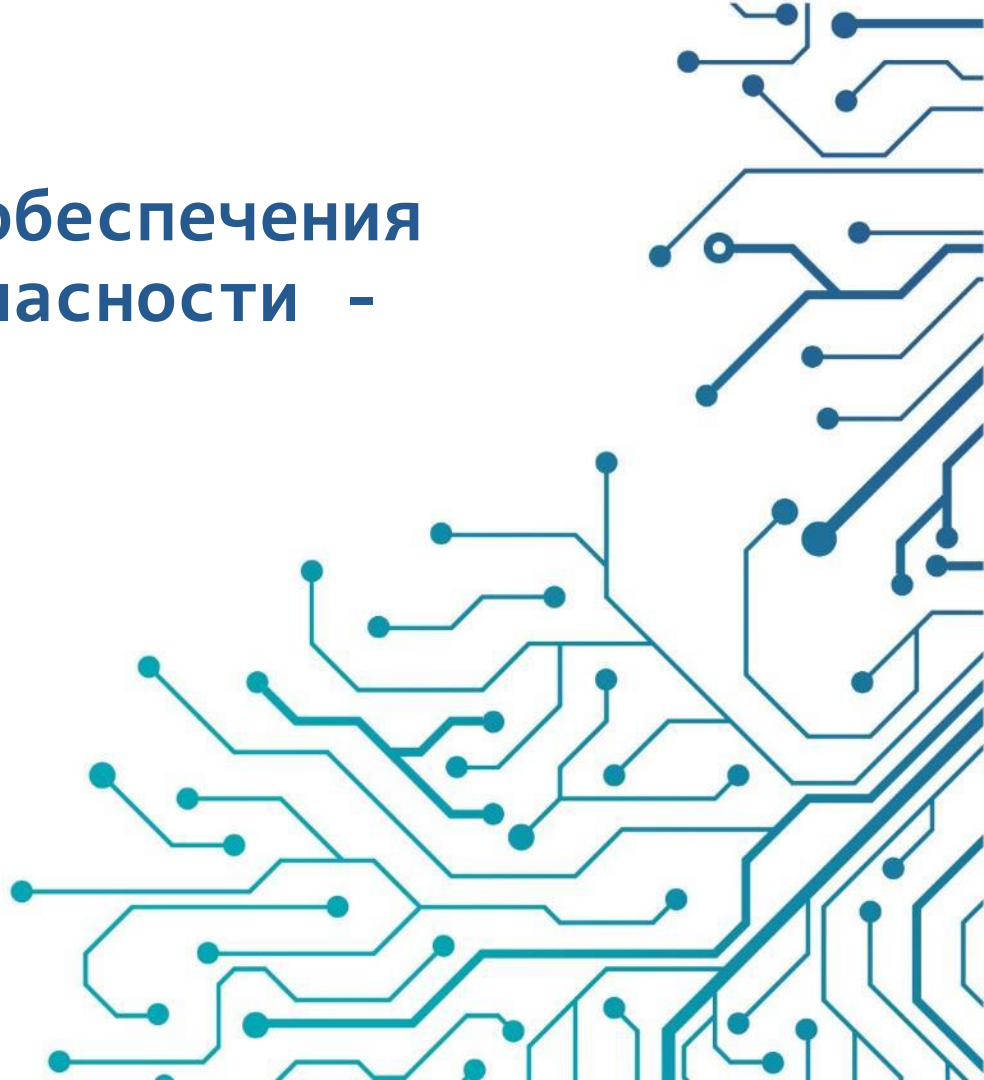
Актуальные вопросы обеспечения информационной безопасности - новое поколение СЗИ

Александр Реунов



infotecs

infotecs

ПроКванТ

- опытное и серийное производство аппаратных платформ квантовых продуктов

СФБ ЛАБ

-аккредитованная испытательная лаборатория в системах сертификации ФСБ России и ФСТЭК России

infotecs УЧЕБНЫЙ ЦЕНТР

- подготовка специалистов в сфере информационной безопасности

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

-исследования безопасности, мониторинг и предотвращение атак, расследования инцидентов, разработка решений информационной безопасности

прокси

-цифровые продукты и сервисы на базе технологий распределенного реестра и смарт-контрактов

Единый Медицинский Портал

- защищенная телемедицинская платформа

Группа компаний «ИнфоТеКС» в цифрах

infotecs

>30
лет работы на рынке

12
офисов по всей стране

> 400
партнеров в регионах

>2000
сотрудников

>60
продуктов для защиты информации

Топ-10
крупнейших компаний в сфере защиты информации

>10 млн
рабочих станций, защищенных продуктами

Топ-5
компаний по количеству патентов в области цифровых технологий

Подходы к обеспечению ИБ

**«Вашу ИТ-инфраструктуру никогда не атаковали?
Значит вы просто об этом не знаете»**

Организационные меры:

Создание подразделения по ИБ
Назначение ответственных
Регламенты работы подразделения ИБ/реагирования на инциденты
...

Установка и настройка систем защиты информации

Сокращение «площади» атаки

Установка и настройка систем защиты информации

Защита / мониторинг / анализ / реагирование

Постоянное обучение и повышение квалификации сотрудников

Тяжело в учении, легче в бою

Продукты и решения ViPNet

* подходят для импортозамещения

1.Для организаций.
Защита каналов по ГОСТ и межсетевое экранирование

Важно:

+ VPN по ГОСТ
+ Сертифицировано ФСБ России, ФСТЭК России
+ Подходит для импортозамещения
+ Возможность межсети БЕСПЛАТНО

Импортозамещение иностранных NGFW

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

Чем замещаем

- ViPNet xFirewall 5.x
- ViPNet Coordinator HW 5

Для пользователей сетей ViPNet 4.x

Что уходит в прошлое?

1. **ГОСТ 28147-89** «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»
2. **ViPNet Administrator 4**

   Программное обеспечение, предназначенное для развертывания и администрирования сети ViPNet корпоративного масштаба
3. **ViPNet Coordinator HW 4**

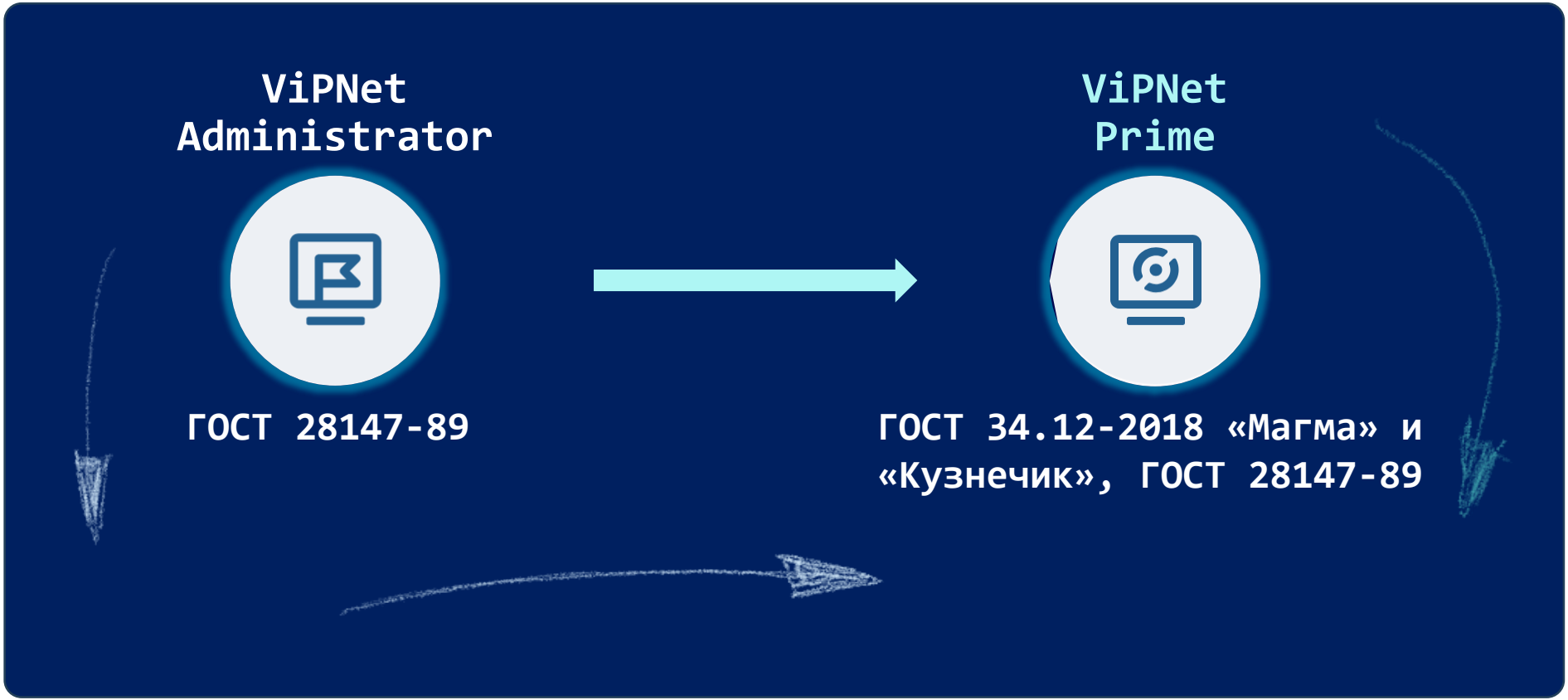
   Шлюз безопасности для защиты каналов связи

Перспективы: 2026 год и далее..

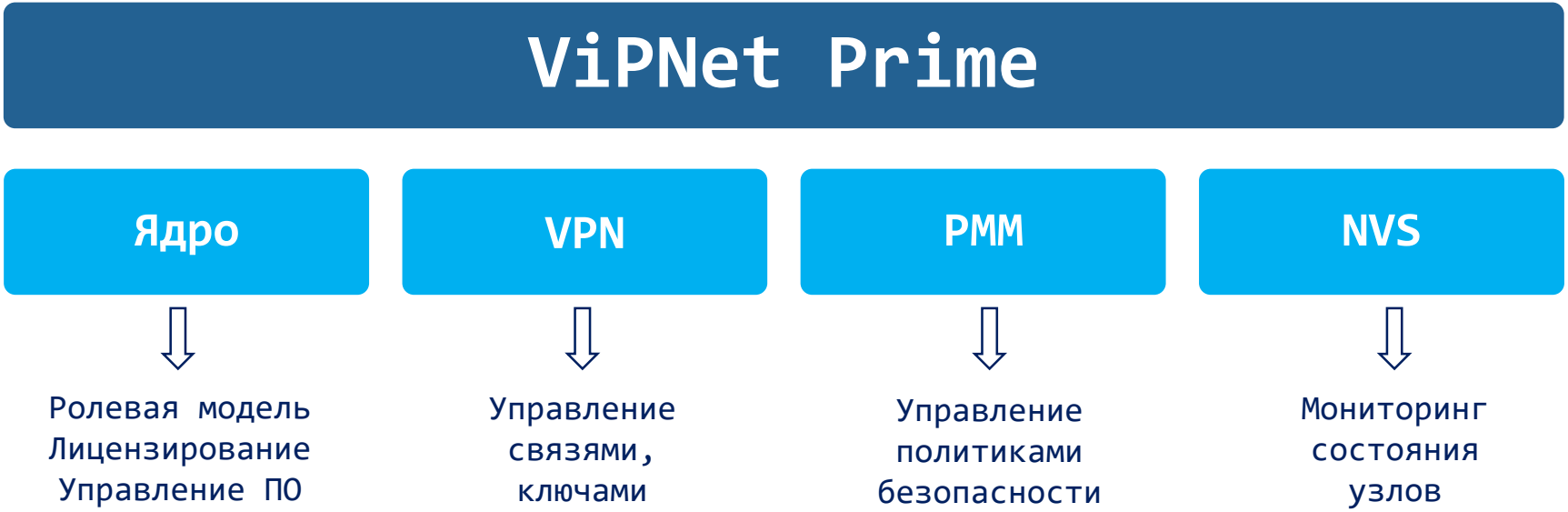
- Что уходит
  - ViPNet Administrator 4
  - ViPNet Coordinator HW 4
  - ViPNet Client 4

- Чем заменяем
  - ViPNet Prime
  - ViPNet Coordinator HW 5
  - ViPNet Client 5

Обо всем по порядку

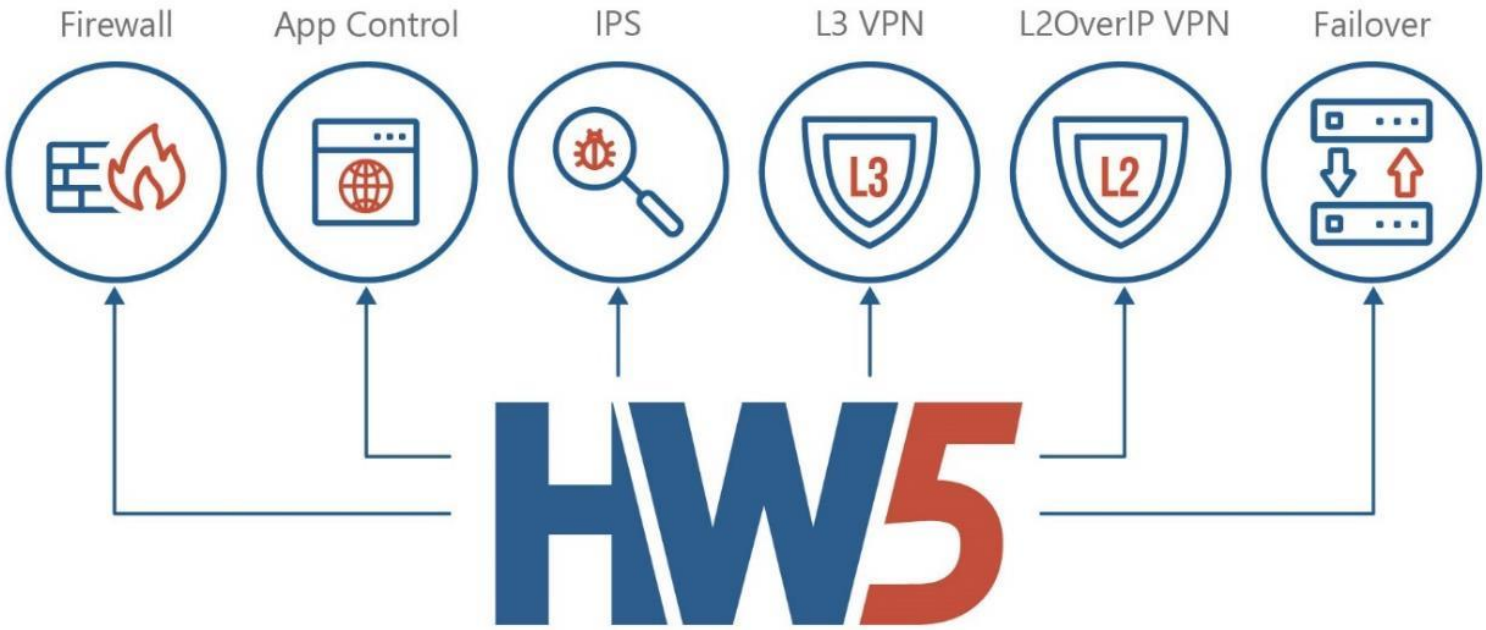


Новая система управления



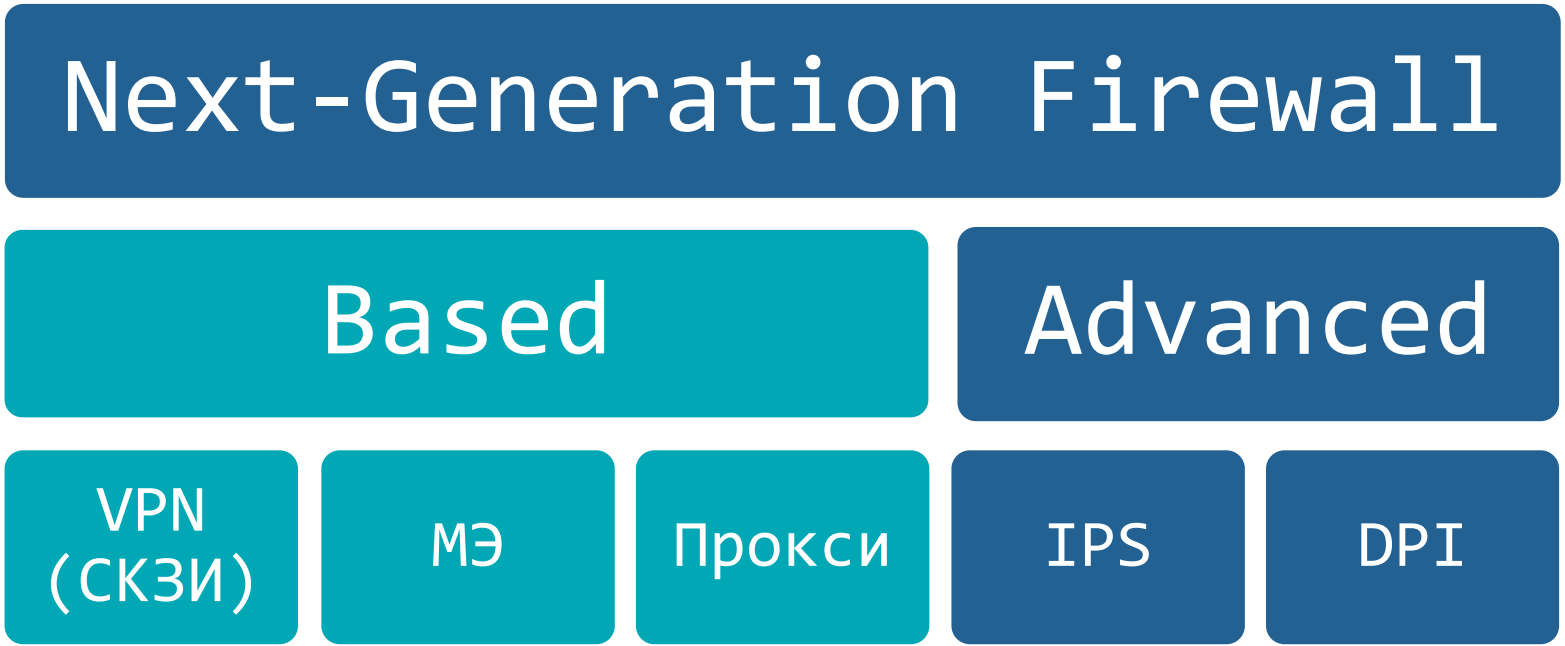
* **Работает в среде импортозамещенных ОС**
* **Поддерживает новые ГОСТы по криптографии**

ViPNet Coordinator HW 5 = NGFW + VPN

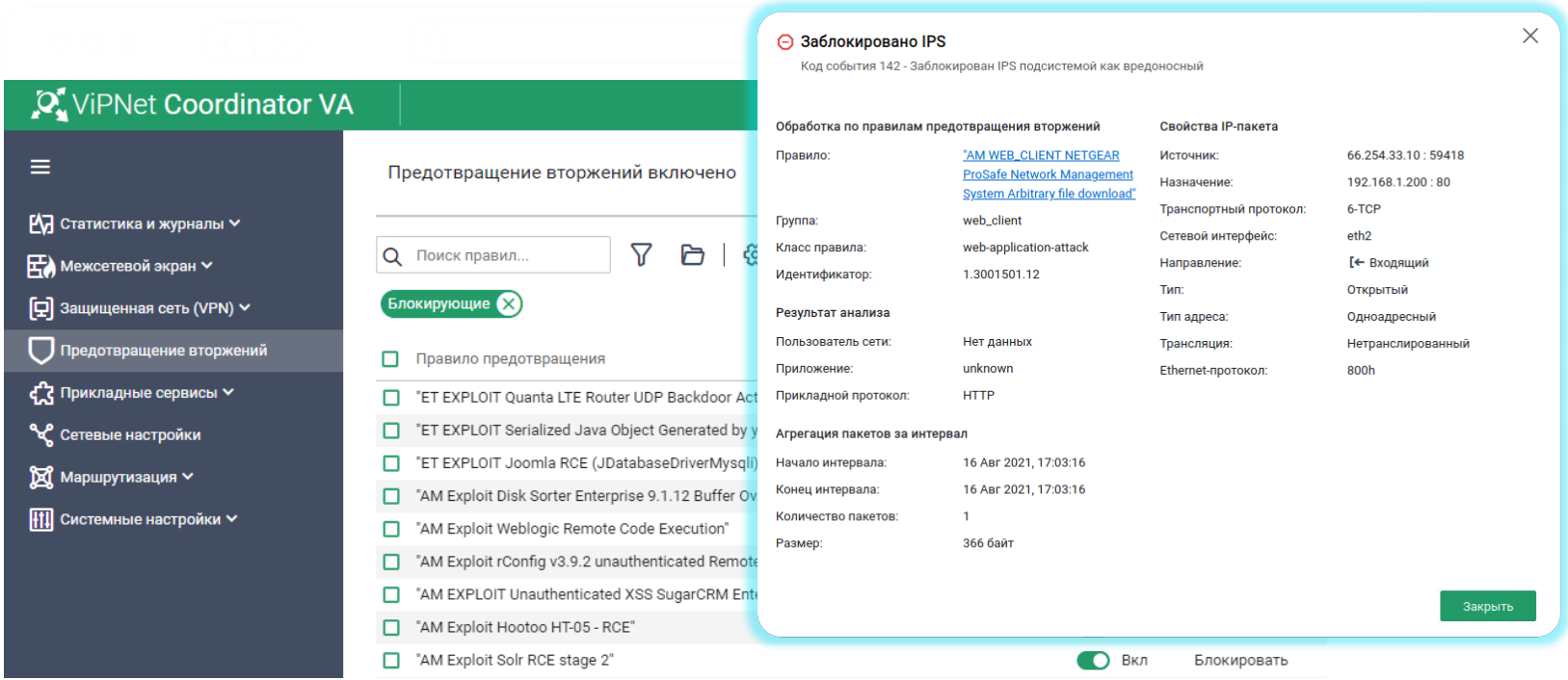


* Сертификат ФСБ России №СФ/124-4972 от 30.08.2024 года
* Сертификат ФСТЭК России №4831 от 25.07.2024 года

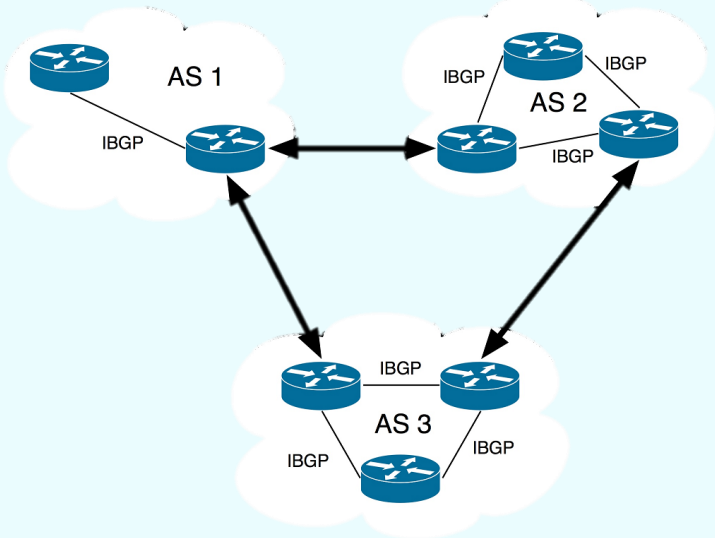
Схема лицензирования HW5



Предотвращение вторжений (IPS)

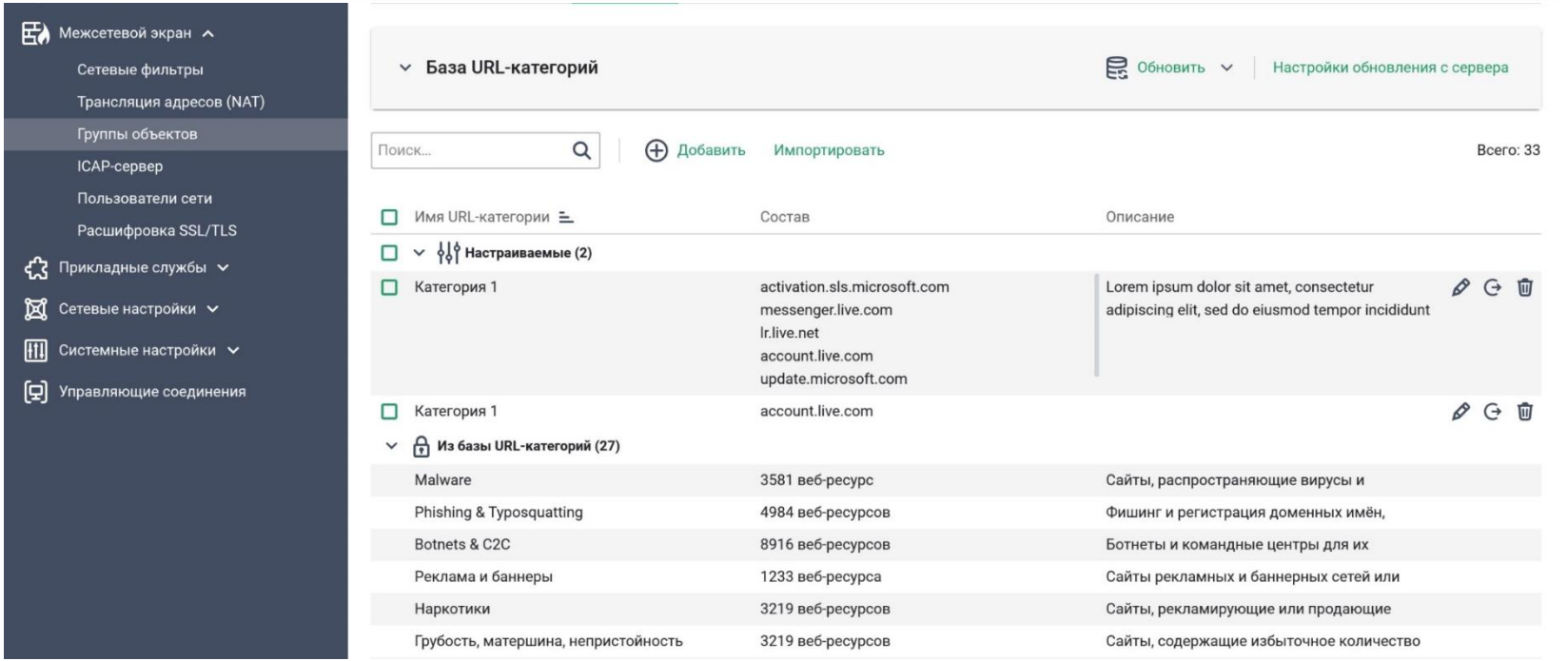


Поддержка протокола BGP



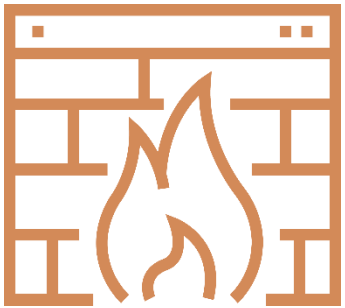
- Создание BGP-окружения или встраивание узла в существующее
- Получение и использование маршрутов по протоколу BGP
- Анонсирование и перераспределение маршрутов
- Балансировка трафика (ECMP, UCMP)

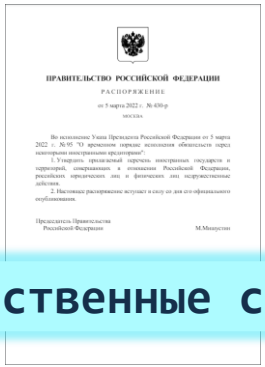
URL-фильтрация



Блокировка по GEO-IP

- Фильтрация трафика на основе данных о географической принадлежности отправителей
- Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)





ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 5 марта 2022 г. № 430-р

Дружественные страны

Сертификаты синхронизированы по версии прошивок!

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

- Межсетевой экран тип «А» и тип «Б» 4 класса
- СОВ уровня сети 4 класса
- 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети NEW

Минцифры России и Минпромторг России

В реестре российского ПО и реестре РЭП

Аппаратные платформы

HW10

HW50

HW100

Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D

Средние офисы

HW2000

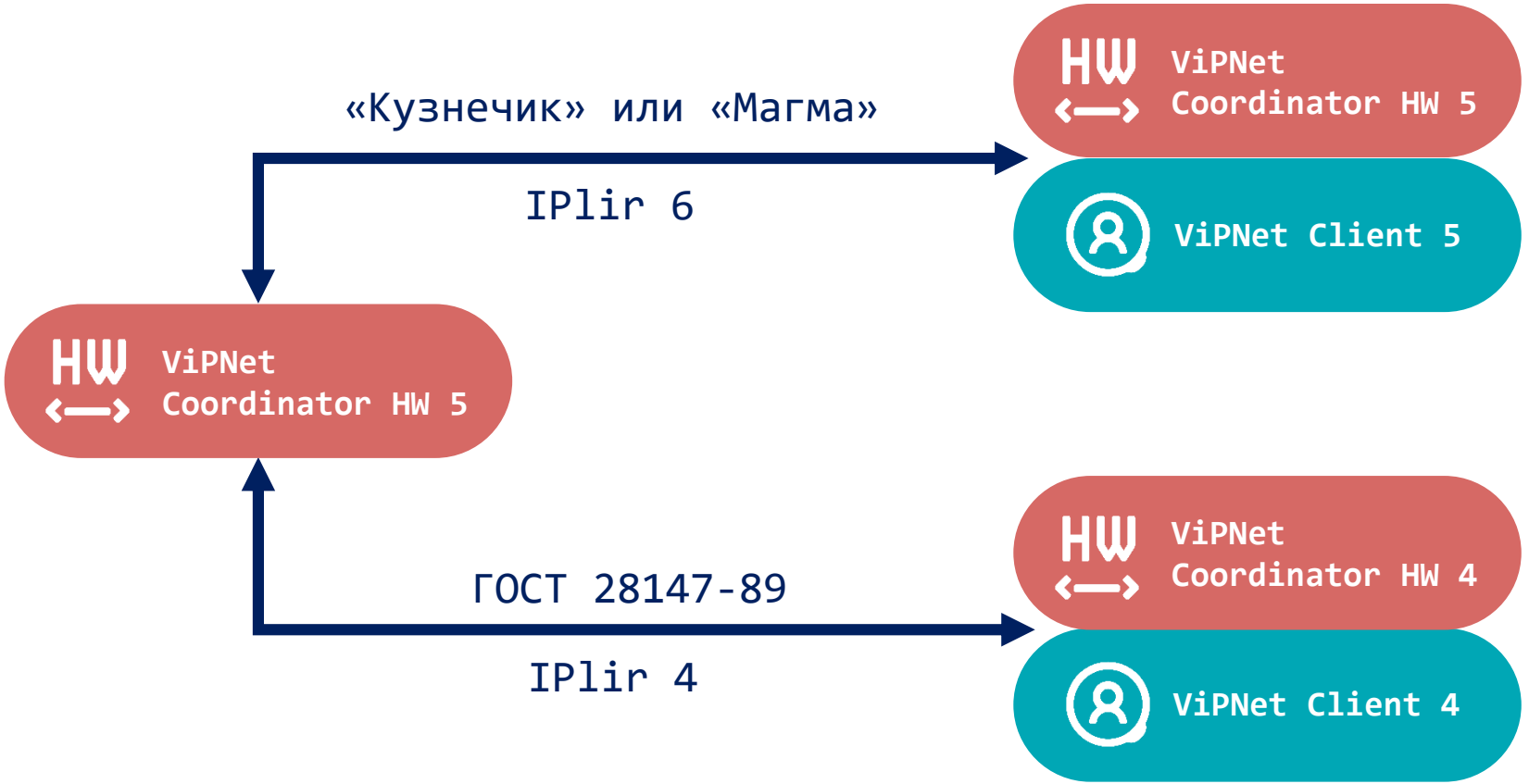
HW5000

Крупные учреждения, ЦОД

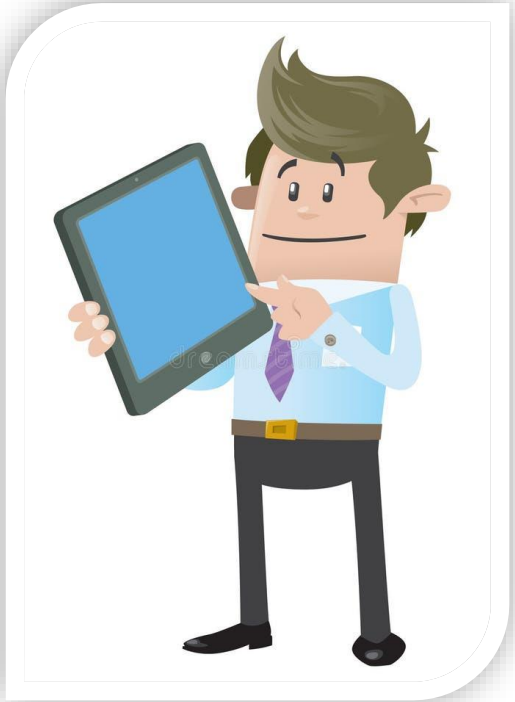
* **Назначенный срок службы платформ – 5 лет (прописан в формуляре)**
* **Поддерживаемые модели прописаны в сертификате соответствия**

Типовая схема применения HW 5

Обратная совместимость



2. Для защиты рабочих мест сотрудников



Комплексная защита рабочих станций

ViPNet Client 5

ViPNet SafePoint

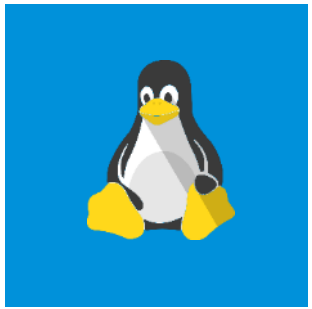
ViPNet SafeBoot 3

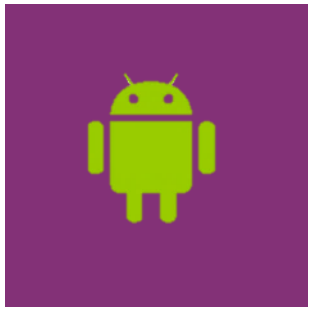
ViPNet EndPoint Protection

VPN-клиенты ViPNet Client

КОМПЬЮТЕРЫ
НОУТБУКИ

ТЕЛЕФОНЫ
ПЛАНШЕТЫ





Встраиваемая
версия
ViPNet Client

LINUX BASED

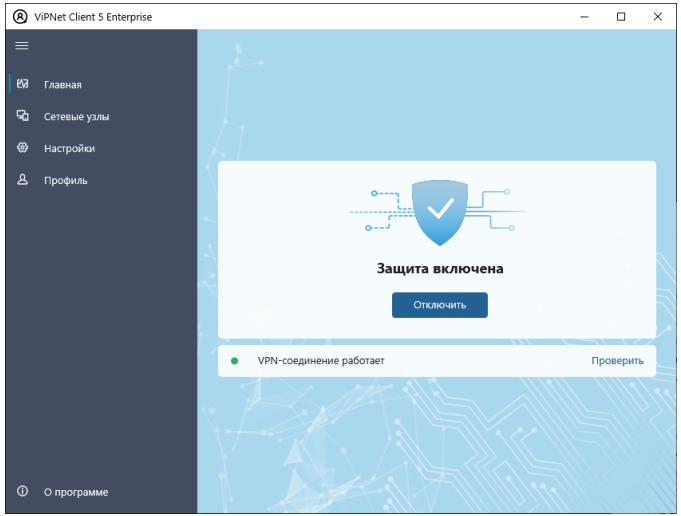
MIPS

МЦСТ
ЭЛЬБРУС

КОНТРОЛЛЕРЫ И КОНЕЧНЫЕ
УСТРОЙСТВА АВТОМАТИЗАЦИИ

Доступны в магазинах приложений*

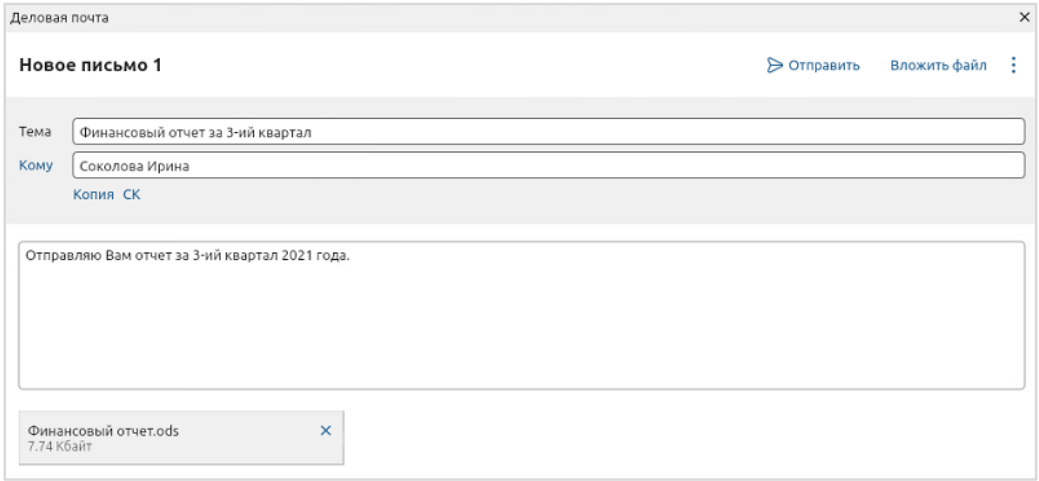
ViPNet Client 5.
Что нового



- Многофакторная аутентификация
- Несколько профилей на устройстве
- Интеграция с ViPNet EPP (МЭ 4В ФСТЭК) + Compliance (ZTNA) – Блокировка трафика в случае отсутствия EPP или выключенных модулей защиты
- Поддержка Деловой почты
- Новые ГОСТы по криптографии
- SDK для сторонних приложений

ДОПОЛНИТЕЛЬНО:
Деловая почта Windows → Linux

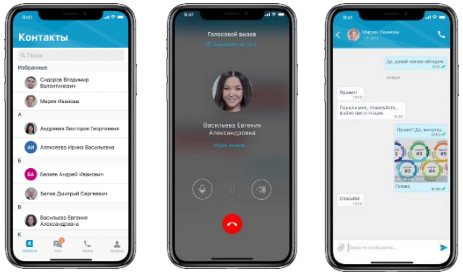
- Встречная работа с **ViPNet Деловая почта** для **ОС Windows**
- Поддержка **ОС Linux** из списка поддержки продукта **ViPNet Client 4U for Linux**
- Прикладное шифрование писем и вложений
- Новый UI в современном стиле
- Отдельный модуль автопроцессинга



ДОПОЛНИТЕЛЬНО:
Защищенные коммуникации сотрудников

Решение:

ViPNet Connect



Что замещаем:

- Slack
- WhatsApp
- …

Особенности:

Функционал мессенджера:

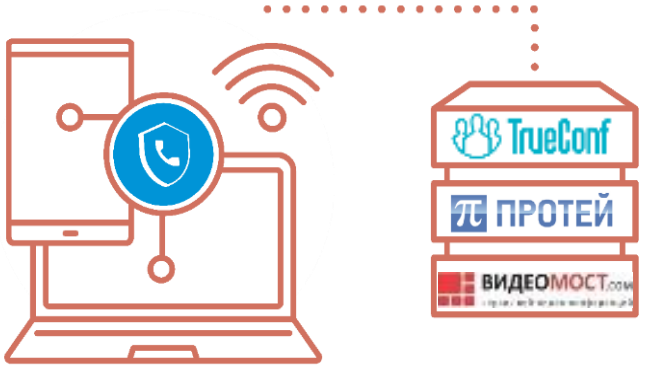
- Чаты, пересылка файлов
- Групповые чаты
- Видеозвонки (напрямую)
- Транслировать свой экран другому пользователю в рамках видеосвязи

* **Сервер чатов – в периметре организации**

ДОПОЛНИТЕЛЬНО:
ViPNet Connect – дополнительные возможности

- Интеграция с SIP

- Интеграция с ВКС



ПМДЗ ViPNet SafeBoot

ViPNet SafeBoot

Программный модуль доверенной загрузки

Устанавливается в UEFI BIOS различных производителей

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

Сертификат ФСТЭК России № 4673

Сертификат ФСБ России № СФ/527-4669

Команда исследователей обнаружила утилиту для перепрошивки BIOS, подписанную UEFI-сертификатом Microsoft. Утилита предназначалась для планшетов DT Research, но т.к. она подписана сертификатом Microsoft, ее можно применить для любой системы.

Найденная уязвимость CVE-2025-3052 представляет огромную опасность для всех UEFI платформ, использующих Secure Boot и стандартные сертификаты Secure Boot (в PK, KEK, db)

ViPNet EndPoint Protection

infotecs

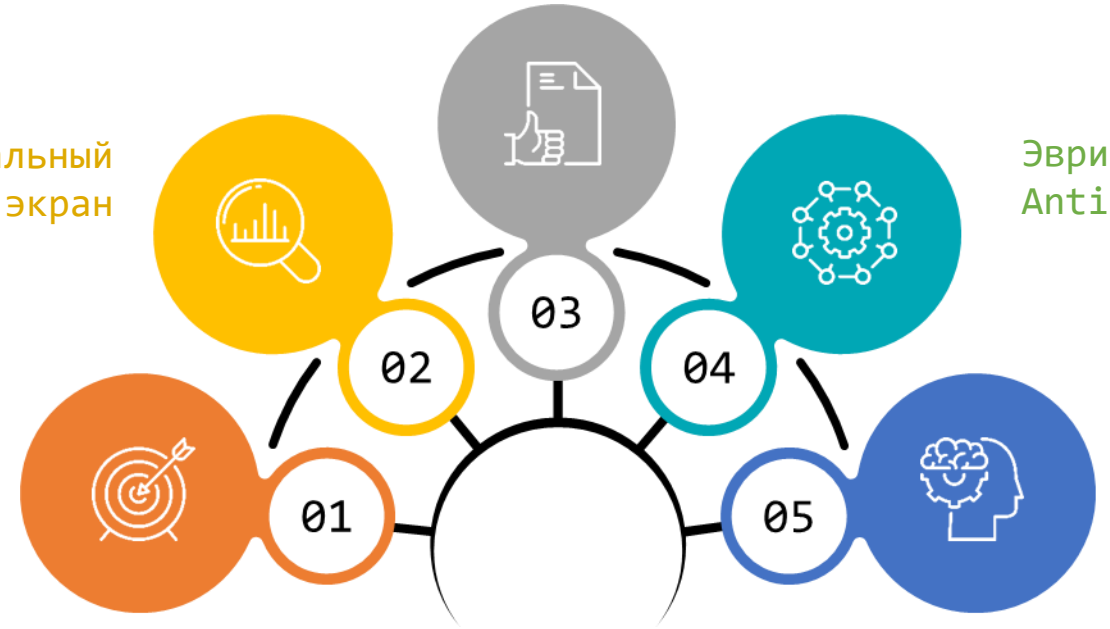
Контроль приложений

Персональный межсетевой экран

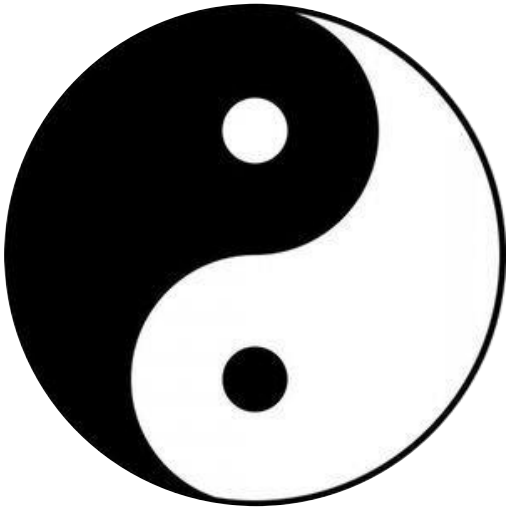
Эвристический Antimalware движок

Система обнаружения и предотвращения вторжений

Модуль поведенческого анализа



ViPNet EndPoint Protection (EPP) – комбинирование методов защиты

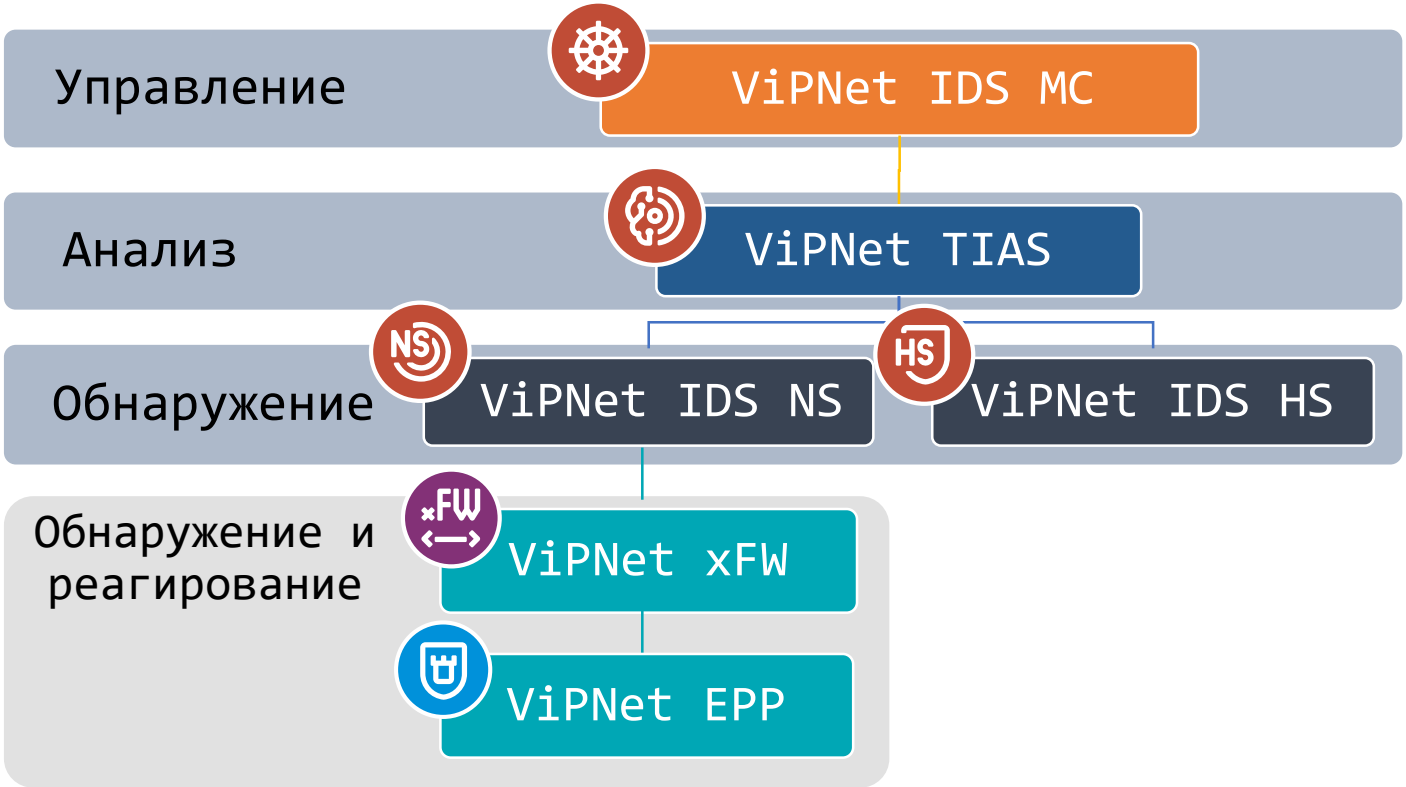


- Сигнатурные методы защиты:
  - правила белого/чёрного списка
  - правила для HIDS/HIPS
  - фильтры межсетевого экрана
- Эвристические методы защиты:
  - Поведенческий анализ
  - Эвристический антивирус (NGAV - бессигнатурный)
  - Математические модели построенные при помощи искусственного интеллекта
- Средства мониторинга и передача событий для последующего анализа

Функции из стека технологий ZTNA ViPNet EPP

- Проверка соответствия хоста на наличие необходимого/требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения, защита реестра
- Блокировка входа в защищенную сеть ViPNet при несоответствии устройства политикам ZTNA, информирование пользователя об этом
- Контроль сетевой активности приложений

3. Решения для обнаружения атак

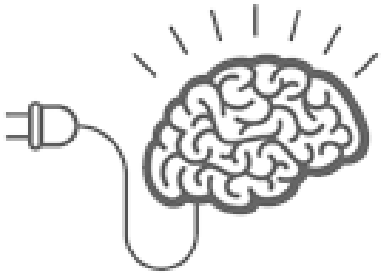


Как это работает?

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

Множество событий ИБ

Модуль анализа *
ViPNet TIAS



Выявление критических событий (инцидентов)

Обработка в SOC

Обработка инцидентов

Статистика и отчеты

Особенности IDS:

- Самообучаемая нейросеть

Особенности TIAS:

- Модель **ИИ** с наставником

* **Первое СЗИ с признаком ИИ в Реестре**

Базы решающих правил для СОВ

Февраль 2022 – отключение иностранных сервисов обновления БРП

Cisco

(VRT, Talos)

- Более 30 000 сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США

ET

(Emerging Threats Pro)

- Более 30 000 сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США

~~StoneSoft~~

ИнфоТеКС

(AM Rules)

- Более 24 000 сигнатур(14 000 собственных)
- ZeroDay сигнатуры
- Страна происхождения: Россия

Новый продукт

infotecs

AML - Web application ~~firewall~~ IDS

Рисунок 1
Пакетный режим

Рисунок 2
Потоковый режим

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

Решения:

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

Особенности:

- Поддержка ГОСТ, иностранных криптоалгоритмов
- Класс КС1 и КС3
- Возможность организации внутренней среды доверия
- Возможность интеграции со СМЭВ

ViPNet PKI Service – ядро УЦ Федерального Казначейства

ViPNet PKI Client – УЦ ФНС России для юр лиц и ИП

ViPNet TLS.
Доступ к защищаемым ресурсам

infotecs

Продукт:

- ViPNet TLS Gateway

Функции:

- Одно/двусторонний TLS
- ГОСТ криптография
- AES/RSA криптография

Ключевые особенности:

- Сертификат ФСБ России КС1-КС3, ПО и ПАКи в реестрах
- Легитимная работа **с любым СКЗИ у пользователя** (ViPNet, КриптоПро, Валидата)
- Легитимная работа **с ГОСТ- и RSA шифрованием**
- Высокая производительность:

Характеристика	Значение
Кол-во единовременных соединений	**> 155 000**
Возможность кластеризации	**До 64 нод в кластере**
MAX одновременных подключений для 64 нод	**До 9 920 000**
Варианты исполнения	**ПАК (СКЗИ КС3)** **VA (СКЗИ КС1)**

Успешный опыт:

- Проект «Цифровой рубль»
- УЦ Федерального Казначейства
- ГОСТЕХ

ViPNet PKI Service: высокопроизводительный сервер подписи/шифрования

infotecs

Продукт:

- ViPNet PKI Service

Функции:

- Проверка/простановка ЭП, шифрование/расшифрование сообщений
- Централизованное хранение и генерация ключей
- Взаимодействие с информационными системами через REST API

Ключевые особенности:

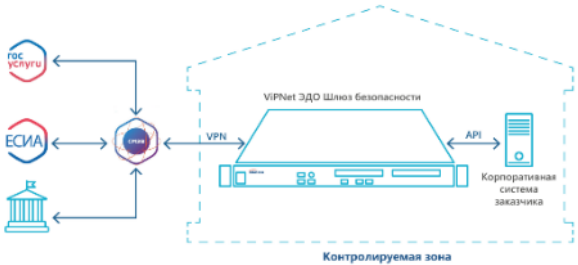
- Экономия за счет реализации всех функций в едином ПАК
- Легитимная возможность работы с неограниченным кол-вом сертификатов разных внешних систем и пользователей
- Высокая производительность + возможность кластеризации:

Размер сообщения/файла	Производительность на 1 ПАК
до 2 Кб	> **10 000** сообщений /секунду
до 100 Кб	> **4 000** файлов/секунду
до 1 Мб	> **700** файлов/секунду

Успешный опыт:

- Проект «Цифровой рубль»
- УЦ Федеральнгого Казначейства
- ГИС «Электронные перевозочные документы»

Шлюз для СМЭВ/ЕСИА. Подключение ИС Заказчика к СМЭВ/ЕСИА



Продукт:

- ViPNet EDI

Функции:

- СКЗИ и средство ЭП для идентификации пользователей мессенджера в ЕСИА, ЦПГ, ЦПО, **поддержка OpenIDconnect**
- Проставление и проверка ЭП по классу КС3
- Подключение к СМЭВ **без необходимости оценки влияния**

Ключевые особенности:

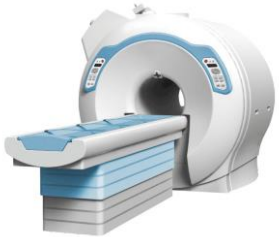
- Возможность работы в режиме proxy или xsd
- Зарегистрирован в реестре российского ПО, рестре Минпромторга и реестре ПАК Минцифры

Успешный опыт:

- ГИС в ГЕОП
- СФР

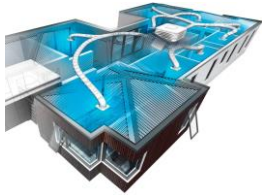
5. Информационная безопасность для «умного» оборудования. Актуально?

Современное оборудование



Обеспечивающие системы

СКУД



Система вентиляции

Система пожаротушения

Управление лифтами

Электро питание

На примере ИТС. Точно надо защищать?

14 апреля 2022 г.

Красноярск

ТОИ - Табло отображения информации

Средства защиты информации индустриального уровня

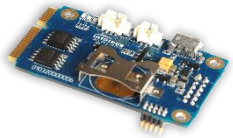
Наложенные средства

Аппаратные

Встроенные средства

Программные

КриптоКлиенты



Аппаратные

Индустриальное исполнение СКЗИ/МЭ 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

Встраивание программного vpn-клиента в «умные» устройства

Пример: 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

Защита данных в индустриальных системах с помощью протокола CRISP

CRISP : Протокол защищенного обмена для индустриальных систем
(Утвержден Приказом Росстандарта от 15 февраля 2024 г. № 235-ст. ГОСТ Р 71252-2024)

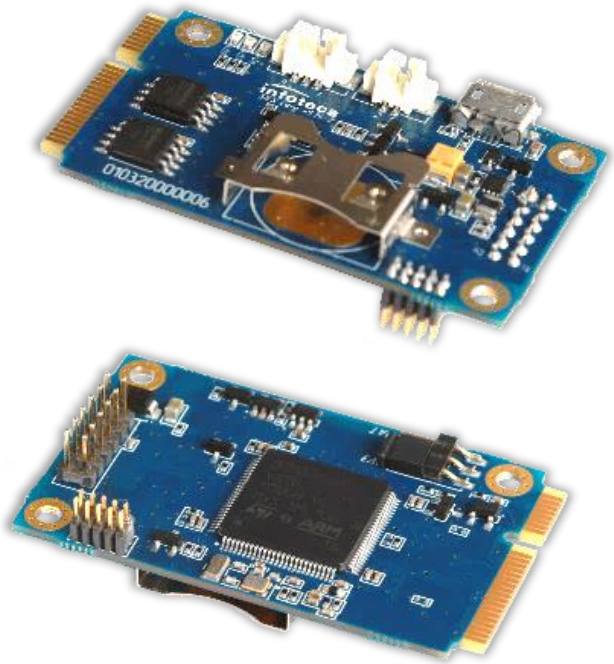
Что обеспечивает:

- Целостность
- Конфиденциальность (опционально)
- Защиту от навязывания повторных сообщений
- Аутентификацию источника сообщений

Особенности:

- Защита адресных и групповых сообщений
- Бессесионный криптографический протокол
- Минимальный оверхед и минимальная нагрузка на сеть
- Реализован в сертифицированных продуктах ViPNet SIES

ViPNet SIES Core – защита сообщений (команд, измерений)



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

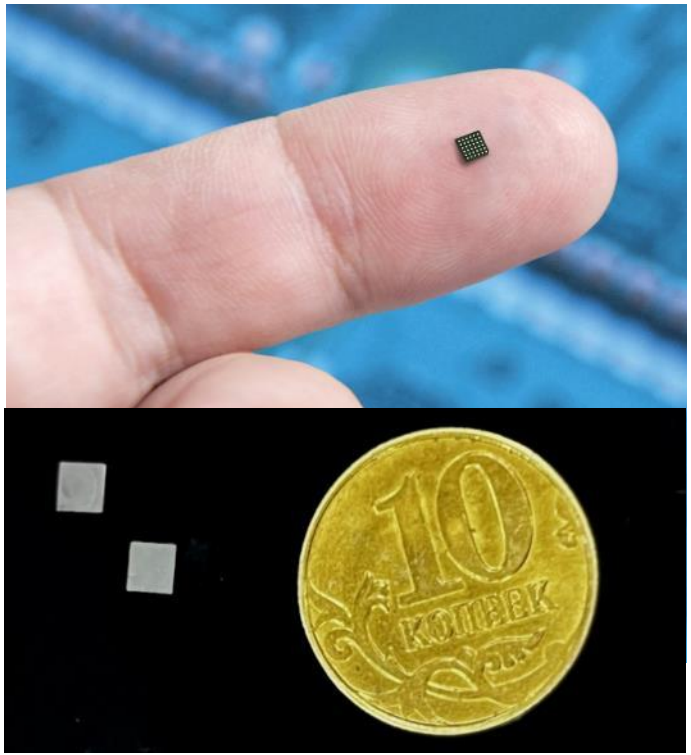
Функциональные особенности:

- 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 сообщений(команд, измерений)



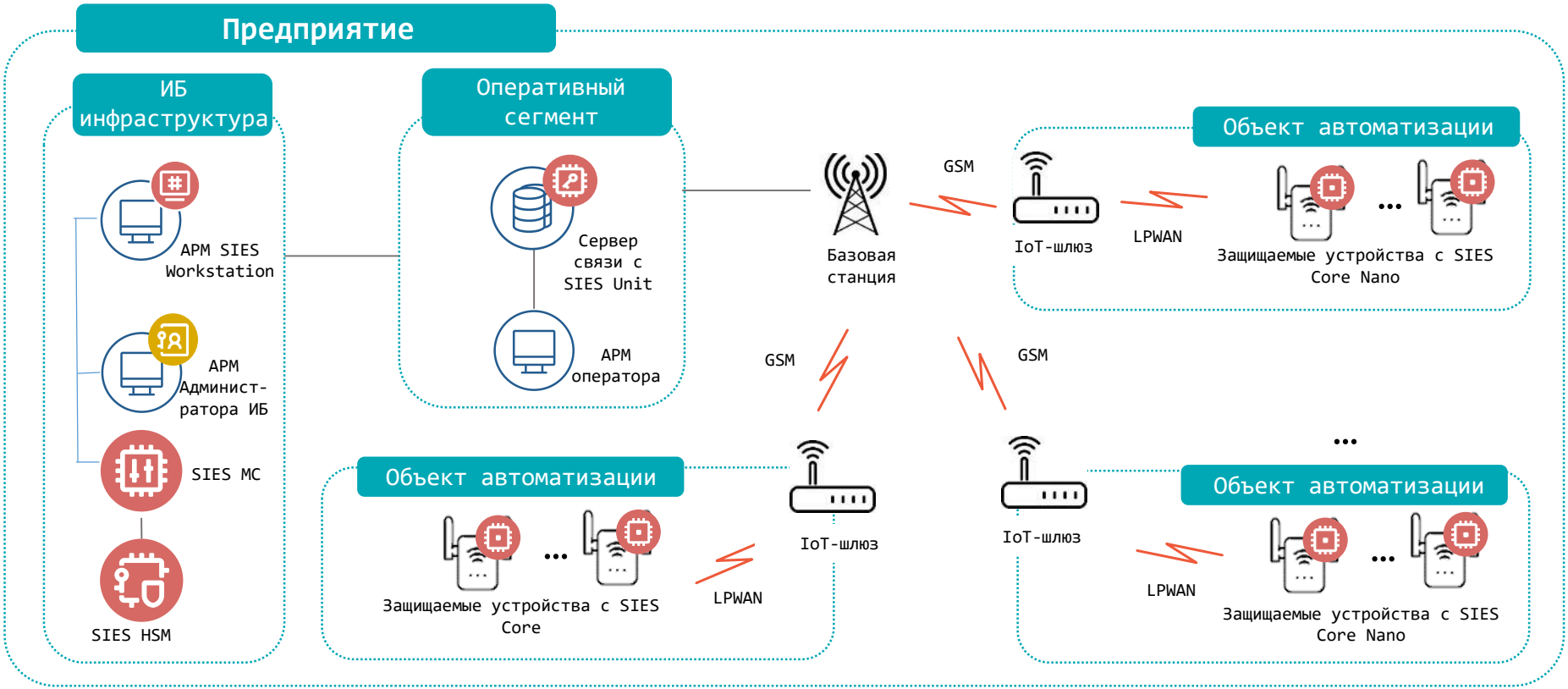
Встраивание:
- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

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^{0}C
- Форм-фактор – микросхема 3x3x0,4 мм

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

Типовые схемы защиты информации в индустриальных системах (IIoT)



Александр Реунов, ra@infotecs.ru
Сергей Дурягин,dsa@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363