Импортозамещение на базе продуктов ViPNet

Классические и новые сценарии

Александр Реунов

infotecs

Группа компаний «ИнфоТеКС»

infotecs

infotecs

infotecs
УЧЕБНЫЙ ЦЕНТР

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

прокси

Единый Медицинский Портал

СФБ ЛАБ

ПроКвантТ

+10%

8,6 млрд рублей в 2022

ИнфоТеКС в цифрах

В **Топ-10**
компаний в сфере защиты информации в России

9
офисов по всей стране

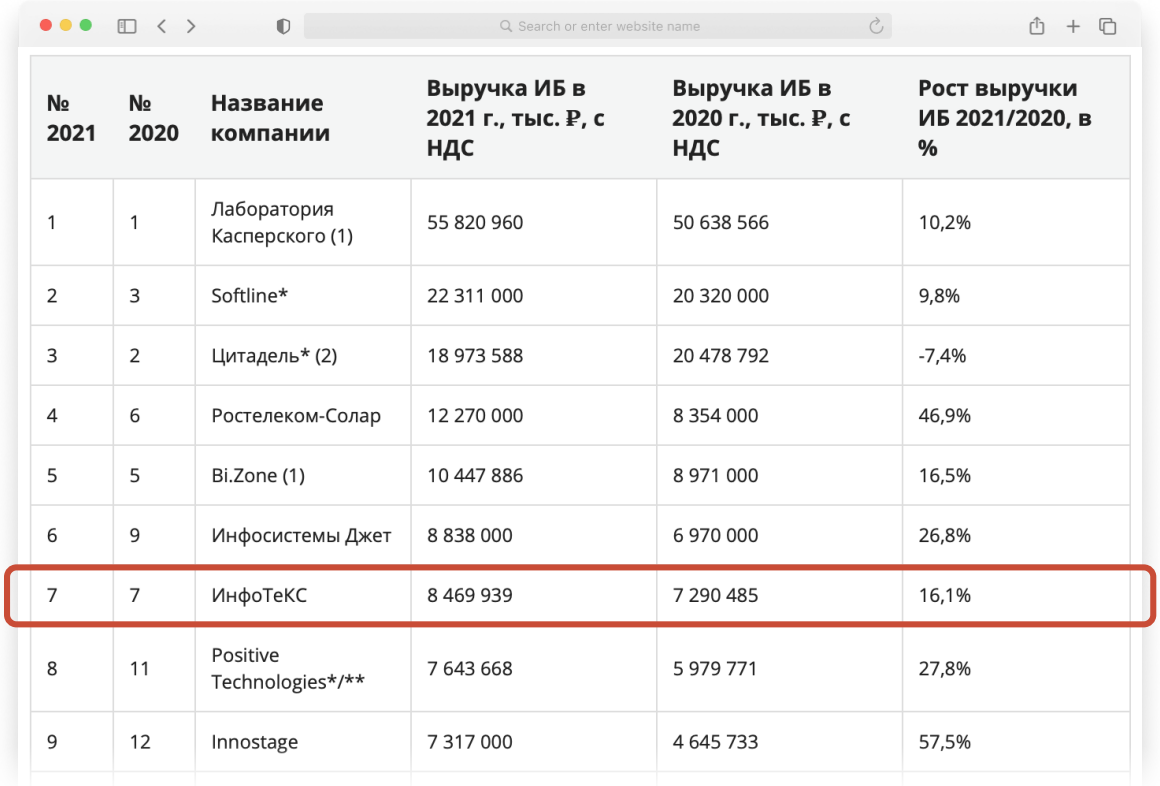
>60
Продуктов для защиты информации

>30
лет работы на рынке ИБ

>1600
сотрудников

>10 млн
рабочих станций, защищенных продуктами ViPNet

CNews Security: Крупнейшие вендоры в сфере защиты информации 2022



№ 2021	№ 2020	Название компании	Выручка ИБ в 2021 г., тыс. ₽, с НДС	Выручка ИБ в 2020 г., тыс. ₽, с НДС	Рост выручки ИБ 2021/2020, в %
1	1	Лаборатория Касперского (1)	55 820 960	50 638 566	10,2%
2	3	Softline*	22 311 000	20 320 000	9,8%
3	2	Цитадель* (2)	18 973 588	20 478 792	-7,4%
4	6	Ростелеком-Солар	12 270 000	8 354 000	46,9%
5	5	Bi.Zone (1)	10 447 886	8 971 000	16,5%
6	9	Инфосистемы Джет	8 838 000	6 970 000	26,8%
7	7	ИнфоТеКС	8 469 939	7 290 485	16,1%
8	11	Positive Technologies*/**	7 643 668	5 979 771	27,8%
9	12	Innostage	7 317 000	4 645 733	57,5%

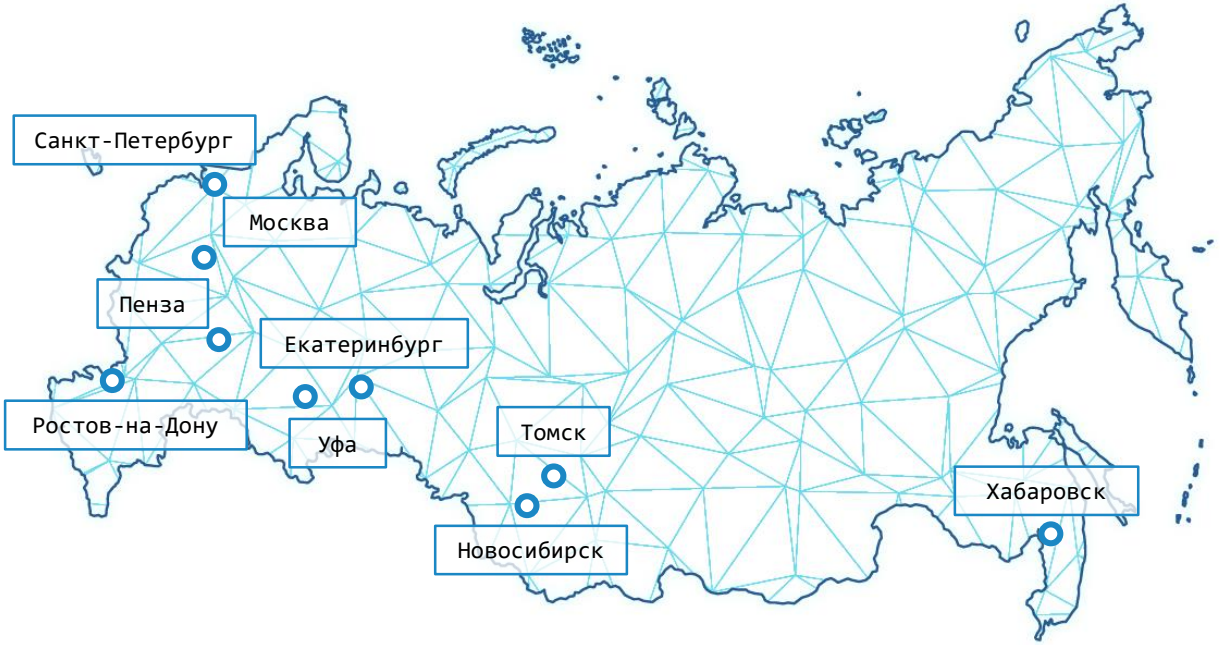
RAEX: Крупнейшие IT-компании разработчики ПО 2023

Рэнкинг крупнейших IT-компаний и групп в области разработки программного обеспечения (2023 год)

• Рейтинг Мнения рынка Аналитика Методика

№	Название	Выручка по направлению за 2022 год (тыс. рублей)	Доля выручки от готового ПО (%)	Доля выручки от проектного ПО (%)	Тип участника рэнкинга
1	T1	83912952	45.2	54.8	группа
2	«МТС Диджитал»	31856750	-	100.0	группа
3	Positive Technologies	12359665	100.0	-	группа
4	«ИнфоТеКС»	6140210	100.0	-	группа
5	IBS	5744874	-	100.0	группа
6	"АСКОН"	3081365	69.3	30.7	группа
7	«Инфосистемы Джет»	2991699	20.0	80.0	группа
8	"Синимекс"	2451106	-	100.0	группа
9	ICL-КПО ВС	2126067	9.2	90.8	группа
10	N3.Group	2081817	19.5	80.5	группа

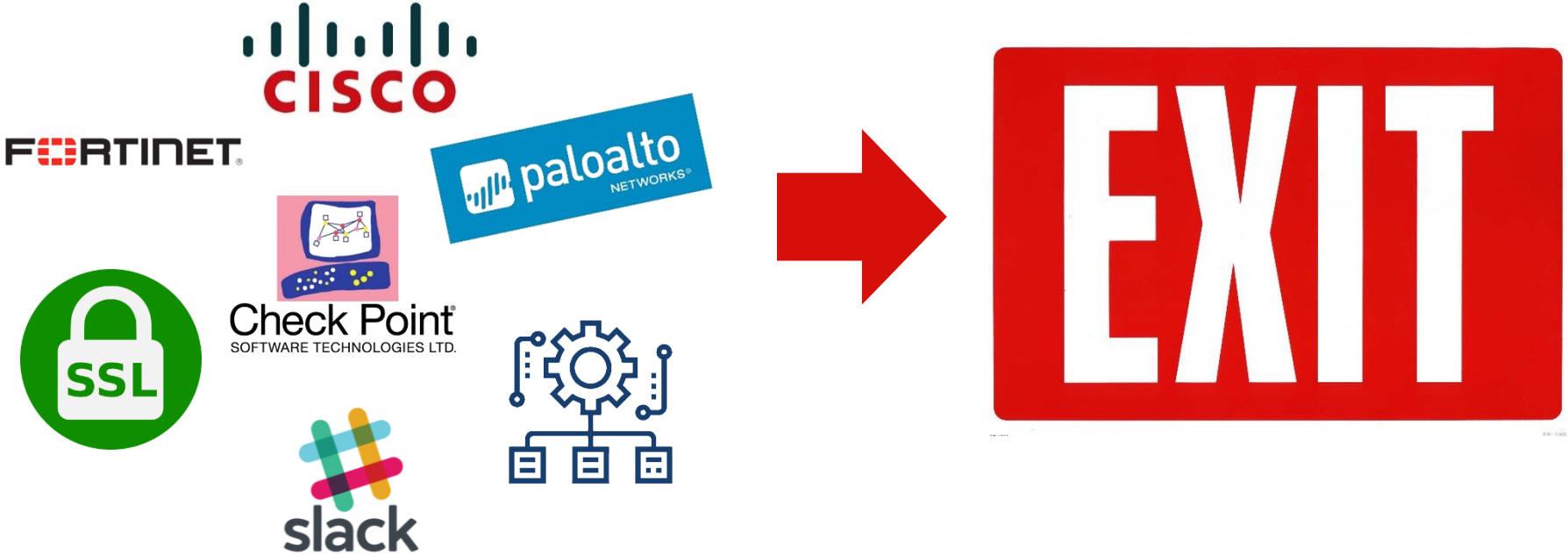
Представительства ИнфоТеКС



1. Москва
2. Санкт-Петербург
3. Хабаровск
4. Томск
5. Уфа
6. Ростов-на-Дону
7. Екатеринбург
8. Пенза
9. Новосибирск

Иностранные компании в России: **уйти** нельзя **остаться?**

Средства защиты информации



Кибератаки: динамика

Кибератаки в 2021 г.

Кибератаки с марта 2022г.

Нормативное регулирование

- **Приказ ФСТЭК России №239**
  «Требования по обеспечению значимых объектов КИИ РФ» от 25.12.2017 г с изменениями от 2020 г.
- **Указ президента РФ №166**
  «О мерах по обеспечению технологической независимости и безопасности КИИ РФ» от 30.03.2022 г.
- **Указ президента РФ №250**
  «О дополнительных мерах по обеспечению информационной безопасности РФ» от 01.05.2022г.

Продукты и решения ViPNet

* подходят для импортозамещения

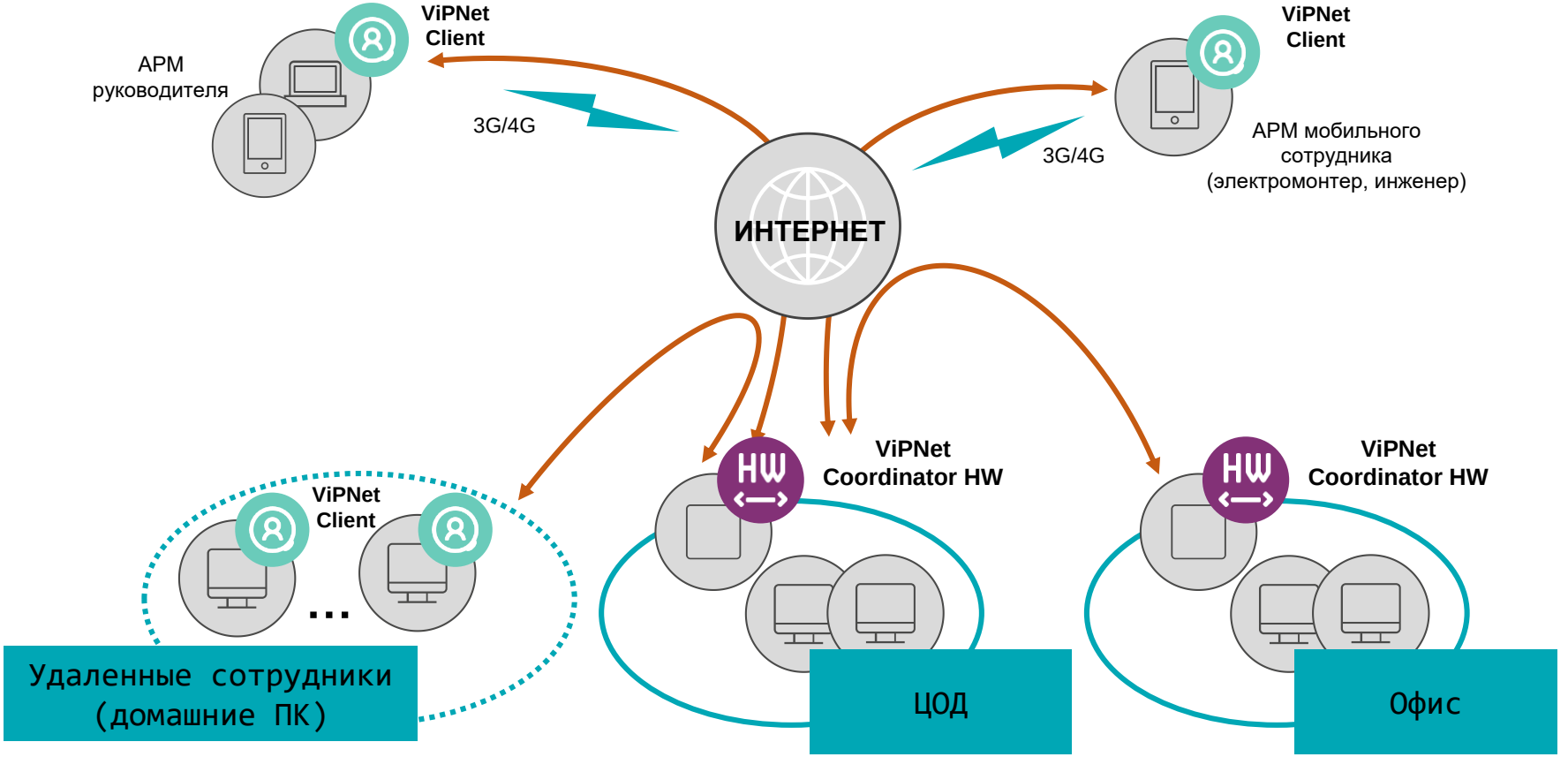
1. Импортозамещение иностранных NGFW

- Что замещаем
  - Fortinet
  - Cisco
  - Check Point
  - Palo Alto
  - …

Чем замещаем

- NGFW ViPNet xFirewall 5.x

2. Защита каналов связи (удаленного доступа) – VPN



Возможности VPN на базе ViPNet

Решения:

- ViPNet Coordinator HW
- ViPNet Coordinator VA
- ViPNet Coordinator KB
- ViPNet L2-10G

Особенности:

- Симметричное шифрование (работа на плохих каналах)
- Централизованное обновление (ПО и ключей)
- Производительность более 10 Гбит/с
- Режимы L2/L3
- Возможность кластеризации
- Возможность межсетевого взаимодействия*

Персональный VPN на базе продуктов ViPNet

Решения:

ЦУС 5 поколения
ViPNet Prime + Rollout Centre

Сертифицированные криптошлюзы (ПАК и VA)
ViPNet Coordinator 4.x → 5.x

Сертифицированные vpn-клиенты для различных ОС

Что замещаем:

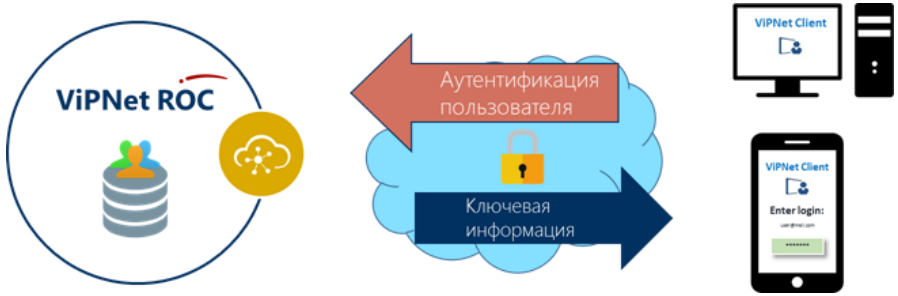
- Cisco AnyConnect
- Check Point
- …

Особенности:

- Оперативного и удобное подключение большого числа пользователей
- Поддержка всех актуальных ОС
- Деловая почта для Линукс*

ЦУС 5 поколения
ViPNet Prime + Rollout Centre (ROC)

1. Интеграция ViPNet Prime с AD
2. Канал для доставки второго фактора (e-mail или тлф)
3. Приглашение пользователю со ссылкой на инсталлятор
4. Автоматическое подключение к серверу ROC для получения ключей шифрования с использованием TLS-канала
5. Автоматическая загрузка ключей на устройства (запрашивается пароль на активацию)
6. Автоматическое применение политик, зафиксированных администратором для пользователя



Сертифицированные vpn-клиенты ViPNet Client

КОМПЬЮТЕРЫ НОУТБУКИ

ТЕЛЕФОНЫ ПЛАНШЕТЫ

КОНТРОЛЛЕРЫ И КОНЕЧНЫЕ УСТРОЙСТВА АВТОМАТИЗАЦИИ

- Доступны в магазинах приложений

ViPNet Coordinator HW 5

infotecs

Firewall
- МЭ с контролем состояния сессий (SPI)
- Контроль приложений (DPI)
- Прокси-сервер
- Идентификация пользователей (AD/LDAP)

VPN
- L3 VPN
- L2OverIP VPN
- Remote Access VPN
- Новые алгоритмы ГОСТ 34.12-2018 ГОСТ 34.13-2018

IPS
- IPS/IDS

Failover
- HA Cluster (active/passive)

Антивирус
- Любой внешний ICAP

Прочее
- Ролевая модель доступа
- Централизованное резервное копирование
- Captive Portal
- Лицензирование отдельных сервисов

Сертифицированные vpn-клиенты ViPNet Client. Нетиповой сценарий №1 - встраивание программного vpn-клиента в «умные» устройства

Встроенный в видеокамеру ViPNet Client Linux 4U

- ✓ Конфиденциальность – защита видеотрафика (биометрические данные, спецобъекты, места массового скопления людей …)
- ✓ Целостность – защита видеотрафика от подмены
- ✓ Отказ в обслуживании – защита от DDOS путем сокрытия адресного пространства (IP-адресов)
- ✓ Защита канала управления видеокамеры и видеосерверов

НОВОЕ!!!
Защита рабочих станций и серверов

Через «дыру» в ноутбуках Dell и HP можно захватить ядро ОС

Безопасность Пользователю Техника

03.02.2020, Пн, 10:24, Мск., Текст: Роман Георгиев

Во встроенном ПО ноутбуков Dell и HP есть уязвимость, позволяющая компрометировать их через режим прямого доступа к памяти

Реальность – повышение значимости и автоматизация работы различных компонентов аппаратных платформ

Вызовы для производителей СЗИ:

- «конечные» устройства – главная цель
- растущие атаки на недоверенные аппаратные платформы
- работа СКЗИ, СЗИ от НСД и др. СЗИ на «уровнях» ниже информационных и операционных систем

ViPNet SafeBoot (компонент ViPNet EPP)

Программный модуль доверенной загрузки

Устанавливается в UEFI BIOS различных производителей

Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS

Сертифицирован как средство доверенной загрузки уровня базовой системы ввода-вывода **второго** класса. С возможностью использования в ИСПДн до УЗ1 включительно и в ГИС до 1-го класса защищенности

Ключевые особенности

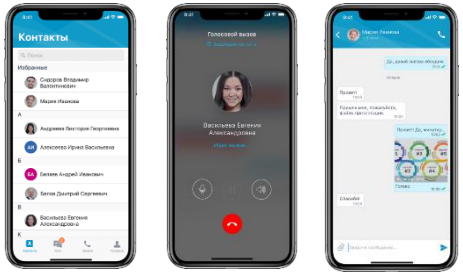
- Поддержка UEFI BIOS на различных платформах
- Возможность программного обновления замка
- Возможность установки в элементы виртуальной инфраструктуры
- Создание шаблонов настройки для удобства ввода в строй парка АРМ
- Отсутствие «железной составляющей»:
  - ✓ Меньше цена продукта
  - ✓ Экономия на логистике

Стоимость ПО ViPNet SafeBoot – 5 000 рублей:

3. Защищенные коммуникации сотрудников

Решение:

ViPNet Connect



Что замещаем:

- Slack
- WhatsApp
- …

Особенности:

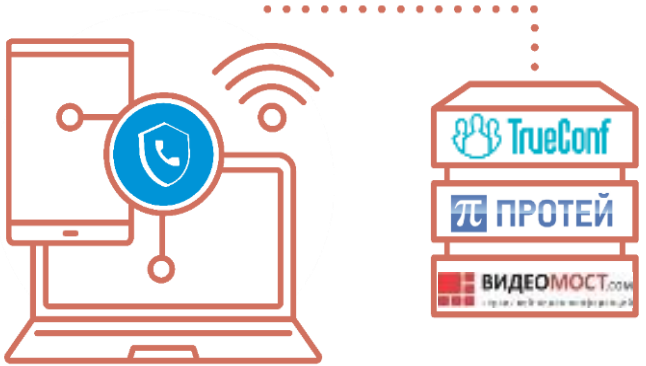
Функционал мессенджера:

- Чаты, пересылка файлов
- Групповые чаты
- Видеозвонки (напрямую)
- Транслировать свой экран другому пользователю в рамках видеосвязи

ViPNet Connect – дополнительные возможности

- Интеграция с SIP

- Интеграция с ВКС

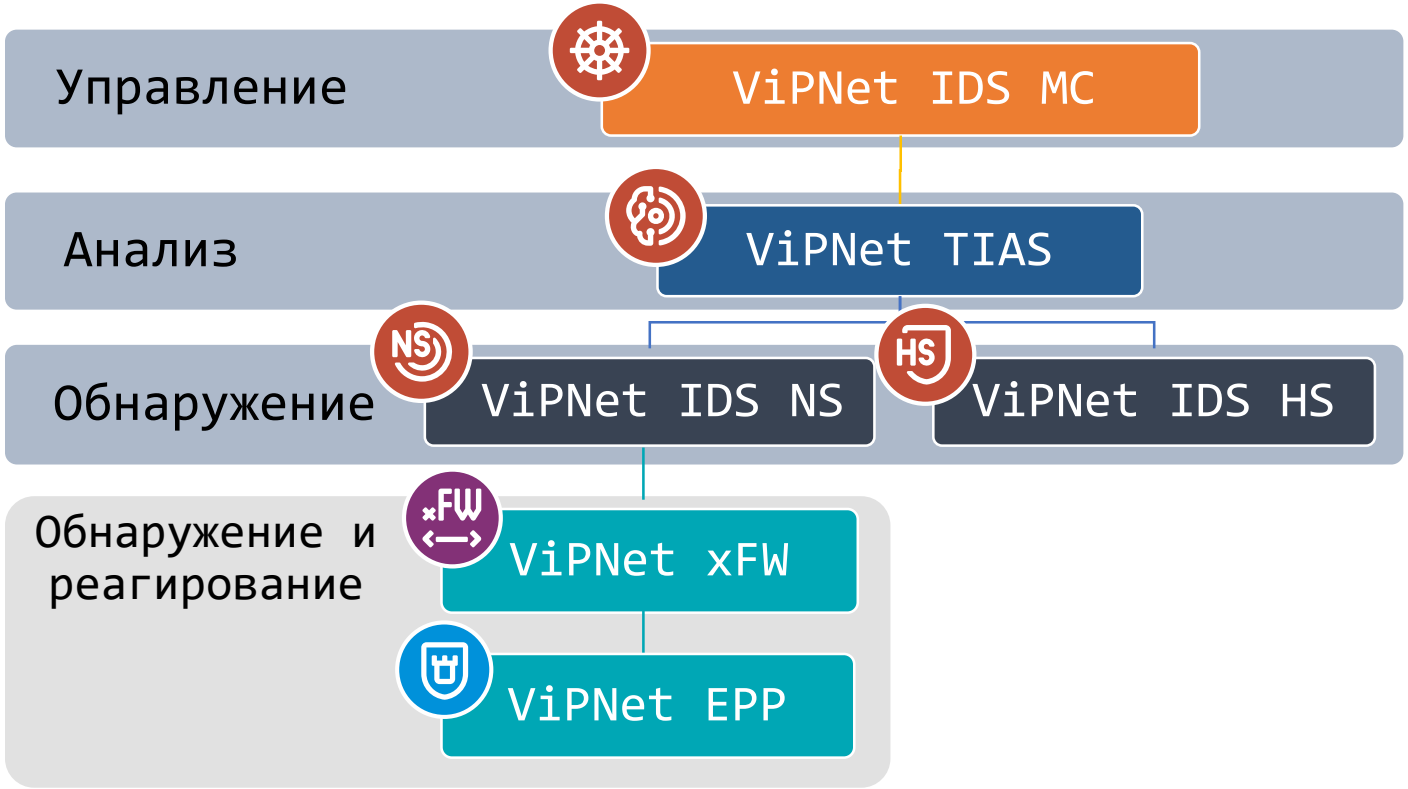


ViPNet Connect.
Нетиповой сценарий – контроль удаленных работ

отправка фото с мест контроля в ЦОД по защищенному каналу

Альтернатива – встраивание библиотеки СКЗИ ViPNet OSSL в приложение

4. Решения ViPNet для мониторинга. Комплекс продуктов



Как это работает?

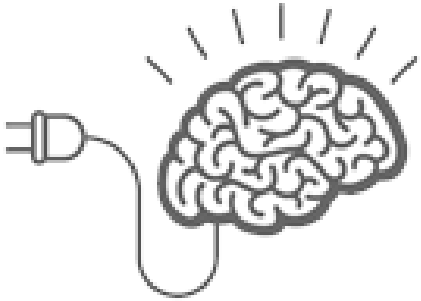
Выявление событий ИБ
(IDS NS, EPP xF..)

Множество событий ИБ

Особенности:

- Использование самообучаемой нейросети

Модуль анализа
ViPNet TIAS



Выявление критических событий (инцидентов)

Особенности:

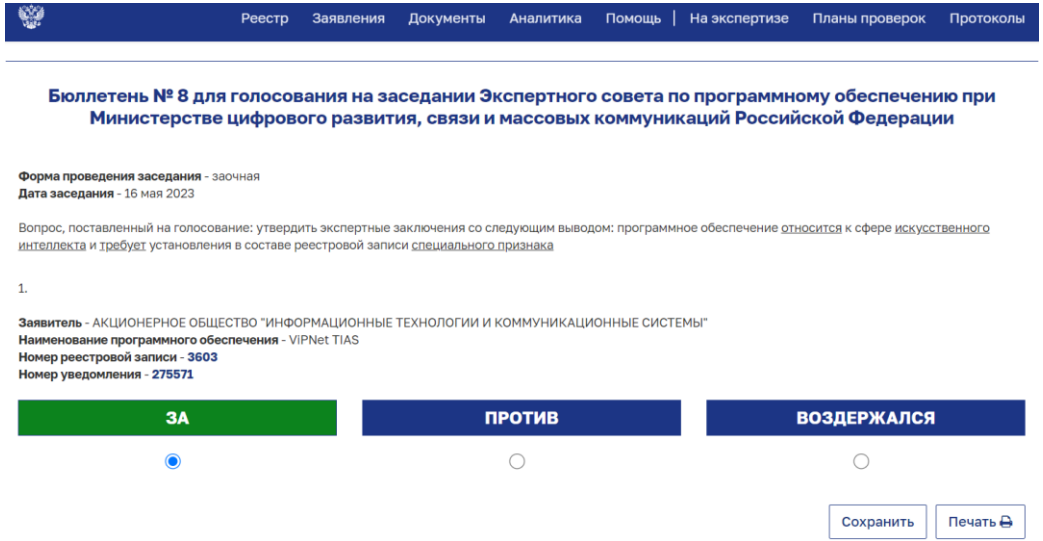
- Модель ИИ с наставником

Обработка в SOC

Обработка инцидентов

Статистика и отчеты

Текущая стадия развития продукта



05.2023

Выполнены проверки программного обеспечения на отнесение к сфере искусственного интеллекта

Первое СЗИ с признаком ИИ в Реестре

Экспертиза.
Создание баз решающих правил для СОВ

Cisco (VRT, Talos)	ET (Emerging Threats Pro)	~~StoneSoft~~	ИнфоТеКС (AM Rules)
Более 30 000 сигнатур	Более 30 000 сигнатур		Более 24 000 сигнатур(14 000 собственных)
ZeroDay сигнатуры	ZeroDay сигнатуры		ZeroDay сигнатуры
Страна происхождения: США	Страна происхождения: США		Страна происхождения: Россия




5. PKI: Защита порталов/ЭДО/Подключение к СМЭВ

Решения:

- ViPNet TLS Gateway
- ViPNet HSM/PKI Service
- ViPNet EDI

Особенности:

- Поддержка ГОСТ
- Класс КС-КС3
- Возможность организации внутренней среды доверия
- Возможность интеграции со СМЭВ

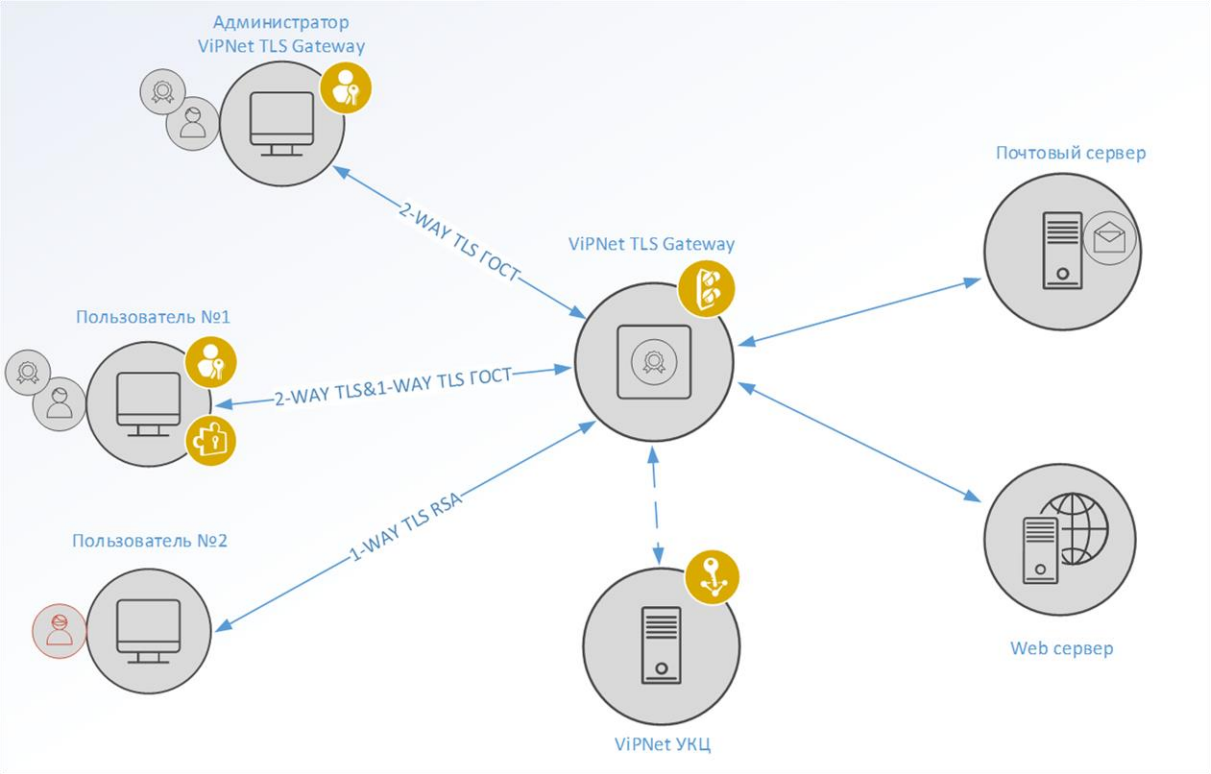
ViPNet TLS.
Доступ к защищаемым ресурсам

Задачи:

1. Защита соединений
2. Аутентификация клиентов

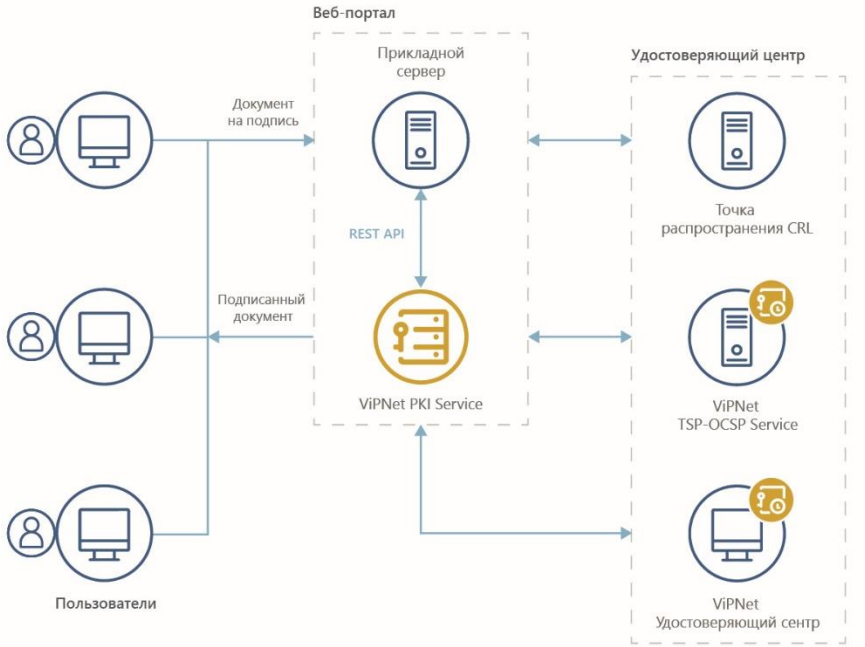
Для этого требуется:

Двусторонний TLS



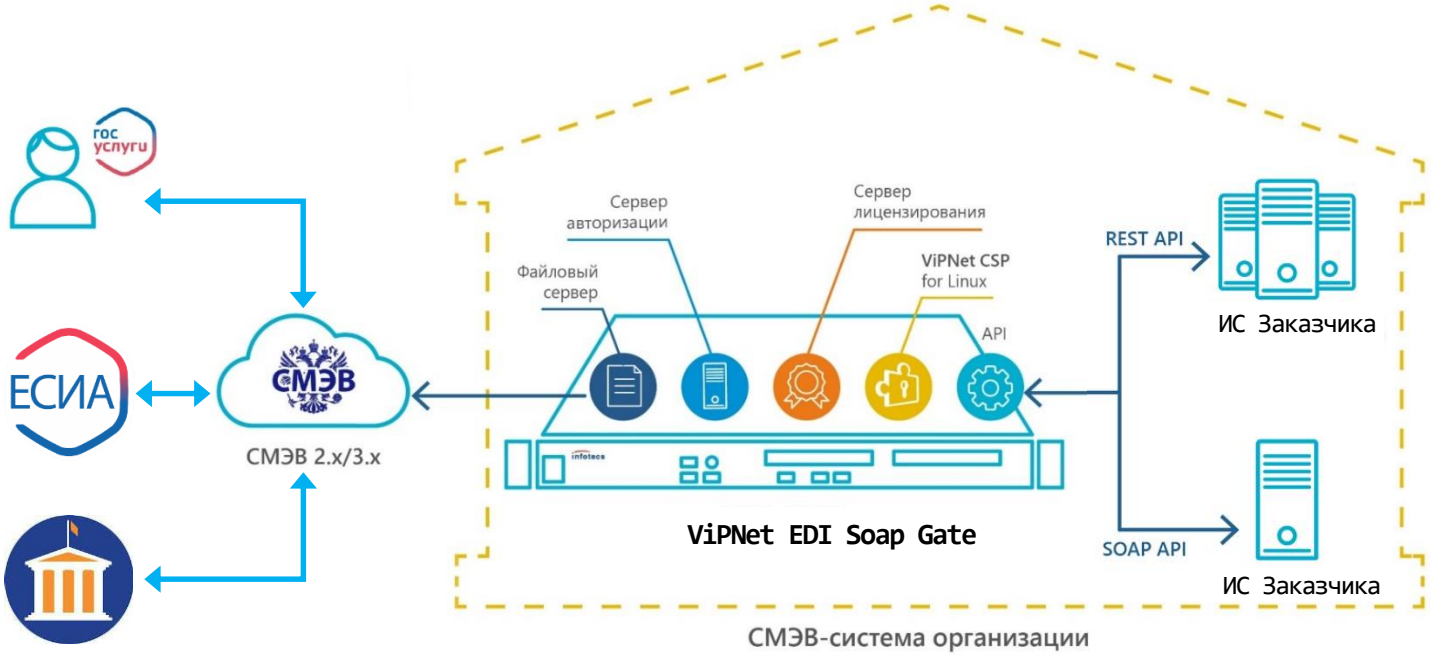
ViPNet PKI Service: функциональные возможности

- Централизованное хранение и генерация ключей
- Выполнение функций создания и проверки ЭП по запросу АИС и пользователей АИС
- Шифрование и расшифрование данных
- Интерфейс для взаимодействия с информационными системами – REST API



Сертифицирован по классу КВ/КВ2, зарегистрирован в Реестре российского ПО

Шлюз для СМЭВ. Подключение ИС Заказчика к СМЭВ



6. Средства защиты информации полевого уровня

Наложенные средства

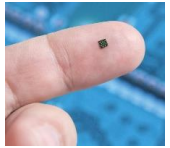
Аппаратные

Встроенные средства

Программные

КриптоКлиенты

Аппаратные



Индустриальное исполнение ViPNet Coordinator IG

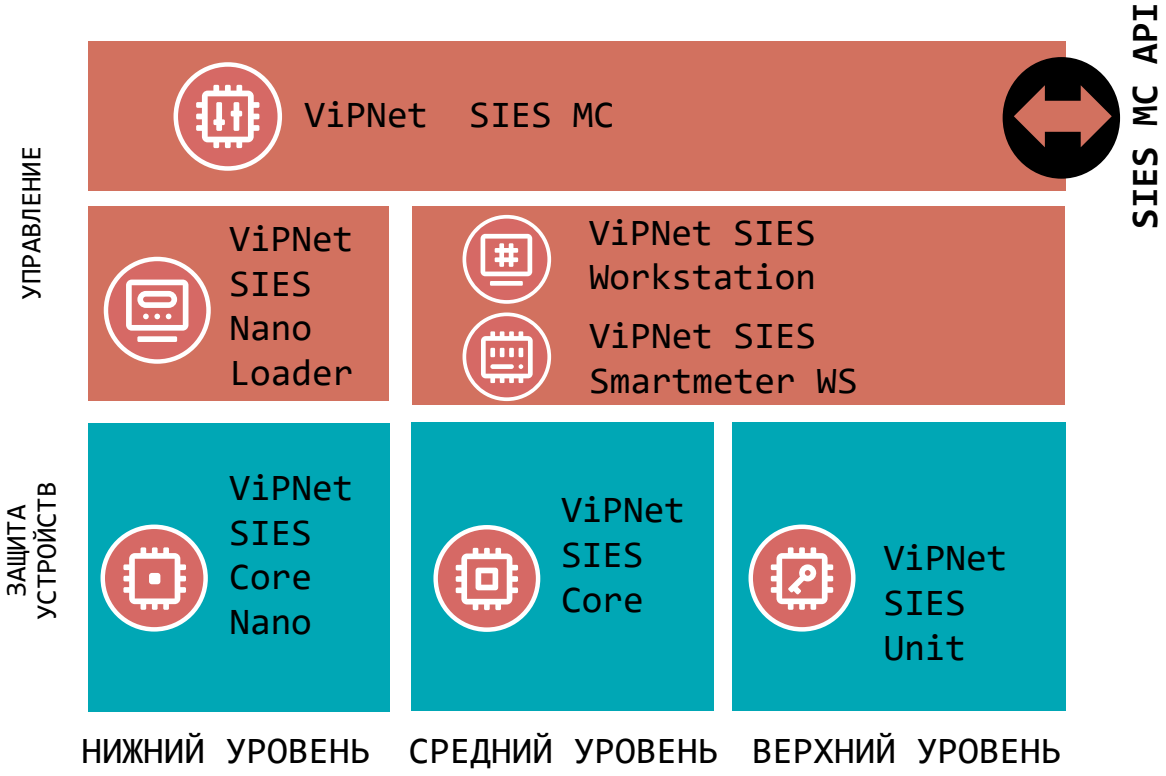
- Защищенная сеть ViPNet
- Межсетевой экран + DPI протоколов Modbus и IEC 104
- Шлюз Modbus
- Коммутатор и маршрутизатор
- Wi-Fi-модуль
- GSM-модем
- Отказоустойчивость
- Мониторинг состояния

Сертифицированные vpn-клиенты ViPNet Client. Встраивание программного vpn-клиента в «умные» устройства

Встроенный в видеокамеру ViPNet Client Linux 4U

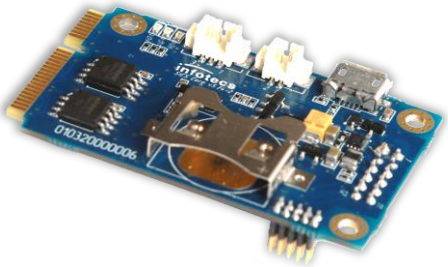
- ✓ Конфиденциальность – защита видеотрафика (биометрические данные, спецобъекты, места массового скопления людей …)
- ✓ Целостность – защита видеотрафика от подмены
- ✓ Отказ в обслуживании – защита от DDOS путем сокрытия адресного пространства (IP-адресов)
- ✓ Защита канала управления видеокамеры и видеосерверов

Встраиваемые СЗИ. Состав решения ViPNet SIES



- СКЗИ класса КС1 и КС3 по требованиям ФСБ России
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств

ViPNet SIES Core – защита шлюзов и базовых станций



Встраивание:

- На аппаратном уровне – UART, USB, SPI
- На программном уровне – SIES Core API
  SDK для Linux (ARM, x86), Windows, RTOS

Криптографические функции:

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

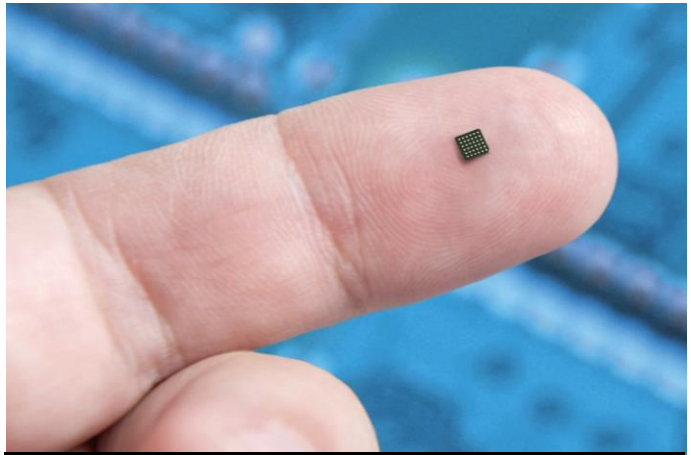
Функциональные особенности:

- Форм-фактор – плата PCI Express® Full-Mini Card
  (51 x 30 x 11,2 мм)
- Поддержка ДНСД для эксплуатации вне
  контролируемой зоны
- Рабочий диапазон температур -40…+70^{0}C

Соответствие требованиям:

- СКЗИ класса КС3

ViPNet SIES Core Nano – защита IIoT-устройств



Встраивание:

- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

Криптографический протокол CRISP:

- Зашифрование/расшифрование
- Вычисление/проверка имитовставки
- Вычисление/проверка хэш-кода

Функциональные особенности:

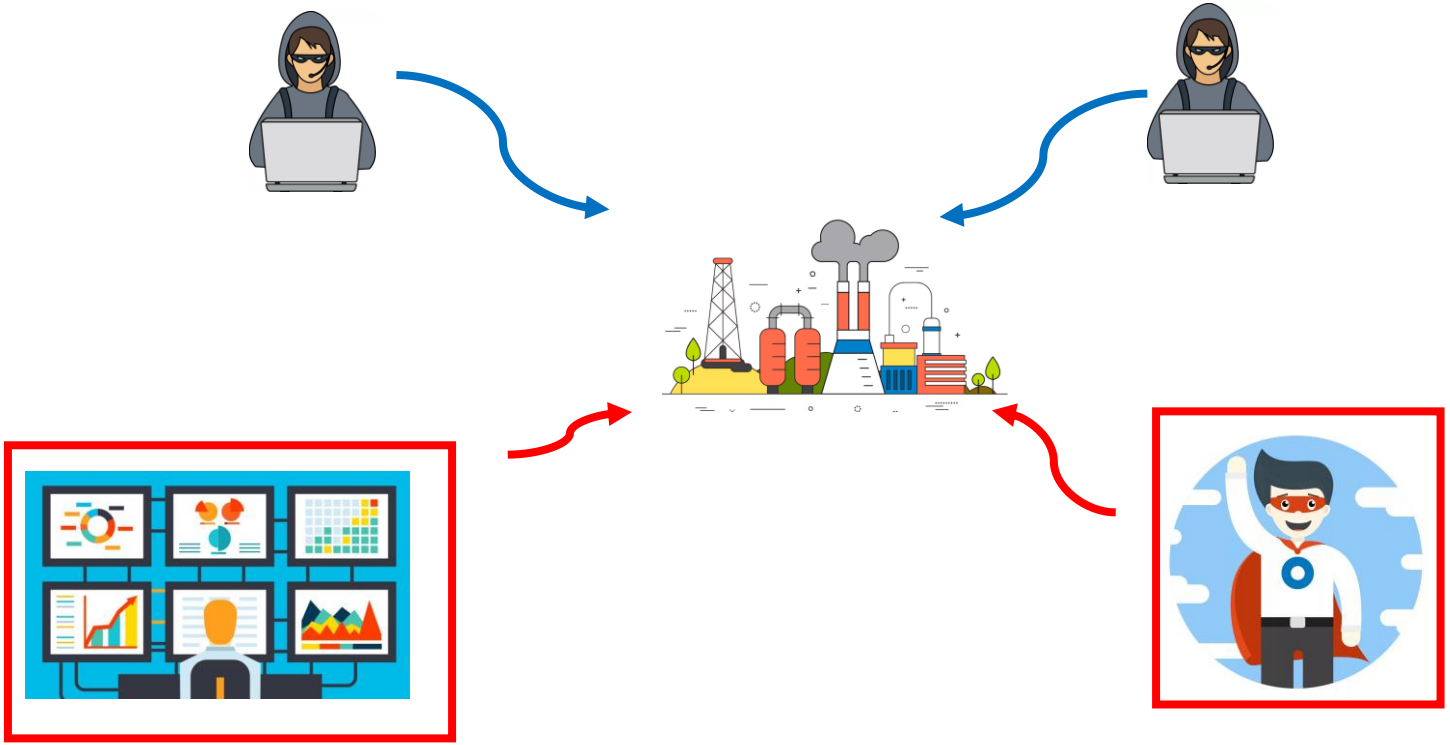
- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40…+85^{O}C
- Форм-фактор – микросхема 3x3x0,4 мм

Соответствие требованиям:

- СКЗИ класса КС3
- Защита от атак инженерного проникновения (СКЗИ-НР)

Люди – главный недостающий ресурс

Киберполигон Ampire.
Тренируем безопасников с 2018 года

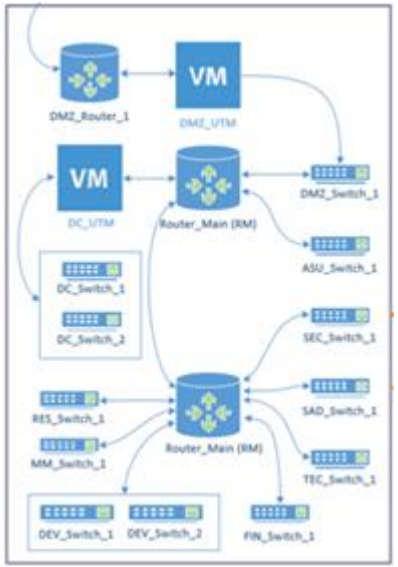


Не виртуалка, а платформа

infotecs

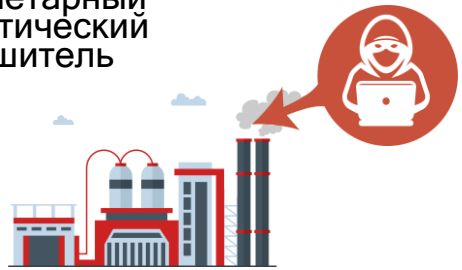
Практические занятия на цифровом двойнике реальной инфраструктуры

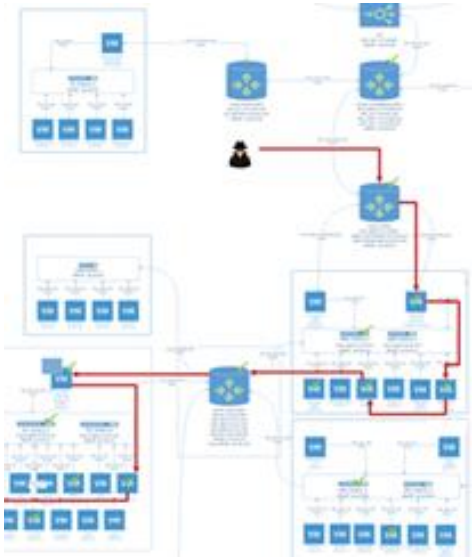
Симуляция сети с ИТ и SCADA-сегментами

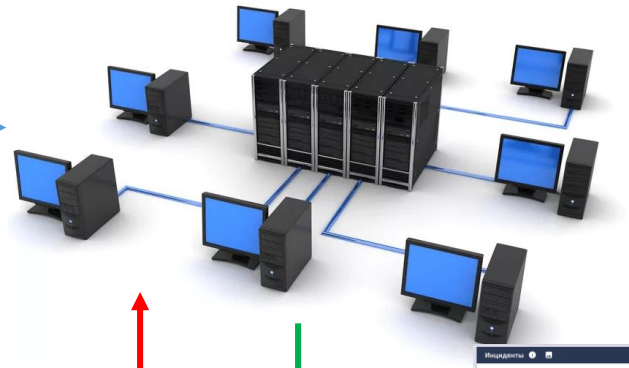


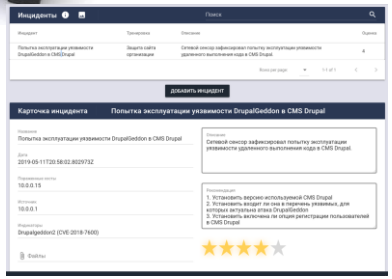
Security Operations Center

Проприетарный автоматический нарушитель









Группа мониторинга

Группа реагирования

Киберучения. Сценарии

- Сценарий №1 "Защита базы данных предприятия"
- Сценарий №2 "Защита контроллера домена предприятия"
- Сценарий №3 "Защита файлового сервера предприятия (MS17-010)"
- Сценарий №4 "Защита данных сегмета АСУ ТП"
- Сценарий №5 "Защита научно-технической информации предприятия"
- Сценарий №6 "Защита корпоративного портала от внутреннего нарушителя"

Целевая аудитория

- Студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.

Развиваем навыки

Проектировать
для защиты

Наблюдать
и управлять

Собирать и
использовать

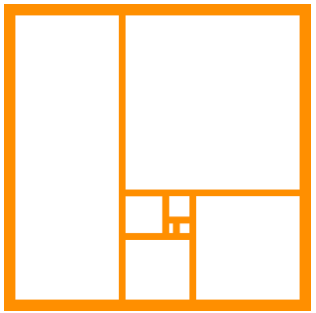
Расследовать

Использовать
и
поддерживать

Охранять и
защищать

Анализировать

Причины выбрать Ampire



Ampire – это решение, на котором ИТ-специалисты могут получать **базовые знания** о защите информации, и в то же время, зрелые ИБ-эксперты могут получать **новые навыки**

Гибкие возможности **конфигурации виртуальной инфраструктуры**, поддержка **различных средств защиты**, средняя цена, облачная и собственная платформа

Спасибо за внимание!

Александр Реунов

ra@infotecs.ru

+7 926 567 38 88

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363