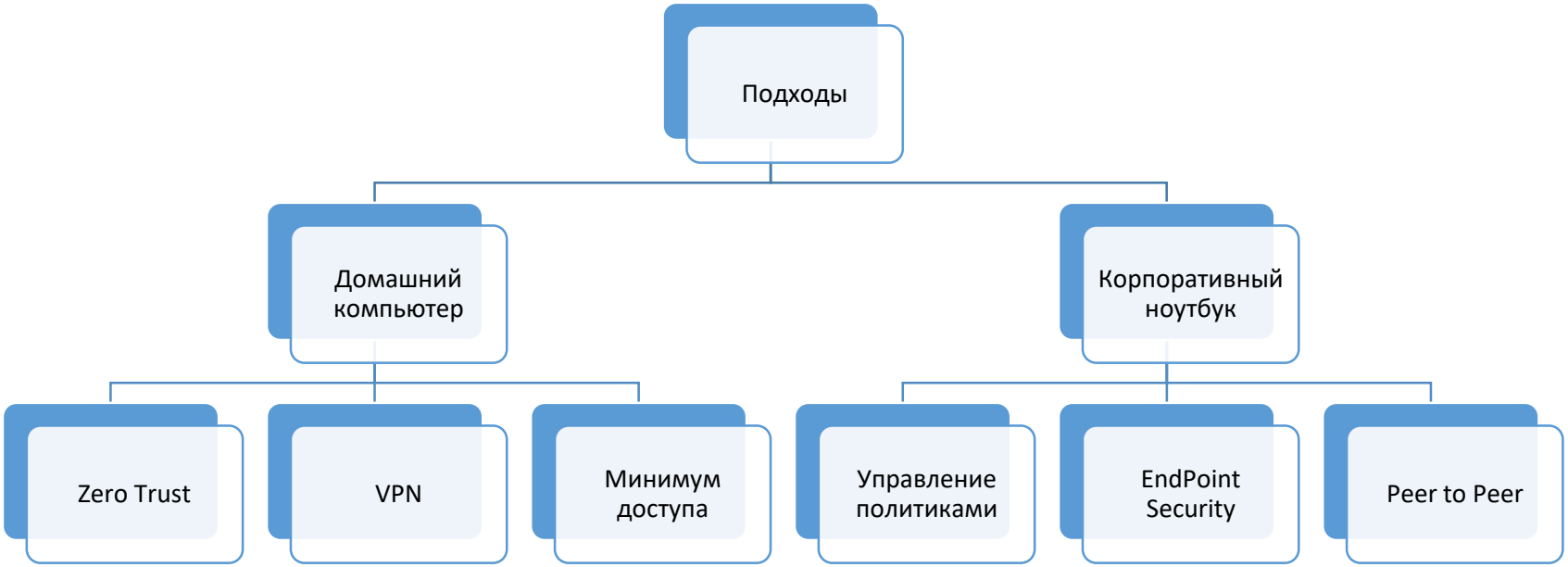
Локальные копии, кэши

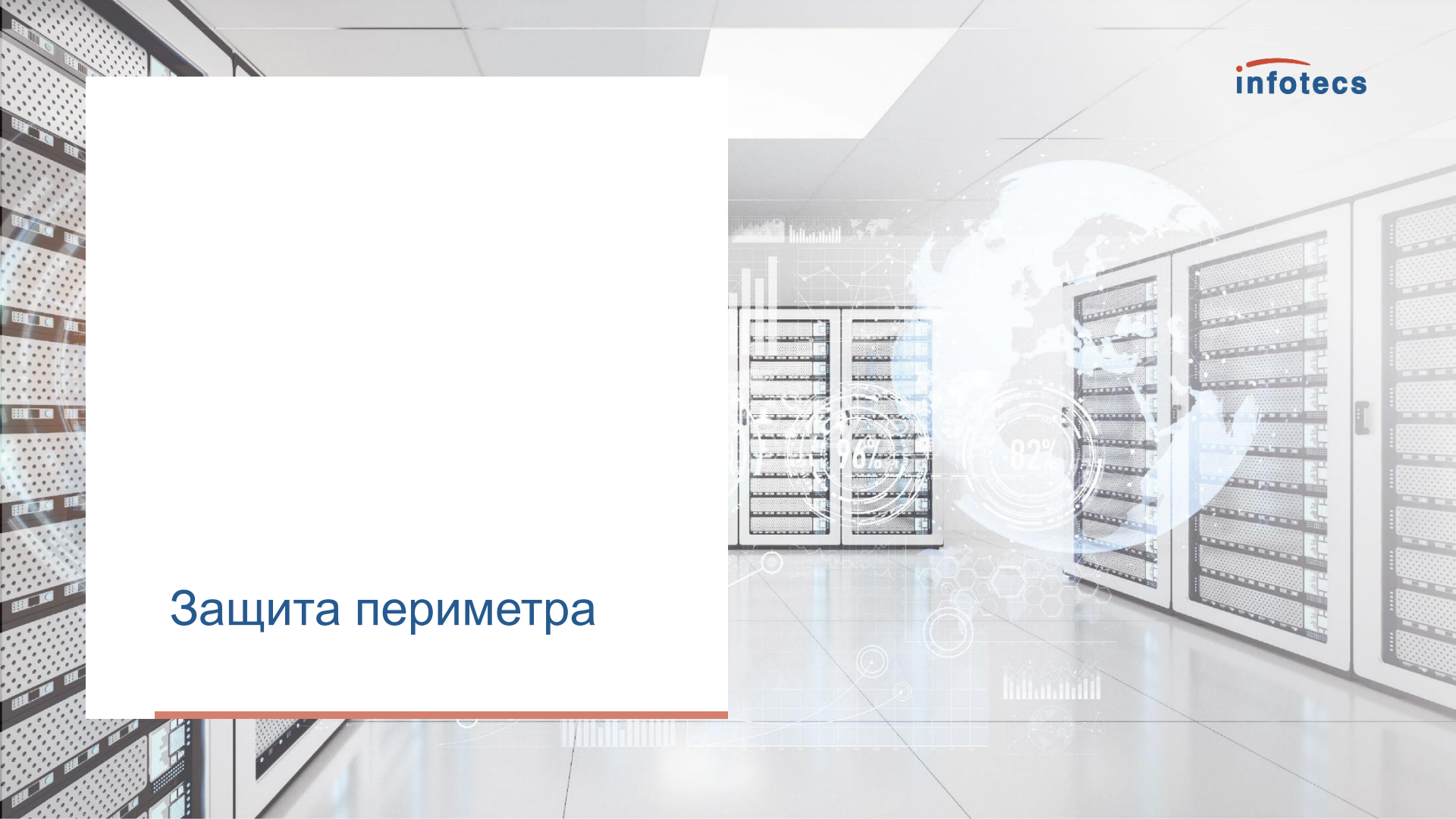
Социальная инженерия



Методы и подходы

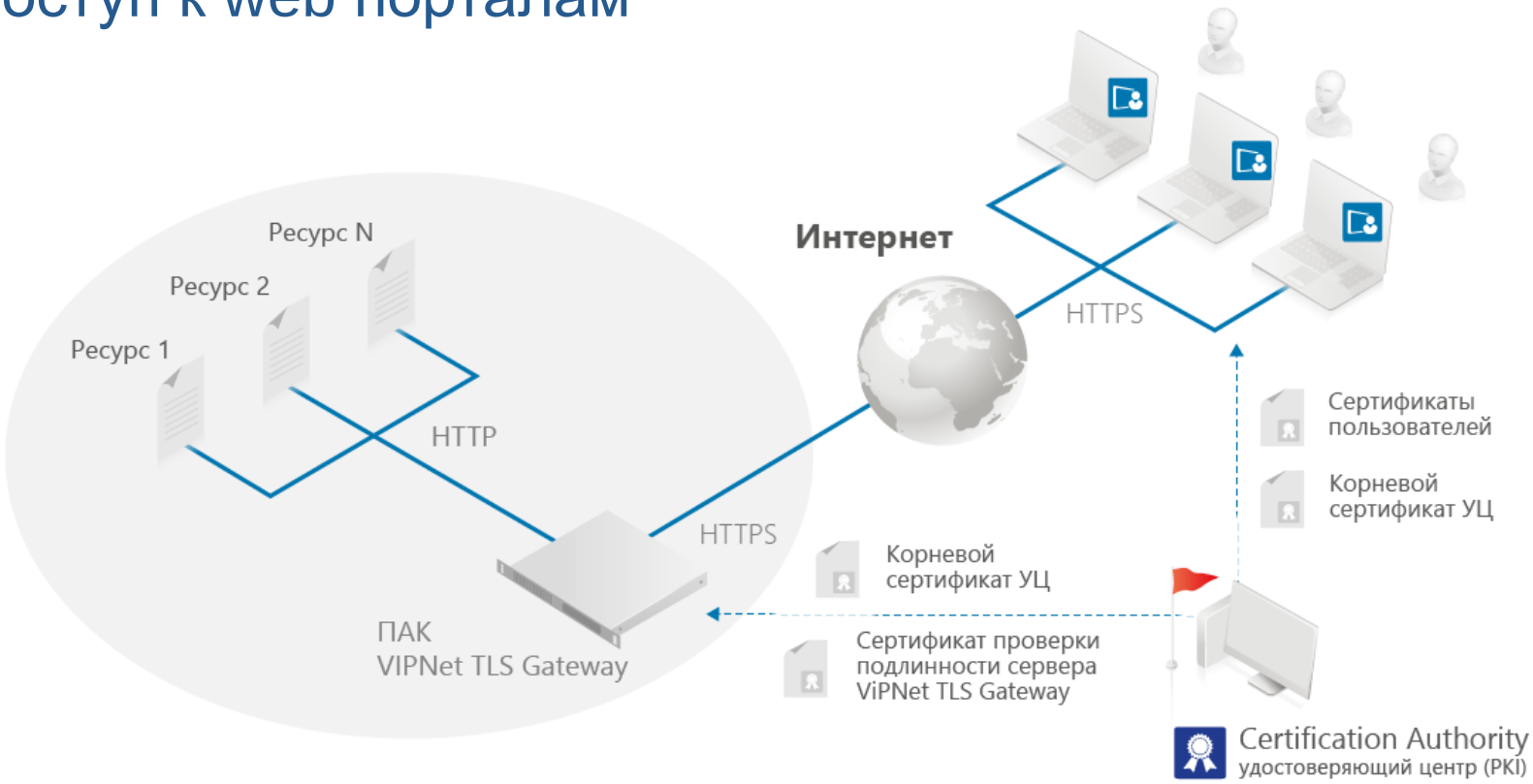
Подходы


Подходы
Домашний компьютер
Корпоративный ноутбук
Zero Trust
VPN
Минимум доступа
Управление политиками
EndPoint Security
Peer to Peer



Защита периметра

ViPNet TLS Gateway – доступ к web порталам

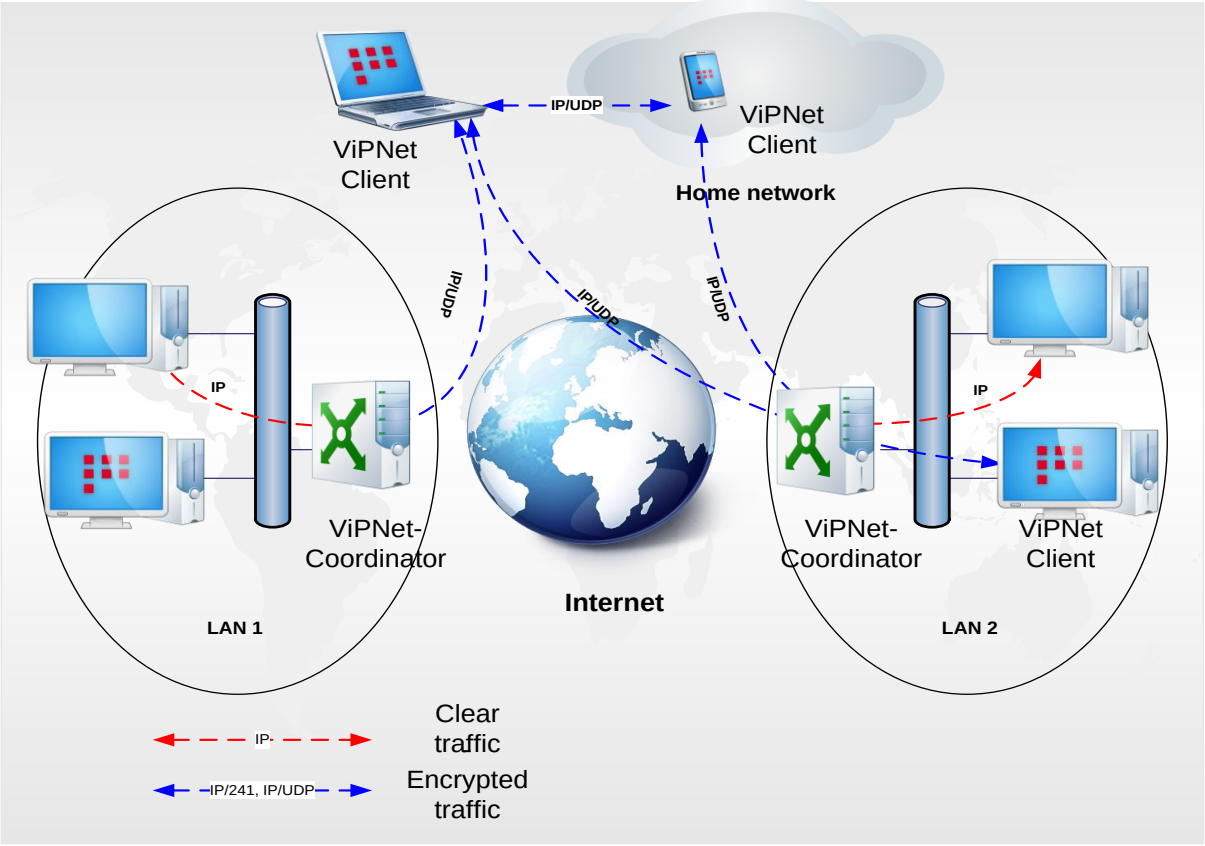


Защита каналов связи L4 VPN



- Совместная работа с ViPNet PKI Client
- Для протоколов RDP, SMTP, POP3, IMAP, WebDAV и др.

Удаленный доступ



- Межсетевой экран
- Stateful Packet Inspection
- NAT, Antispoofing
- Application Layer Gateway
- Proxy-server

- VPN Шлюз
- L3 VPN
- L2VPN (L2OverIP)
- Traversal NAT



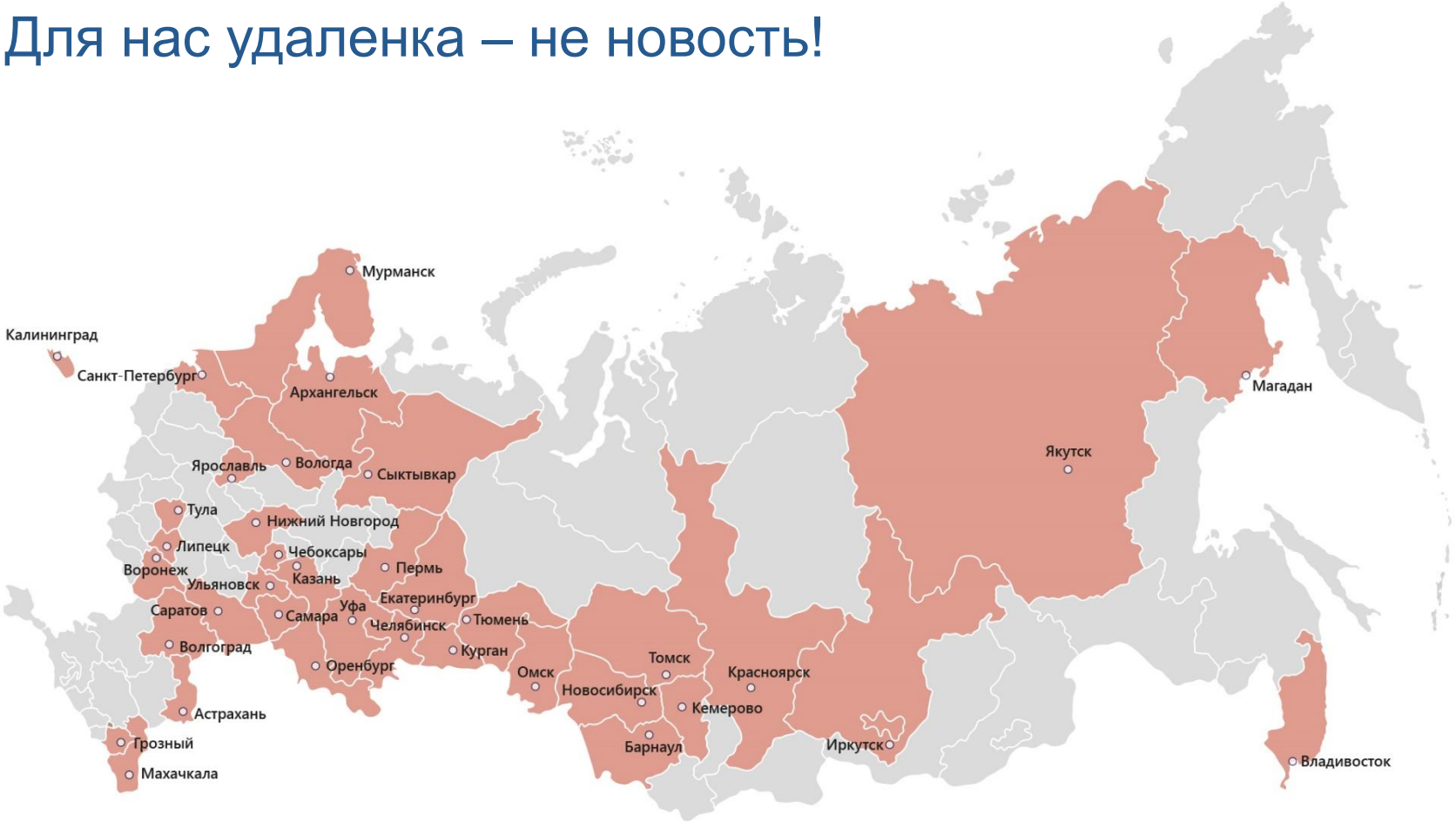
- Сетевые сервисы
- DNS server
- NTP-server,
- DHCP-server,
- DHCP-Relay
- VLAN, QoS support

- Транспортный сервер
- Горячей резерв (failover)

ViPNet TLS Gateway
или ViPNet Coordinator HW

Риски	TLS Gateway	HW
Терминальные сервера и другие ресурсы	Да	Да
Механизмы аутентификации (логин - пароль)	Да	Да
Служебные подключения к поддерживающим сервисам	Нет	Да
MITM	Да	Да
BYOD (политики, вредоносы)	Нет	Да
Мобильный доступ	Нет	Да
Не контролируемые работы в облаках	Нет	Да
Работы с ЭП	Нет	Да

Для нас удаленка – не новость!

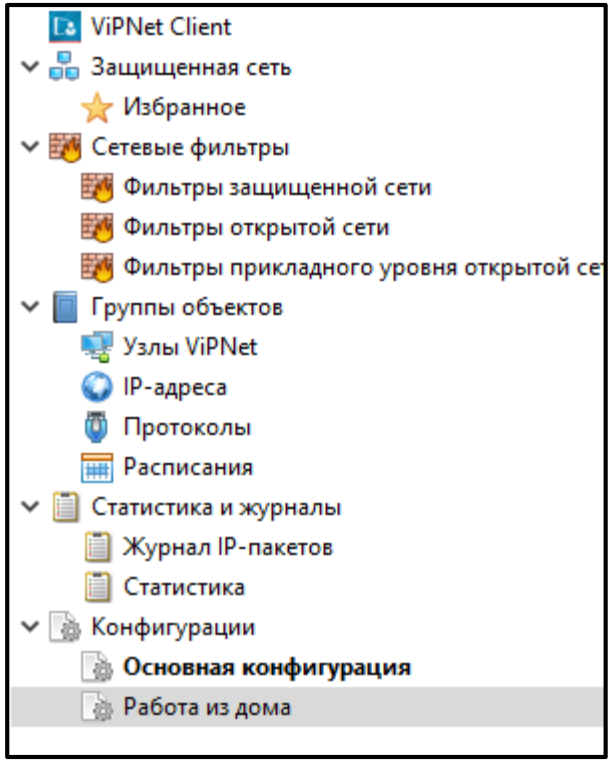


ViPNet Client это:

- VPN-клиент для работы в защищенных сетях ViPNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Поддерживает ОС Windows, Linux, MacOS, Android, iOS, Sailfish
- Имеет сертификаты ФСБ на СКЗИ по классам от КС1 до КС3

ViPNet Client for Windows | ViPNet Client for Linux | ViPNet Client for Android | ViPNet Client for iOS | ViPNet Client for MacOS | ViPNet Client for Sailfish

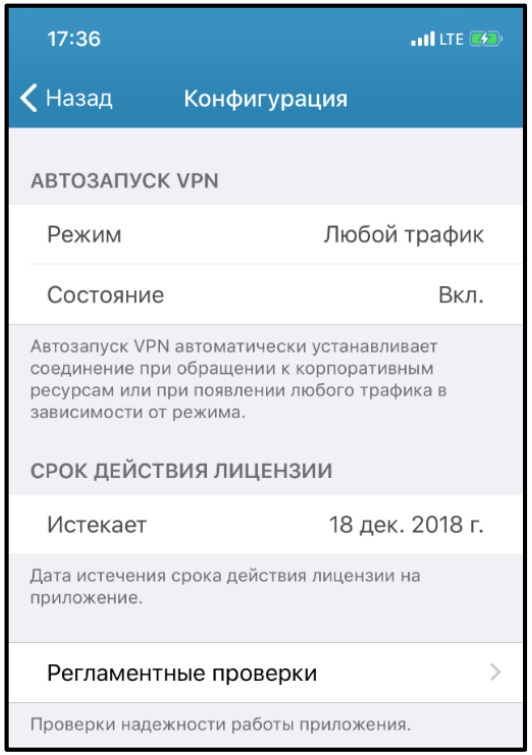
ViPNet Client: основные особенности



ViPNet Client позволяет настраивать уникальные шаблоны настроек и фильтров открытой и защищенной сети, называемых конфигурациями

Это позволяет одновременно использовать продукт как для работы с защищаемыми Ресурсами через закрытый канал, так и для работы с ресурсами сети интернет

ViPNet Client: основные особенности



Доступ к ресурсам корпоративной сети может быть организован с использованием доменных имен и защищенного DNS сервера

VPN включается автоматически после перезагрузки устройства, либо только при появлении определенного типа трафика или команды от внешнего приложения

При наличии в сети передачи данных факта блокировки UDP трафика провайдером, ViPNet Client автоматически перейдет на работу по протоколу TCP, портам 80 или 443

Обновление ключей шифрования проходит незаметно для пользователя.



Рабочее место сотрудника

VPN для организации RDP – обязательно! А что дальше?

- Для подключения к рабочему компьютеру большинство используют RDP по защищенному каналу
- НО подключение идет с домашнего компьютера
- Как найти компромисс с сотрудником по доверию к его домашнему компьютеру?



Домашний компьютер – коллективная собственность



Подключаемся к рабочему компьютеру, а там…

1. Стоит SafePoint, усилили политики!

Ограничиваем:

- установку дополнительного ПО пользователем
- запуск обновлений имеющегося ПО
- внесение изменений в значимые ветки реестра

2. Стоит ViPNet IDS HS, расширяем политики аудита.



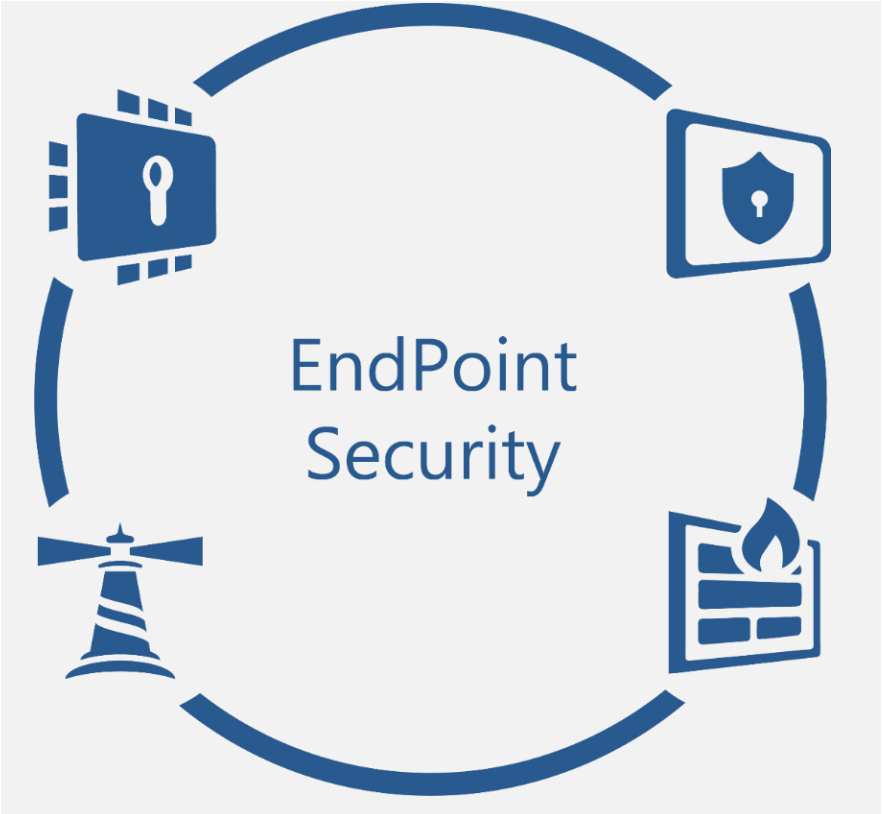
Организация выдала корпоративный ноутбук



Что мы используем для организации защиты Endpoint

В зависимости от сценария

- ViPNet SafePoint – классическое средство защиты информации от несанкционированного доступа
- ViPNet IDS HS – система обнаружения вторжений уровня хоста
- ViPNet SafeBoot – программное средство доверенной загрузки





Корпоративный ноутбук дома – объект желанный

- Отошли...
- Пошли помогать жене(мужу)
- Решили вечером отдохнуть

ОНИ тут как тут ☺

Надежно разграничим доступ и не оставим «ИМ» шанса



Установка ViPNet SafeBoot – не позволит никому кроме вас включить компьютер и быть уверенным в сохранности данных



Идентификация и аутентификация в ViPNet SafePoint – если компьютер был заблокирован или ушел в гибернацию.

Корпоративный ноутбук дома – это далеко за периметром защиты

ViPNet SafePoint:

- политик доступа к локальным и внутрикорпоративным ресурсам
- организация замкнутой программной среды
- разграничение доступа к принтерам
- наделение администратора ИБ полномочиями:
  - доступа к удалённой файловой системе без SMB
  - возможности чтения запущенных процессов
  - возможности принудительного завершения привилегированного процесса

ViPNet IDS HS:

- расширение политик аудита





infotecs

С защитой рабочих станций разобрались!
А что с коммуникациями?



infotecs

Защищенные коммуникации на удаленке

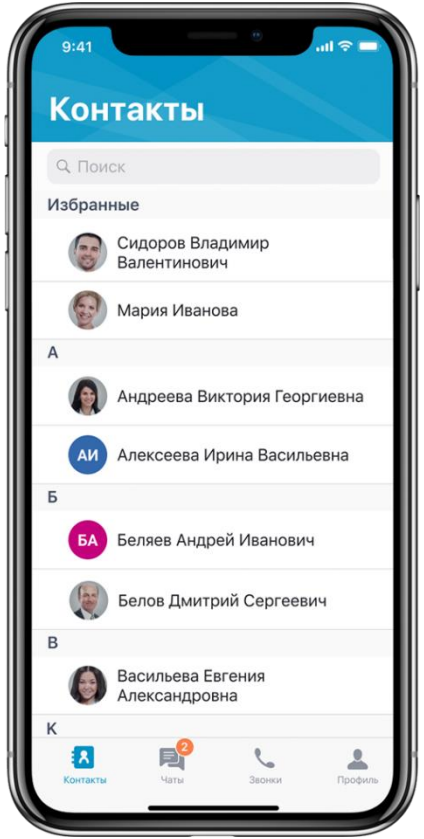
ViPNet Connect. Что это?



Изолированная система для организации защищенного контура корпоративных коммуникаций

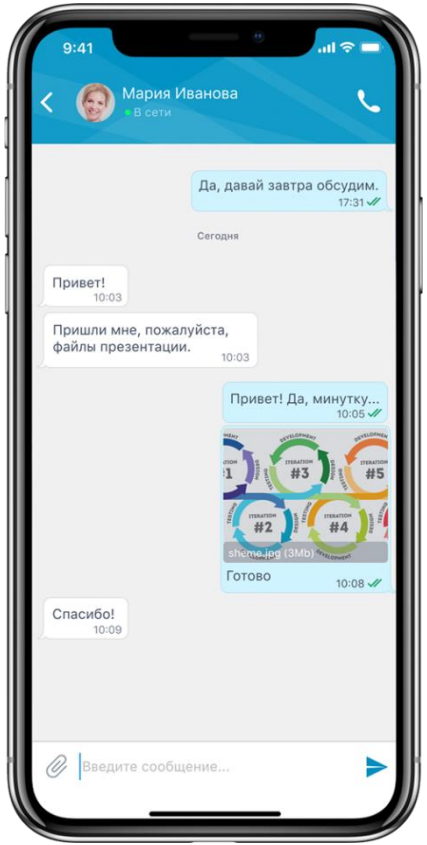
ViPNet Connect

ViPNet Connect обладает выделенной адресной книгой, которой управляет офицер безопасности, что исключает возможность непреднамеренной утечки информации



ViPNet Connect. Возможности

ViPNet Connect позволяет обмениваться любыми файлами без изменения их качества, организовывать чаты точка-точка, групповые чаты, рассылки, удобно цитировать и упоминать пользователей в переписке.



Поддержка популярных платформ

ViPNet Connect обладает интуитивно понятным интерфейсом и доступен для популярных платформ: **iOS, Android, Windows, macOS, Linux, Sailfish***



* в разработке

Интеграция с SIP инфраструктурой



ViPNet Connect обладает возможностью интеграции
с инфраструктурой доверенных SIP-серверов заказчика,
что позволяет встроить его в существующий контур IP-телефонии

ViPNet Connect. Как его используем мы

- Замена GSM телефона для ведения конфиденциальных переговоров
- Замена штатного IP телефона
- Внутрикорпоративный мессенджер
- Групповые чаты для различных задач
- Передача файлов и вложений
  без изменения их качества



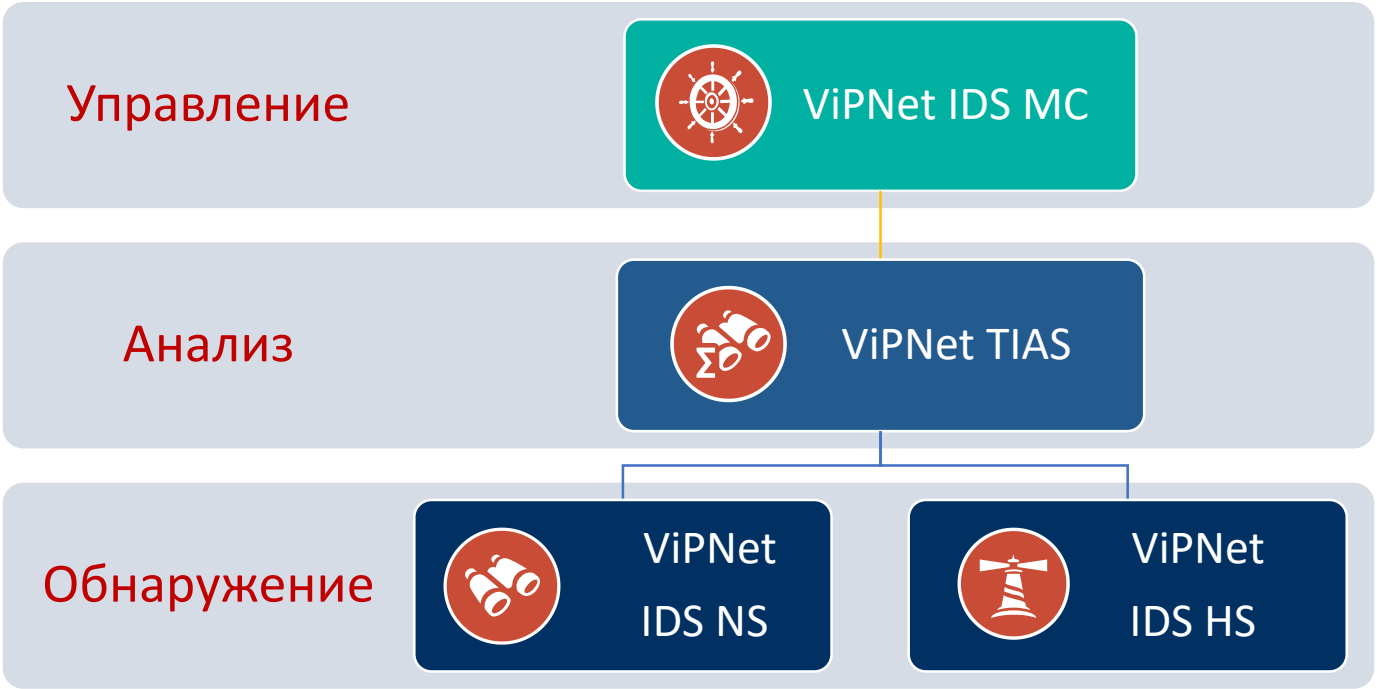
А как работать удаленно специалисту по ИБ?

А в чем проблема?

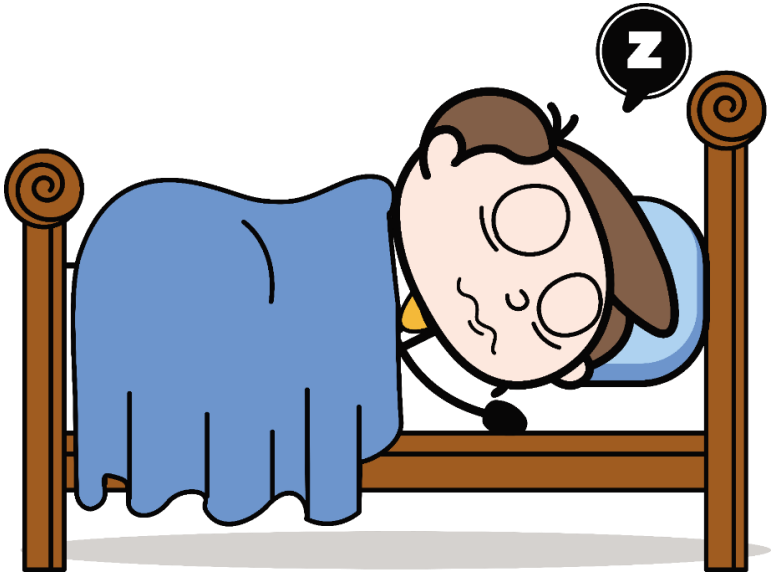


- Периметра нет
- Поверхность атак увеличена
- Недоверенные устройства в сети
- Удаленная работа самих специалистов ИБ

Решение Threat Detection & Response



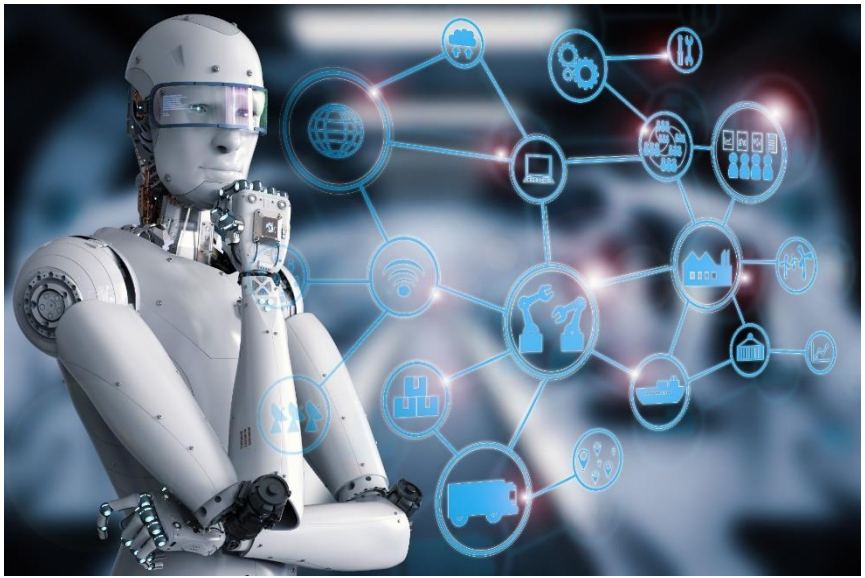
Солдат спит, служба идет



- Автообновление БРП и сигнатур
- Мониторинг работы сенсоров
- Автообновление экспертных данных

ViPNet IDS MC

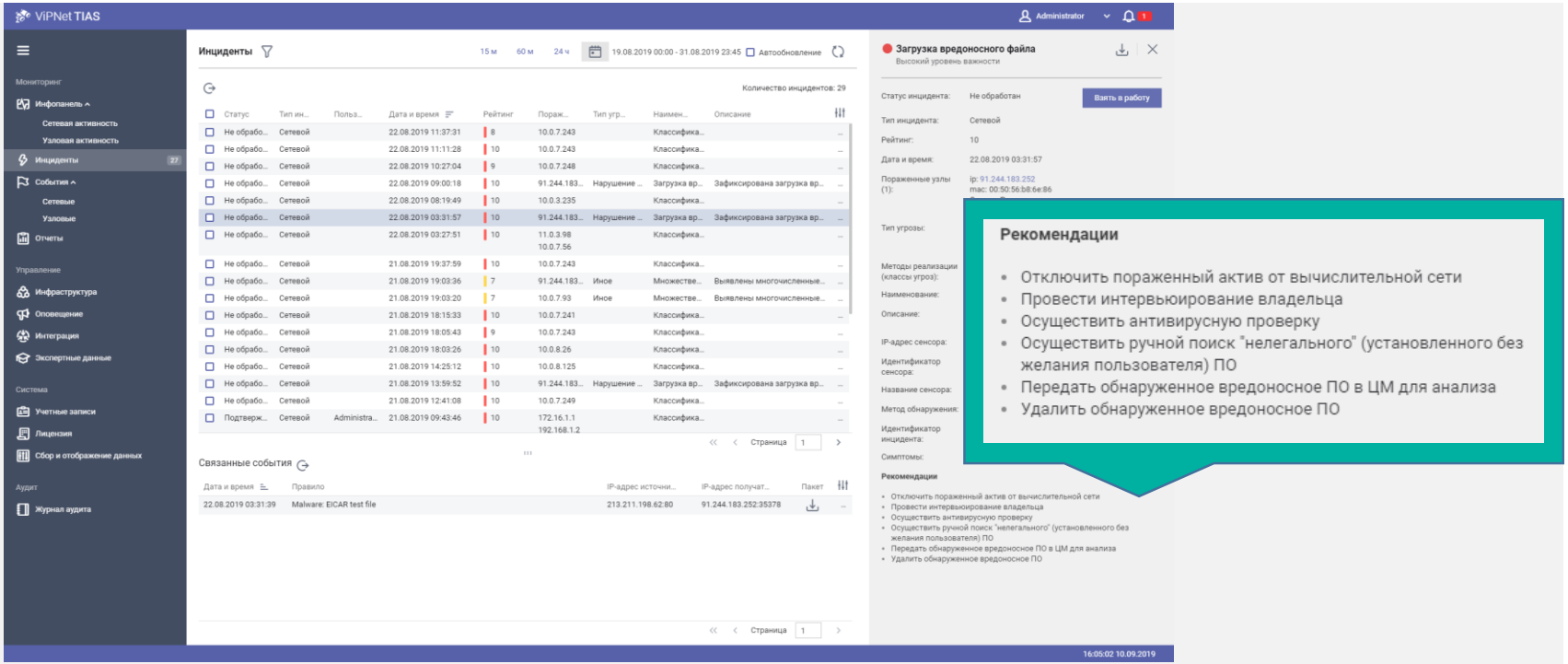
Пусть работает искусственный интеллект



- Настроен сбор событий от сенсоров
- Настроено автообновление экспертных данных
- Настроить уведомление об инцидентах по e-mail

ViPNet TIAS

А если есть только IT-специалист?



Рекомендации

- Отключить пораженный актив от вычислительной сети
- Провести интервьюирование владельца
- Осуществить антивирусную проверку
- Осуществить ручной поиск "нелегального" (установленного без желания пользователя) ПО
- Передать обнаруженное вредоносное ПО в ЦМ для анализа
- Удалить обнаруженное вредоносное ПО

Не можешь сделать сам – делегируй!



- 30+ операторов, исследователей и аналитиков
- 40+ организаций на мониторинге
- < 60 минут на отработку инцидента

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Реагирование

Вариант 1: домашний компьютер

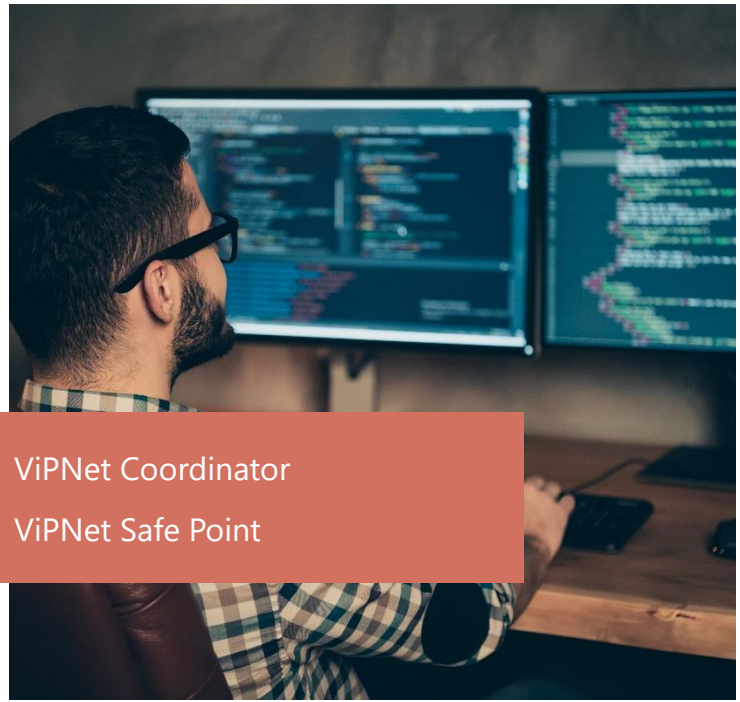
ViPNet Coordinator

межсетевой экран для домашних устройств с ViPNet Client

Вариант 2: корпоративный ноутбук

ViPNet Safe Point

- централизованное управление политиками
- полный доступ к компьютеру





Полезные ссылки

Вебинары

- Все вебинары вы можете найти на нашем сайте - https://infotecs.ru/webinars/archive/
- Обеспечение защиты рабочих станций и серверов продуктами ИнфоТеКС. Обзор новых версий продуктов направления Endpoint Security - https://youtu.be/lF11vhPIyn4
- Обзор продуктов ViPNet для клиентских платформ - https://youtu.be/4JnHZ8Jogao
- ViPNet Connect — как защитить свои корпоративные коммуникации - https://youtu.be/LCHbp4Tf3gw
- Социальная инженерия на практике. Проектный опыт «Перспективного мониторинга» - https://youtu.be/FWMSrBWEa5k

ИнфоТеКС предоставит на безвозмездной основе лицензии на свое ПО для организации защищенного удаленного доступа



- ПО ViPNet Client, ViPNet Connect, ViPNet IDS HS и ViPNet SafeBoot
- На безвозмездной основе на 6 месяцев
  - https://infotecs.ru/about/press-centr/news/infoteks-predostavit-litsenzii-na-svoe-po-dlya-organizatsii-udalennogo-dostupa-na-bezvozmezdnoy-osno.html

infotecs

Спасибо
за внимание!