
infotecs
ВЕБИНАР
УДАЛЕННАЯ
РАЗБОР ПОЛЕТОВ
РАБОТА

Призы для участников вебинара

За самый интересный вопрос

Внешний аккумулятор
на 5 000 mAh

За активное участие

Магнитный держатель для смартфона
в автомобиль и шторка для ноутбука

Основные сценарии организации удаленной работы и анализ по итогам двух месяцев

Алексей Данилов, руководитель направления продуктового развития ОАО «ИнфоТеКС»

infotecs

Мир изменился

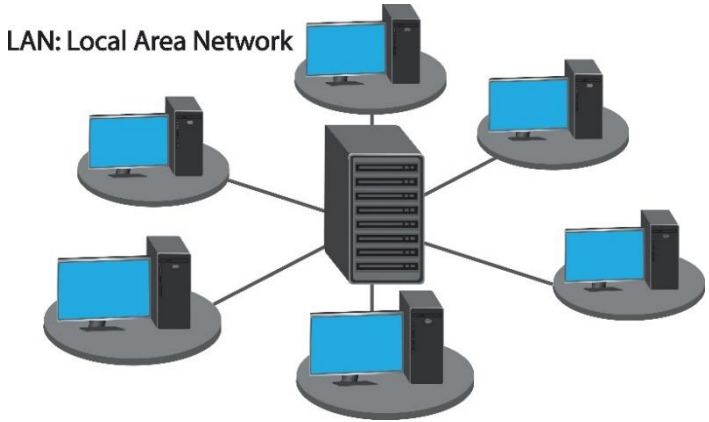
Давным-давно, примерно 11 недель назад…

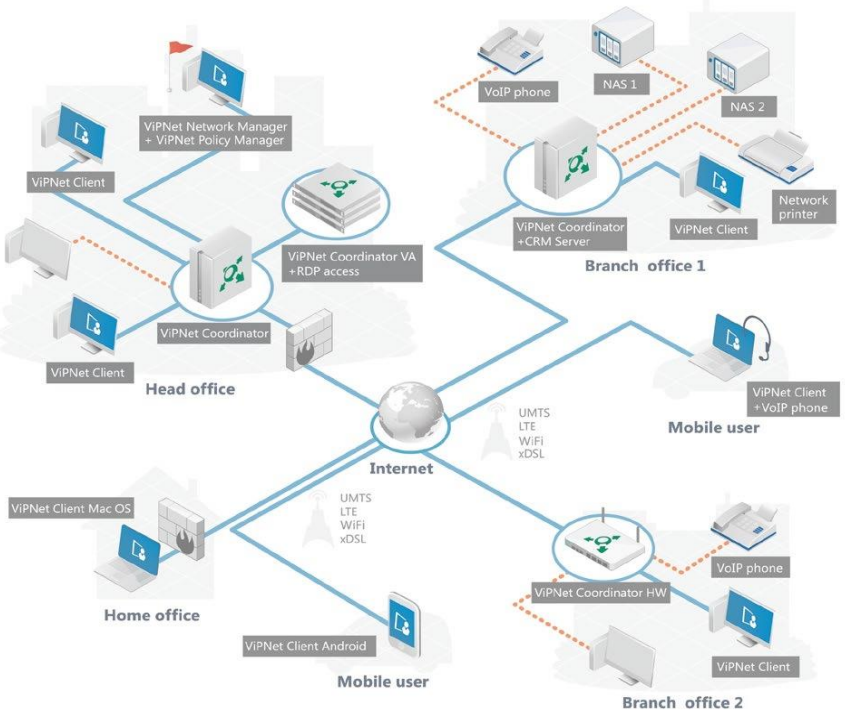
- Чтение блогов
- Facebook, VK, Одноклассники
- Twitter
- IM/WhatsApp
- Загрузка файлов (Dropbox, Яндекс.Диск)
- Потоковое видео (Youtube, Ivi)
- Потоковое аудио (Яндекс.Музыка)
- Качаем торренты
- Удаленный рабочий стол (TeamViewer, RDP)

Всех переводят на удалёнку

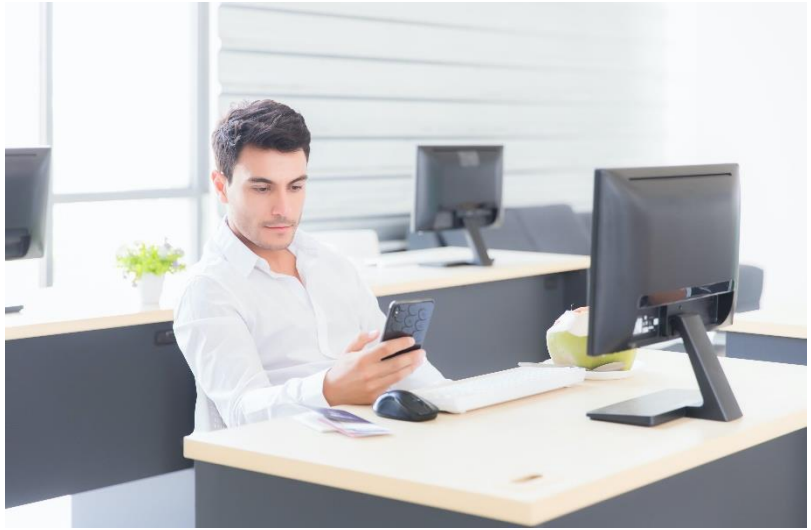
- 76% организации перевели 50 – 100% персонала на удаленный режим работы
- 44% при этом не использовали удаленный режим работы ранее
- А 17% справились с переводом за 1 день
- А 55% потратили на переход от 2 до 5 дней

44% опрошенных планируют сохранить режим удаленной работы





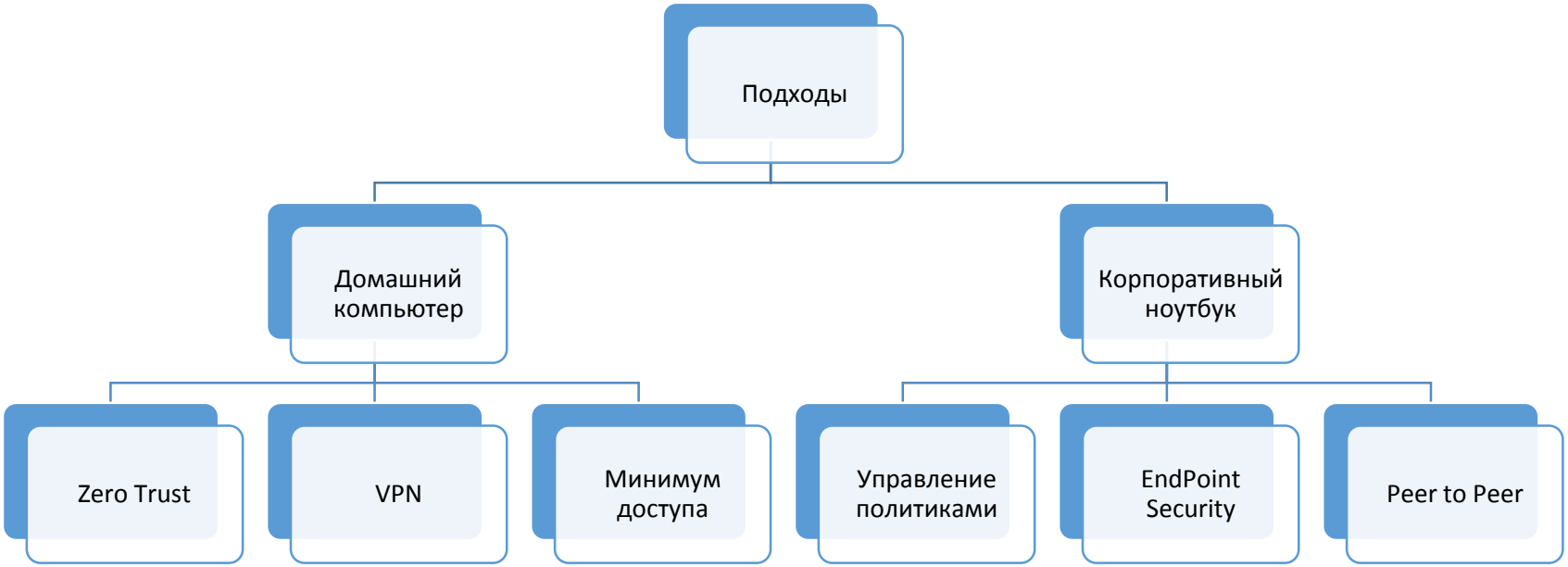
Личное или корпоративное устройство

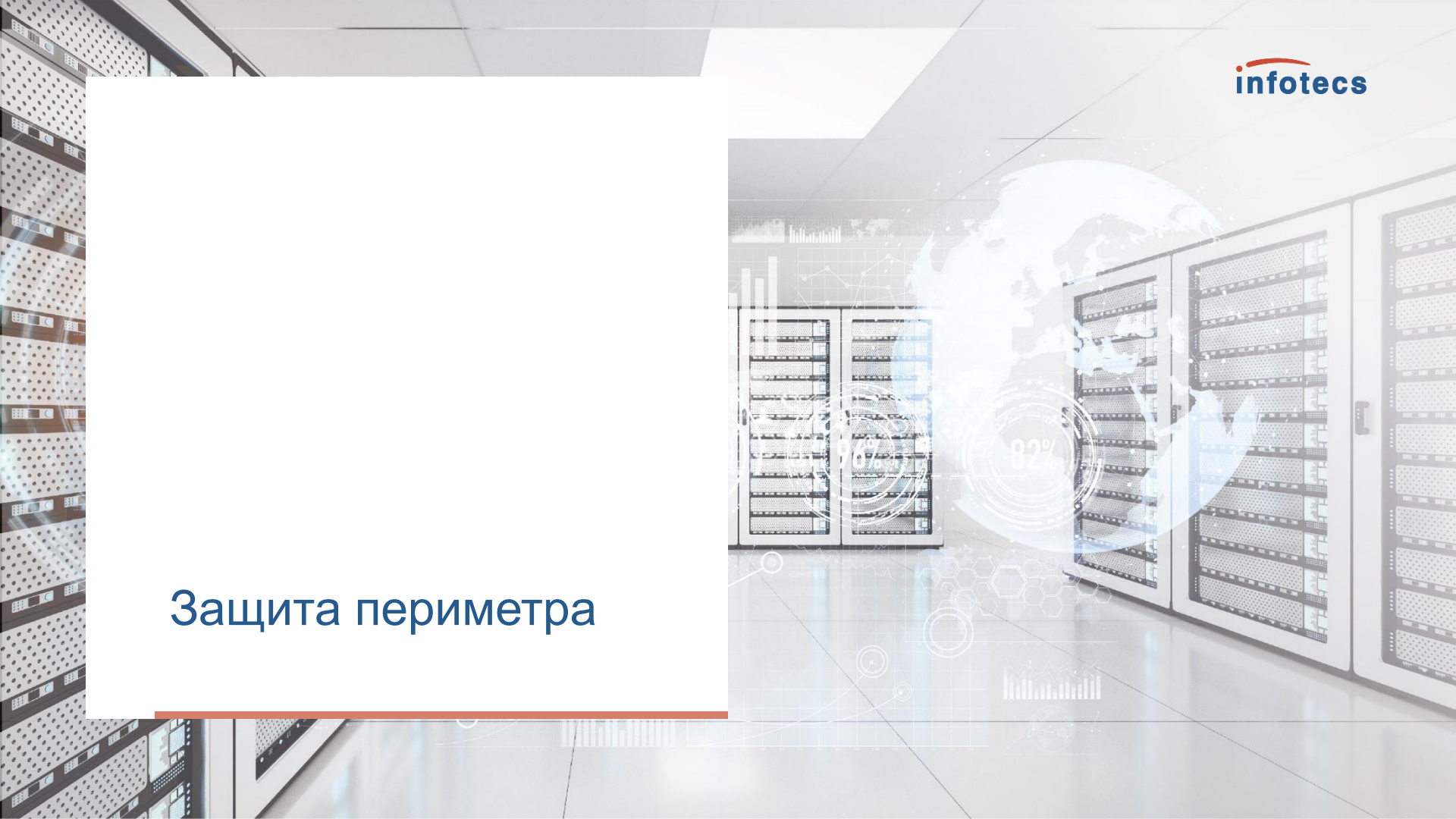


15% используют только личные устройства

18% используют только корпоративные устройства

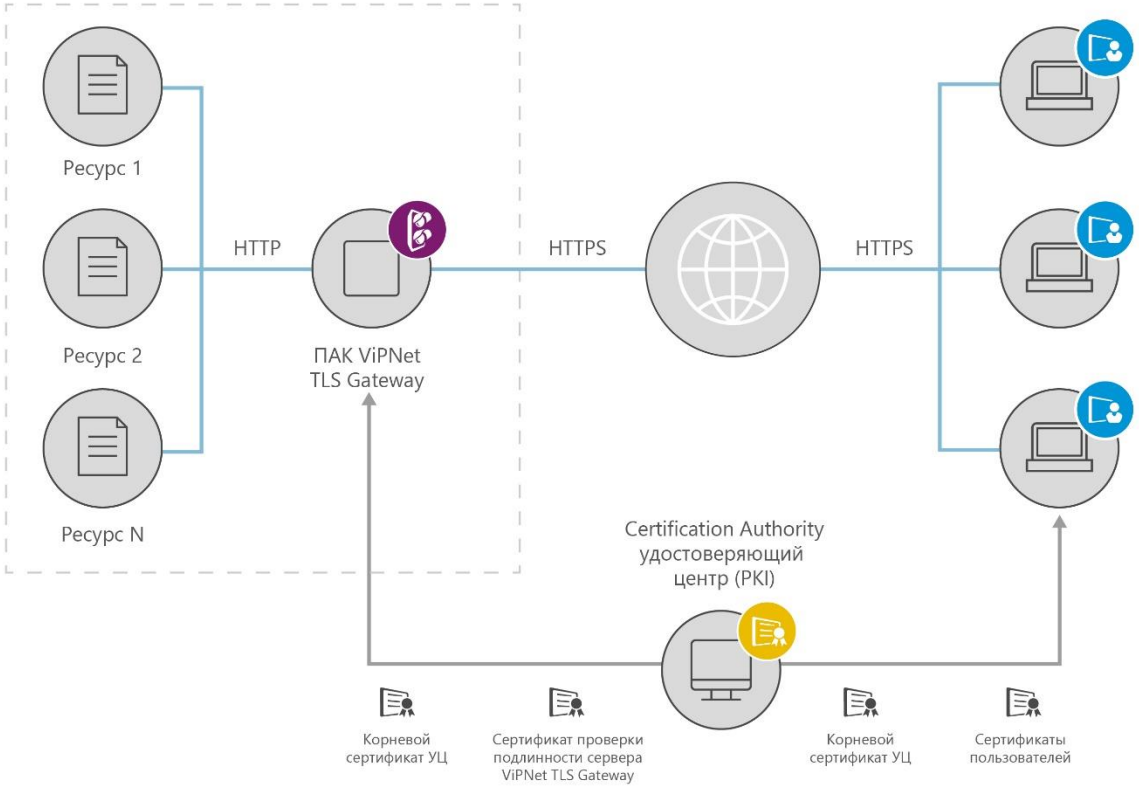
Подходы


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



Защита периметра

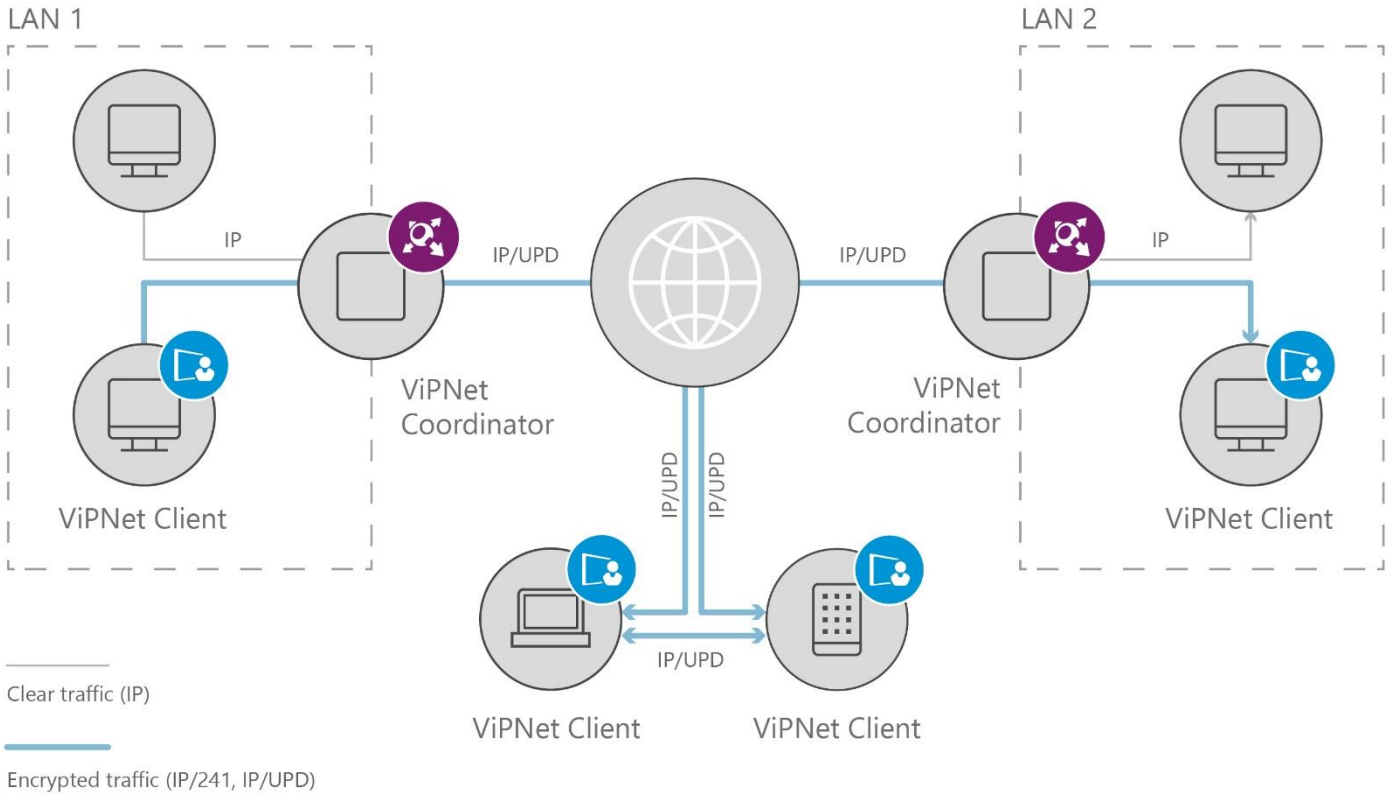
ViPNet TLS Gateway – доступ к web порталам



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
- Горячий 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

12% не используют VPN

50% используют web-доступ

infotecs

ViPNet Client

Пользовательский опыт

11% столкнулись с необходимостью обучать сотрудников

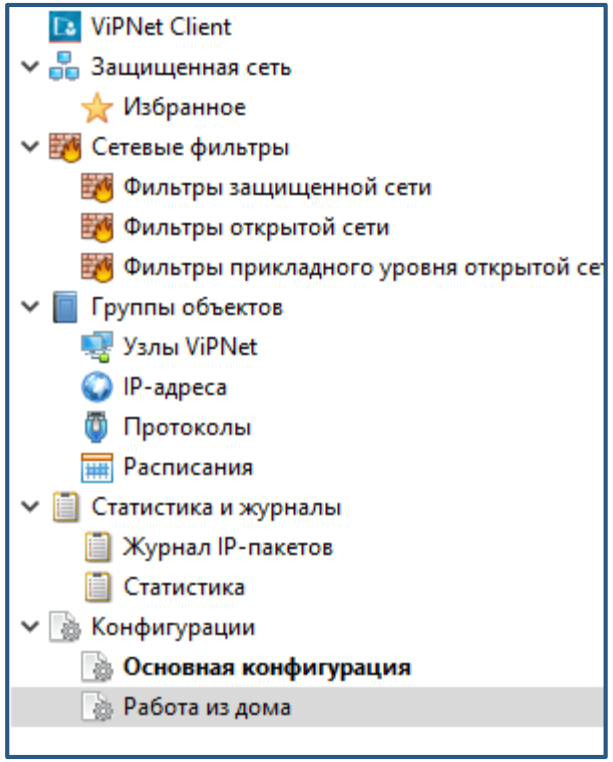
6% столкнулись с проблемами с сетевым подключением – wi-fi, плохие каналы связи и тд

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

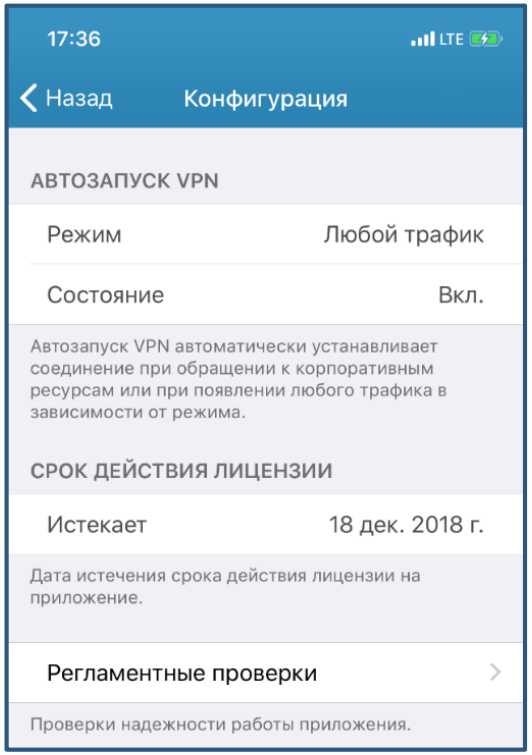
ViPNet Client: основные особенности



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?
- 26% не устанавливают дополнительные СЗИ на домашние компьютеры

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

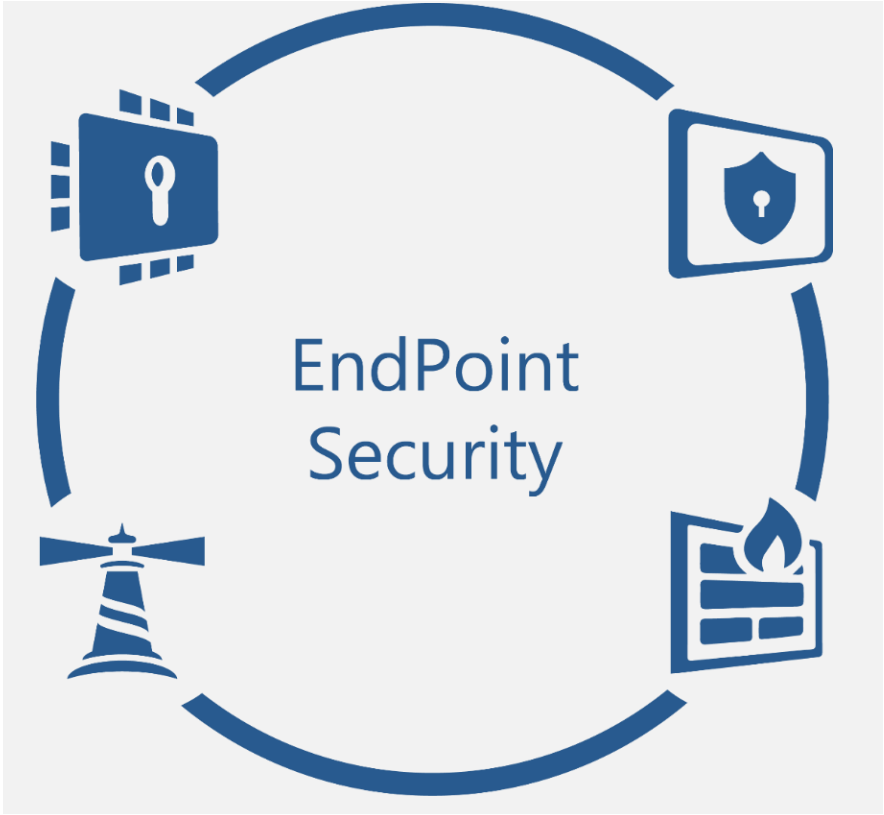
Что мы используем для организации защиты Endpoint

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

26% используют СЗИ от НСД

30% используют хостовые СОА/СОВ



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:

- политика 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?

41% используют корпоративные мессенджеры

44% используют облачные мессенджеры

6% используют ViPNet Connect

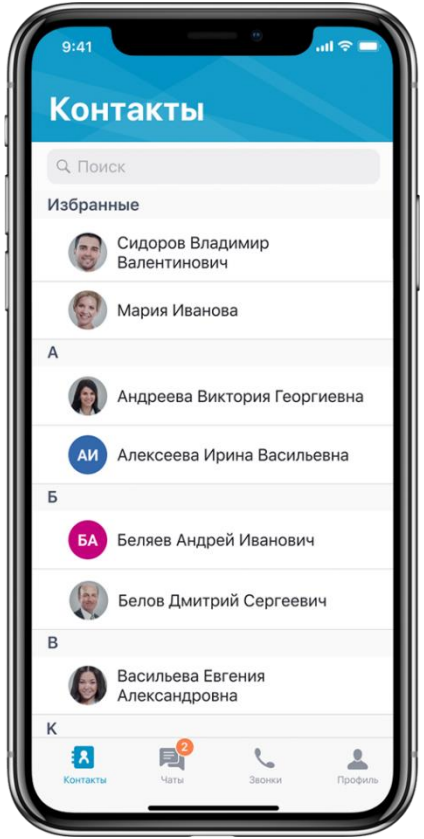
Защищенные коммуникации на удаленке

ViPNet Connect. Что это?

Изолированная система для организации защищенного контура корпоративных коммуникаций

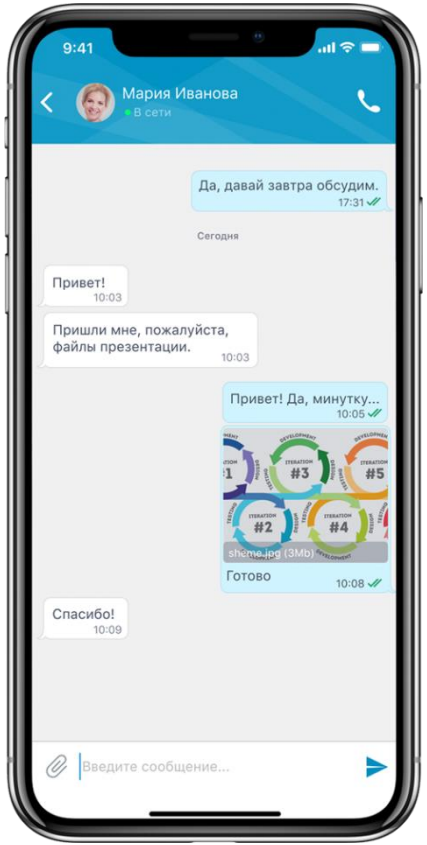
ViPNet Connect

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

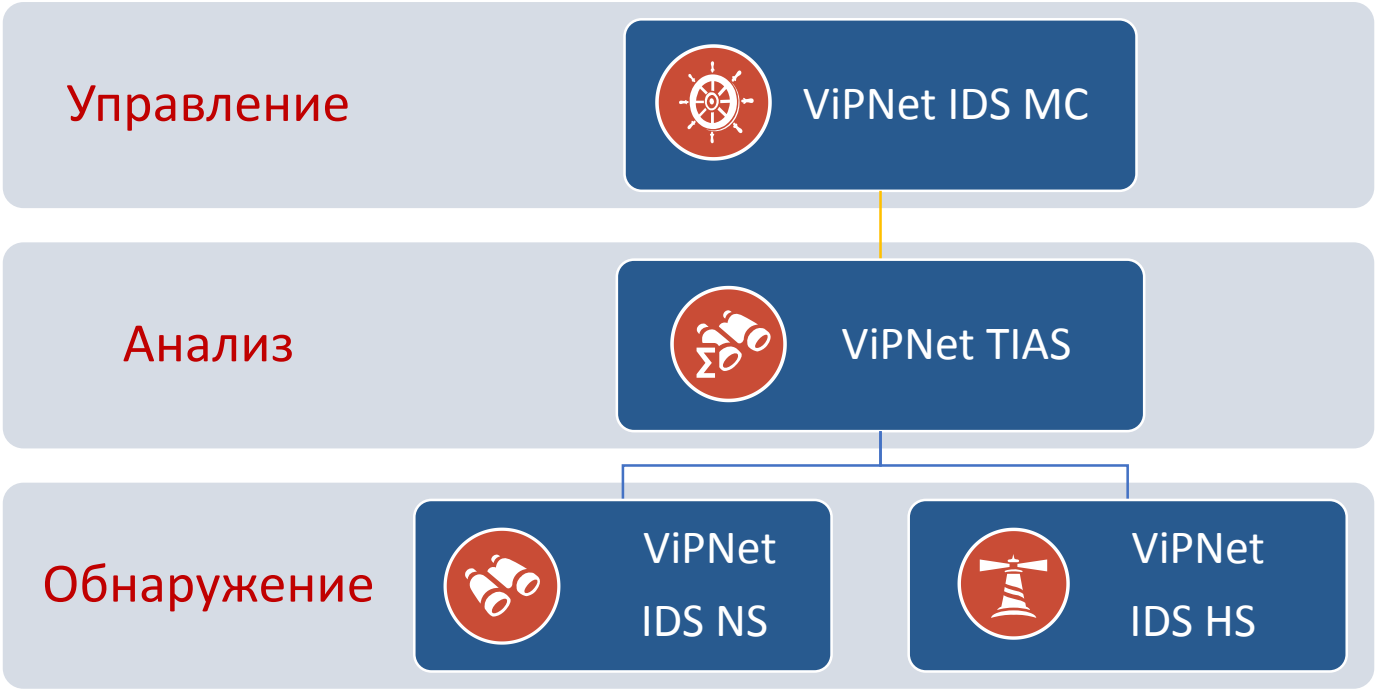
- Замена GSM телефона для ведения конфиденциальных переговоров
- Замена штатного IP телефона
- Внутрикорпоративный мессенджер
- Групповые чаты для различных задач
- Передача файлов и вложений без изменения их качества

А как работать удаленно специалисту по ИБ?

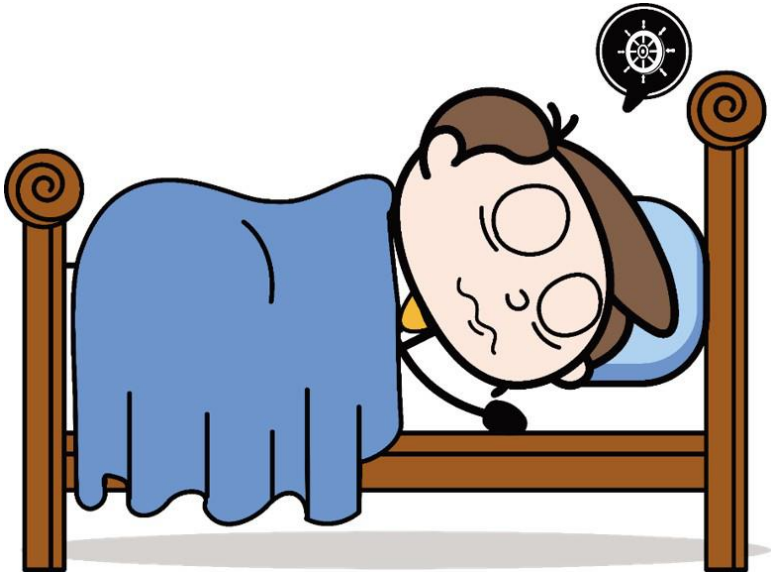
А в чем проблема?

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

Решение Threat Detection & Response



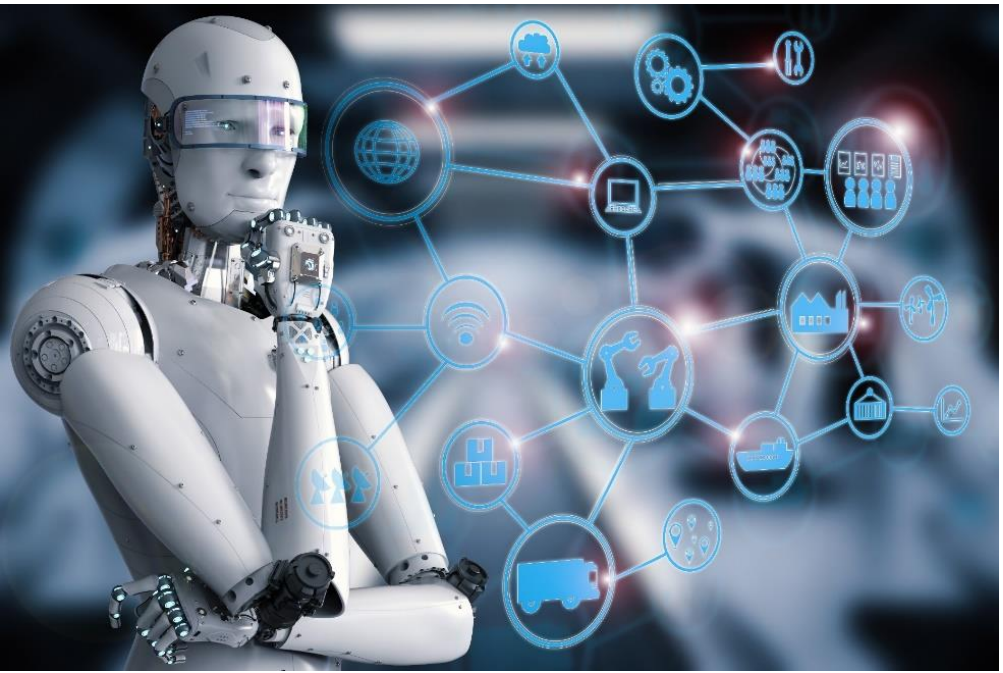
Солдат спит, служба идет



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

ViPNet IDS MC

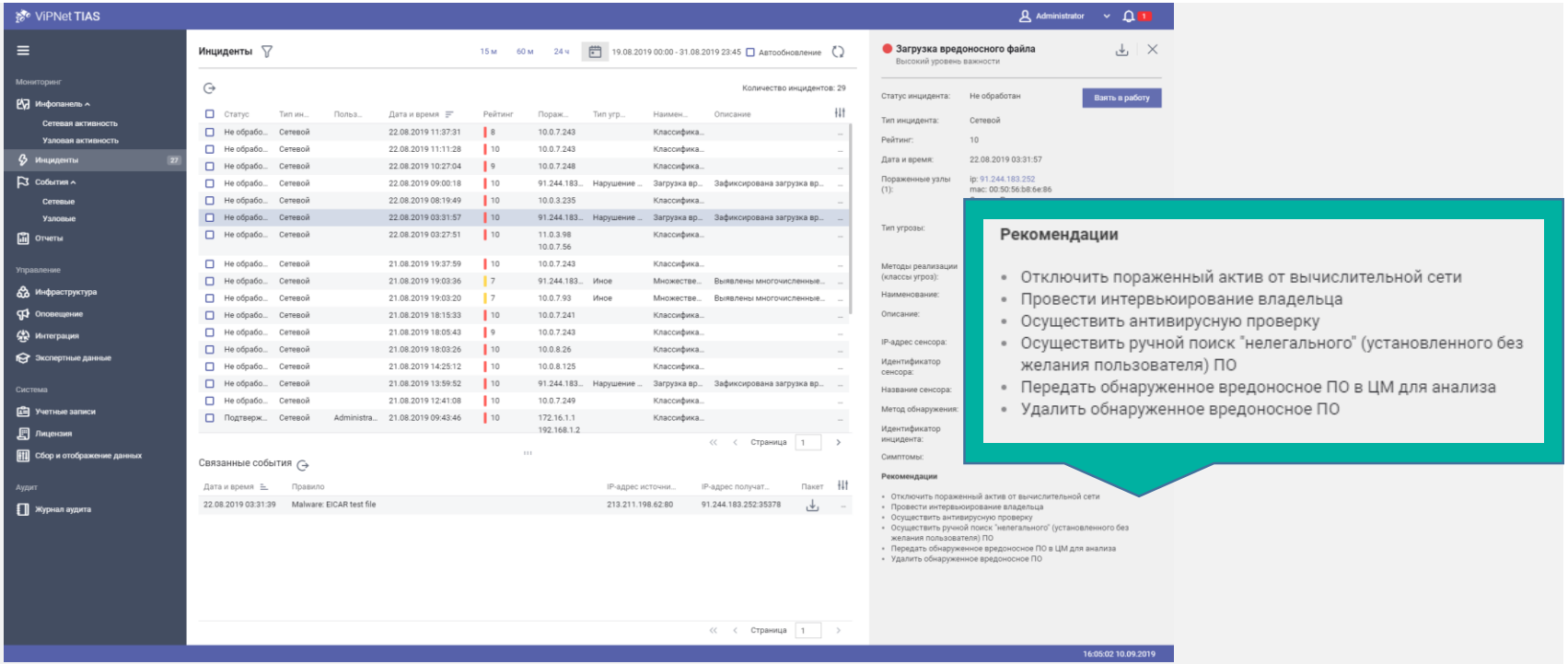
Пусть работает искусственный интеллект



- Настроен сбор событий от сенсоров
- Настроено автообновление экспертных данных
- Настроено 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
- 20 организаций на мониторинге
- < 60 минут на отработку инцидента

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Реагирование

Вариант 1: домашний компьютер

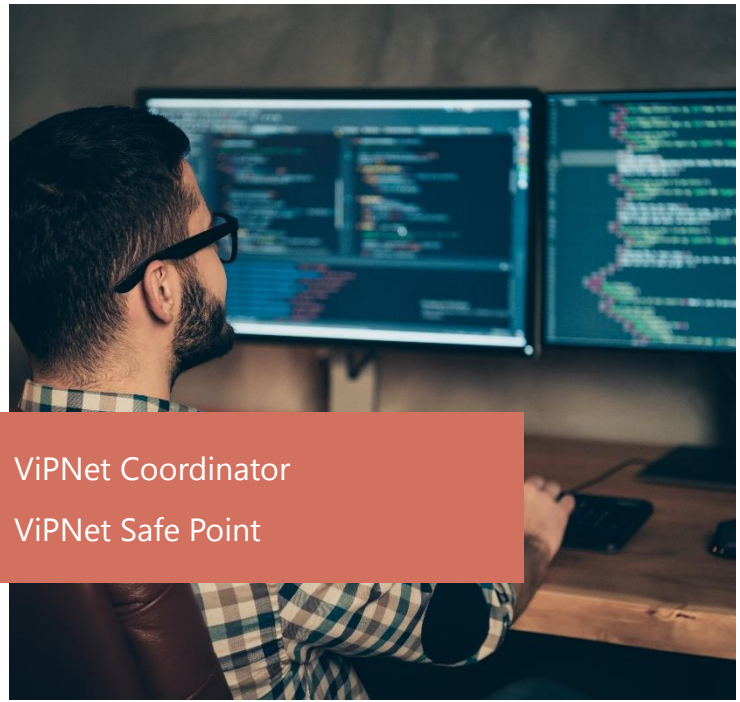
ViPNet Coordinator

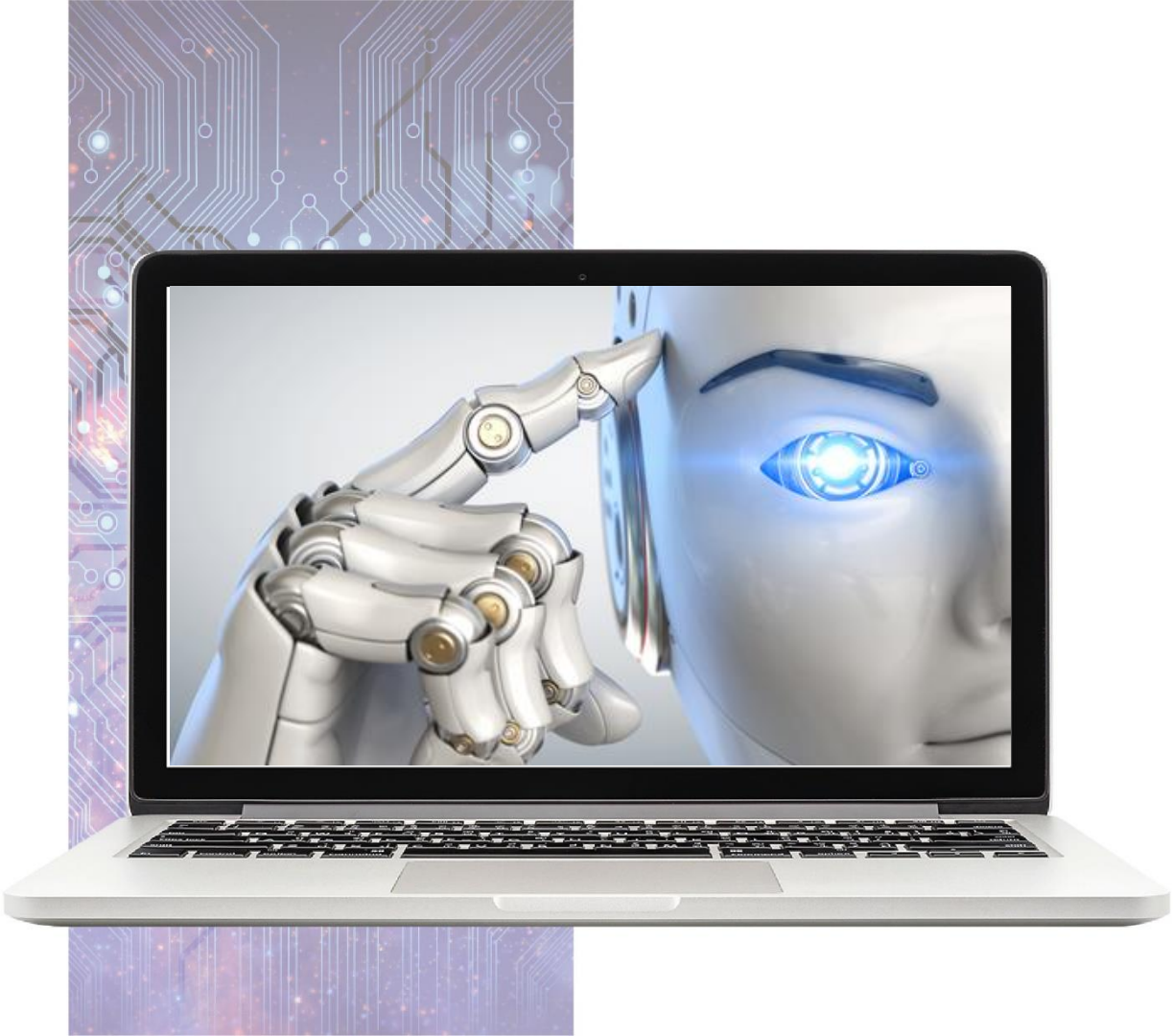
межсетевой экран для домашних устройств с ViPNet Client

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

Лицензии, предоставленные на безвозмездной основе для организации безопасного удаленного доступа

ITDP	Network Security	PKI	Security Connection	End Point Protection
				
72	**828 541**	**265 776**	**7 188**	**19 937**

Общий итог 1 121 514 лицензий

на сумму 4 511 368 320* р.

***по ценам для конечного пользователя согласно действующему прайс-листу компании**

Период 15 марта – 20 мая 2020 года

infotecs

Спасибо
за внимание!

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Анализ событий и инцидентов информационной безопасности за два месяца удалённой работы

Сергей Нейгер

Менеджер по развитию бизнеса

«Перспективный мониторинг»

Повестка встречи

1. О Центре мониторинга
2. Как работает Центр мониторинга
3. Пусть говорят
4. Наши наблюдения

Мы вторые.

Это значит, что мы больше стараемся.

Сравнение услуг коммерческих SOC. Anti-malware.ru, конец 2019 года

Центр мониторинга

2014
год запуска

с 2017
Центр ГосСОПКА к. А

17
клиентов

30
операторов, исследователей, аналитиков и инженеров

Площадки:
Москва
Санкт-Петербург
Новосибирск

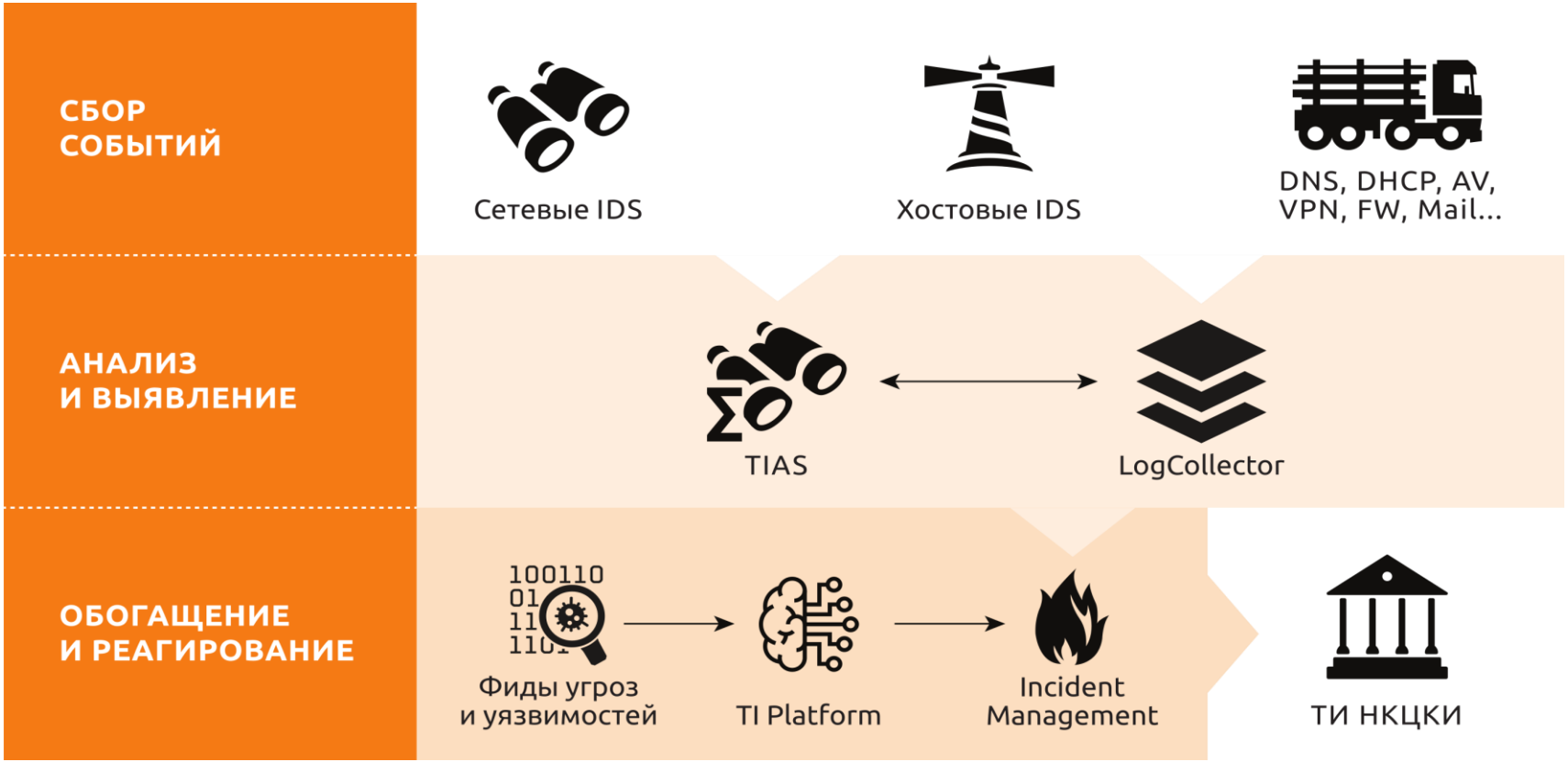
1,5 млрд
событий за 2019 г.

1 400
инцидентов за 2019 г.

13 000
собственных сигнатур атак для IDS

Чиорт пабери! (от без. «Инциденты случаются»)

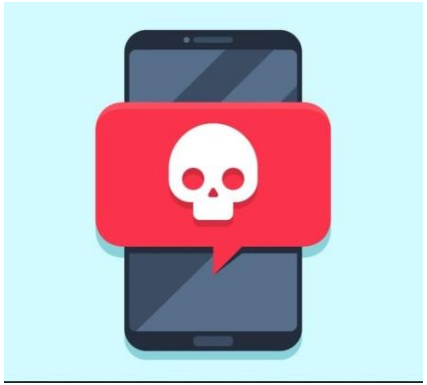
Схема подключения

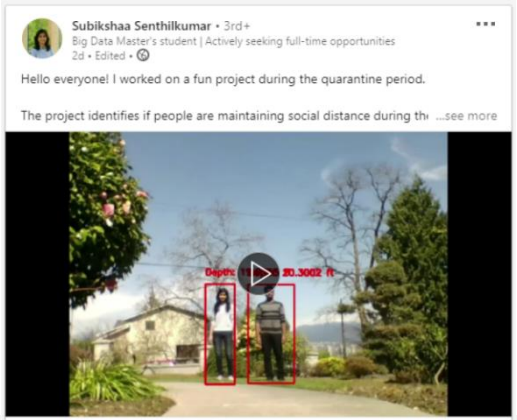


Пусть говорят

Все говорят

DIGITAL IMAGE. A Zoom session was disrupted by a hacker sharing x-rated footage. Credit: 7NEWS.com.au





PT говорит

1. Выросли спрос и предложение на доступы(«Средняя стоимость привилегированного доступа к локальной сети сейчас составляет порядка 5000 долларов»).
2. Только в 1/10 компаний пандемия стала поводом перейти на удалёнку.
3. В 80% компаний хотя бы часть сотрудников используют домашние компьютеры и ноутбуки.
4. Чуть больше половины опрошенных не планируют менять схемы удалённого доступа.

R-S говорит

1. Больше корпоративных серверов доступны из Интернета. Рост брутфорса.
2. Количество устройств, доступных по RDP

   ↑ Россия 15% ↑ Мир 20% (начало марта). Но RDP — основной вектор начала атак.
3. Структура типов атак не поменялась по сравнению с прошлым полугодием (по моему мнению).
4. Вектор атак сместился на удалённых пользователей.
5. Можно рассматривать варианты постоянной удалёнки.

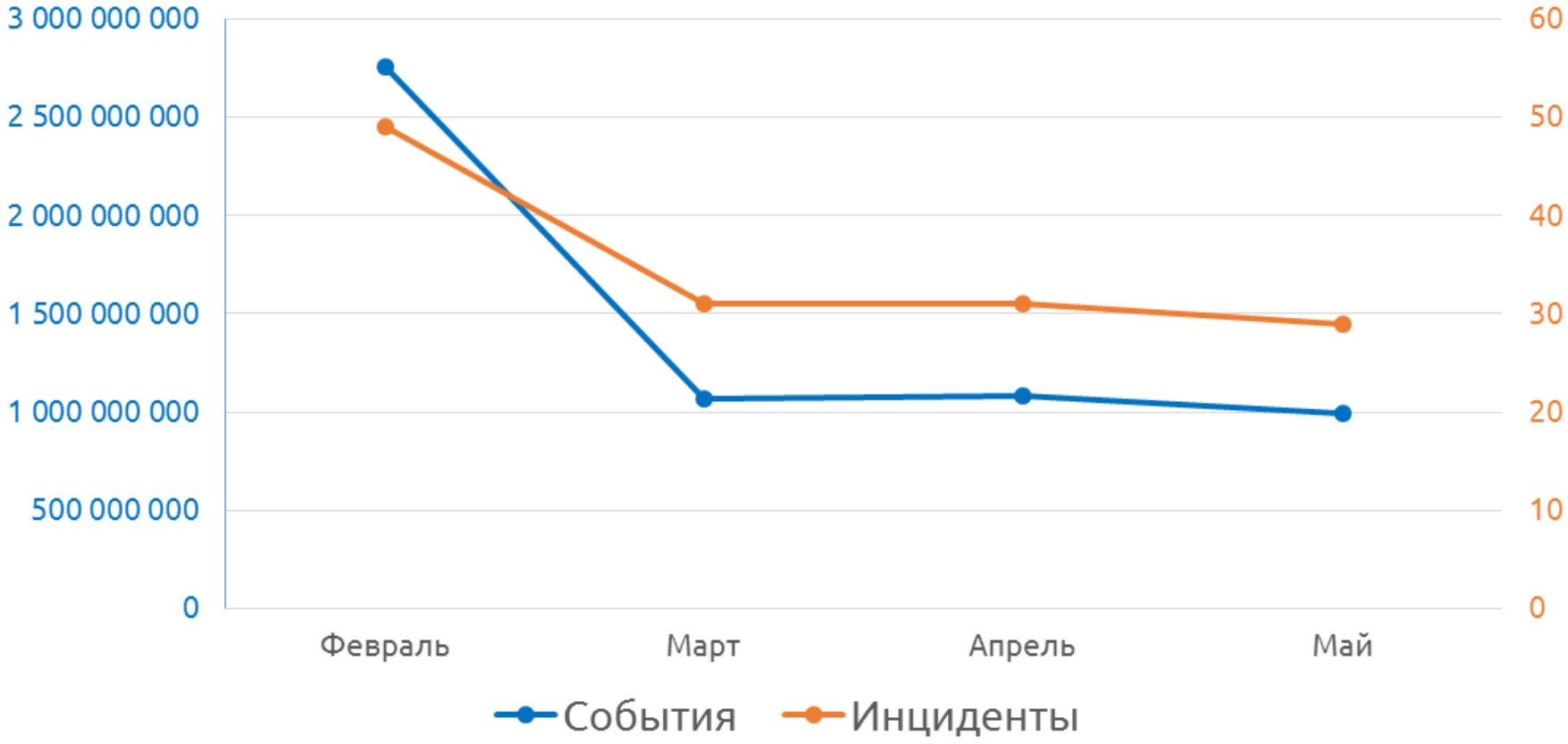
ПМ говорит

Наш календарь на 2020

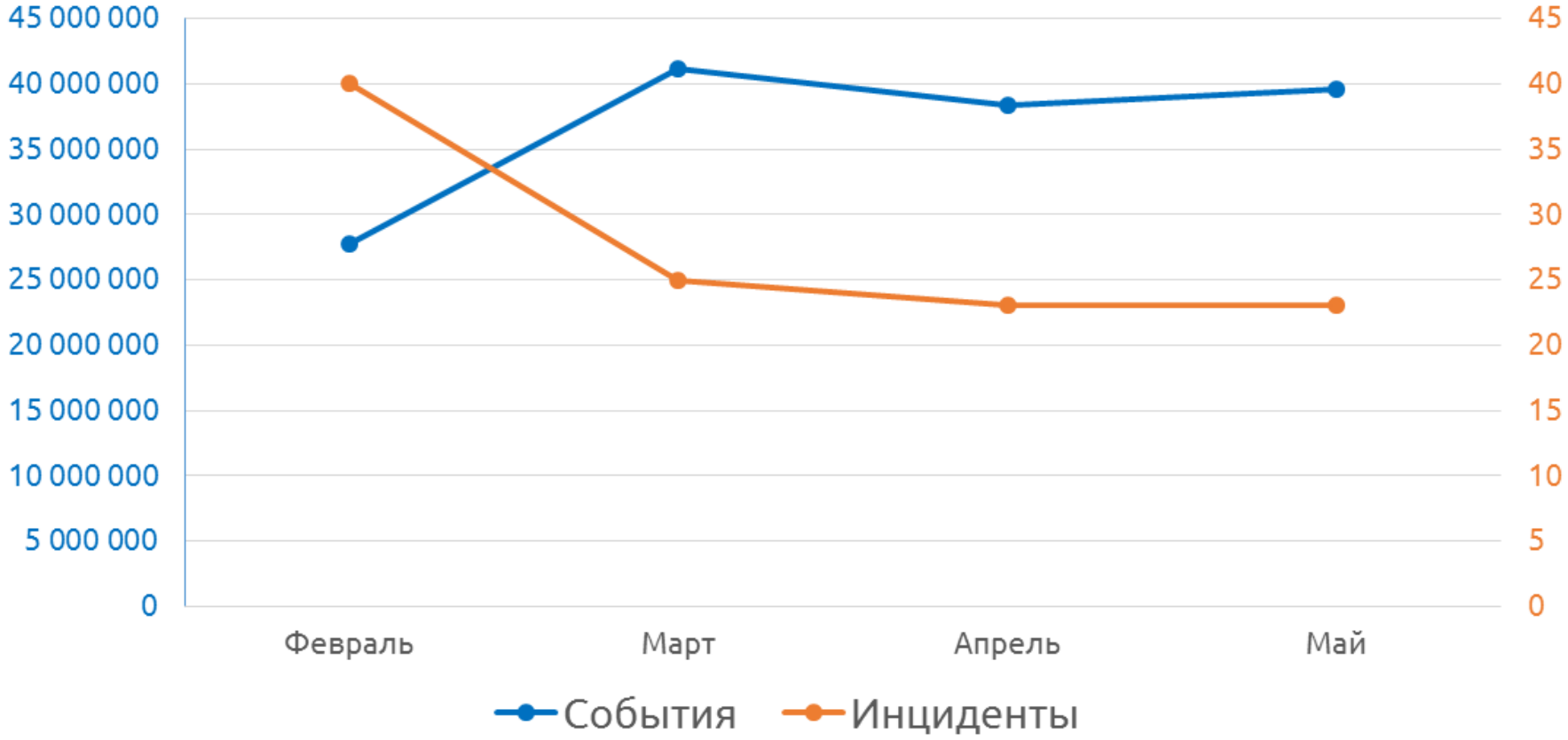
ПМ говорит

1. Количество событий ИБ не возросло (в ¾ случаях даже снижение на 15–40%).
2. По одному из заказчиков был 1 млрд, стало 800 млн.
3. Начиная с апреля ситуация январская.
4. В целом картина по структуре событий и инцидентов не поменялась.

Февраль – Май


3 000 000 000
2 500 000 000
2 000 000 000
1 500 000 000
1 000 000 000
500 000 000
0
60
50
40
30
20
10
0
Февраль
Март
Апрель
Май
События
Инциденты

Без ИнфоТеКСа



С чем это связано

Проблемы теперь дома

Не всем дали доступ

Скорость реакции снизилась

Спасибо за внимание!

И накатите патчи!

Сергей Нейгер

Менеджер по развитию бизнеса

компании «Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru





Алексей Данилов

Руководитель направления
продуктового развития ОАО «ИнфоТеКС»
danilov@infotecs.ru

Сергей Нейгер

Менеджер по развитию бизнеса
компании «Перспективный мониторинг»
Sergey.Neyger@amonitoring.ru

Призы для участников вебинара

За самый интересный вопрос

Внешний аккумулятор
на 5 000 mAh

За активное участие

Магнитный держатель для смартфона
в автомобиль и шторка для ноутбука