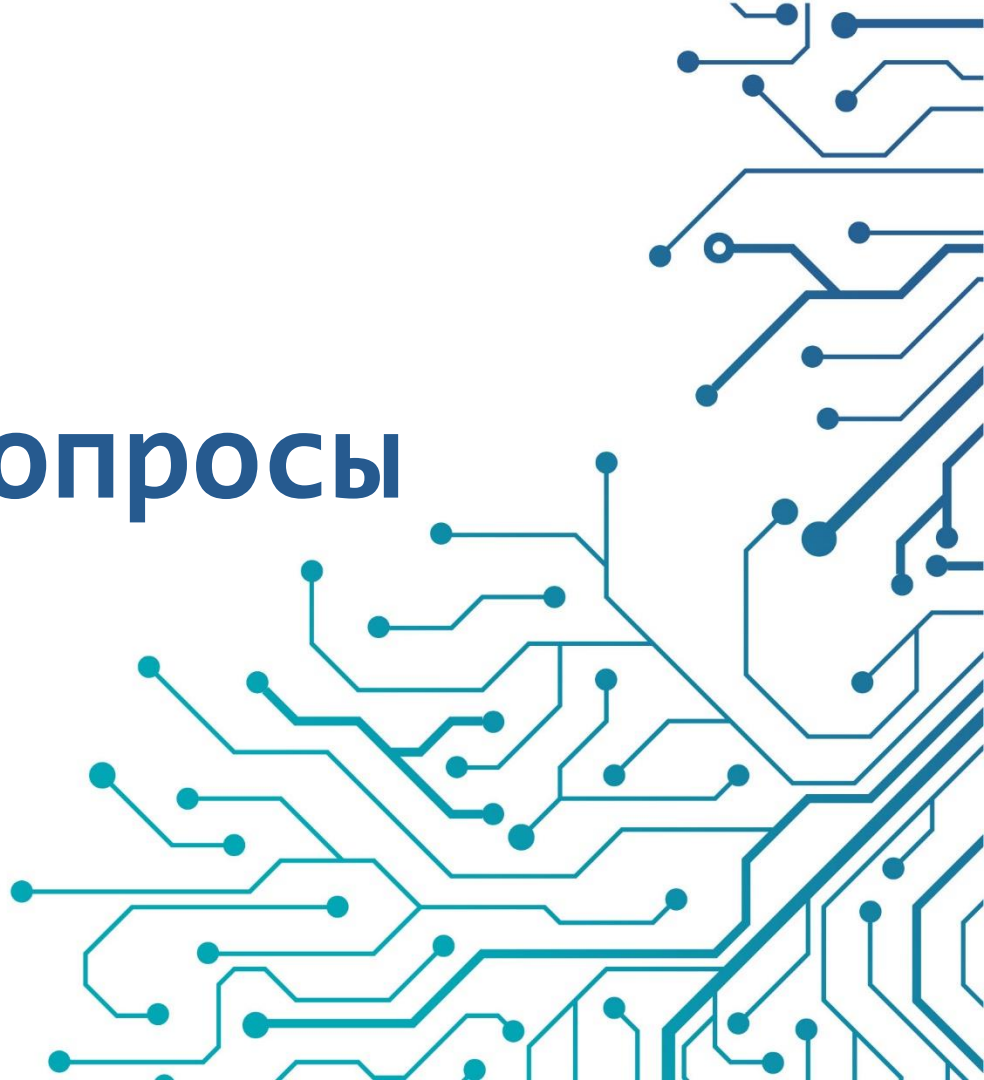


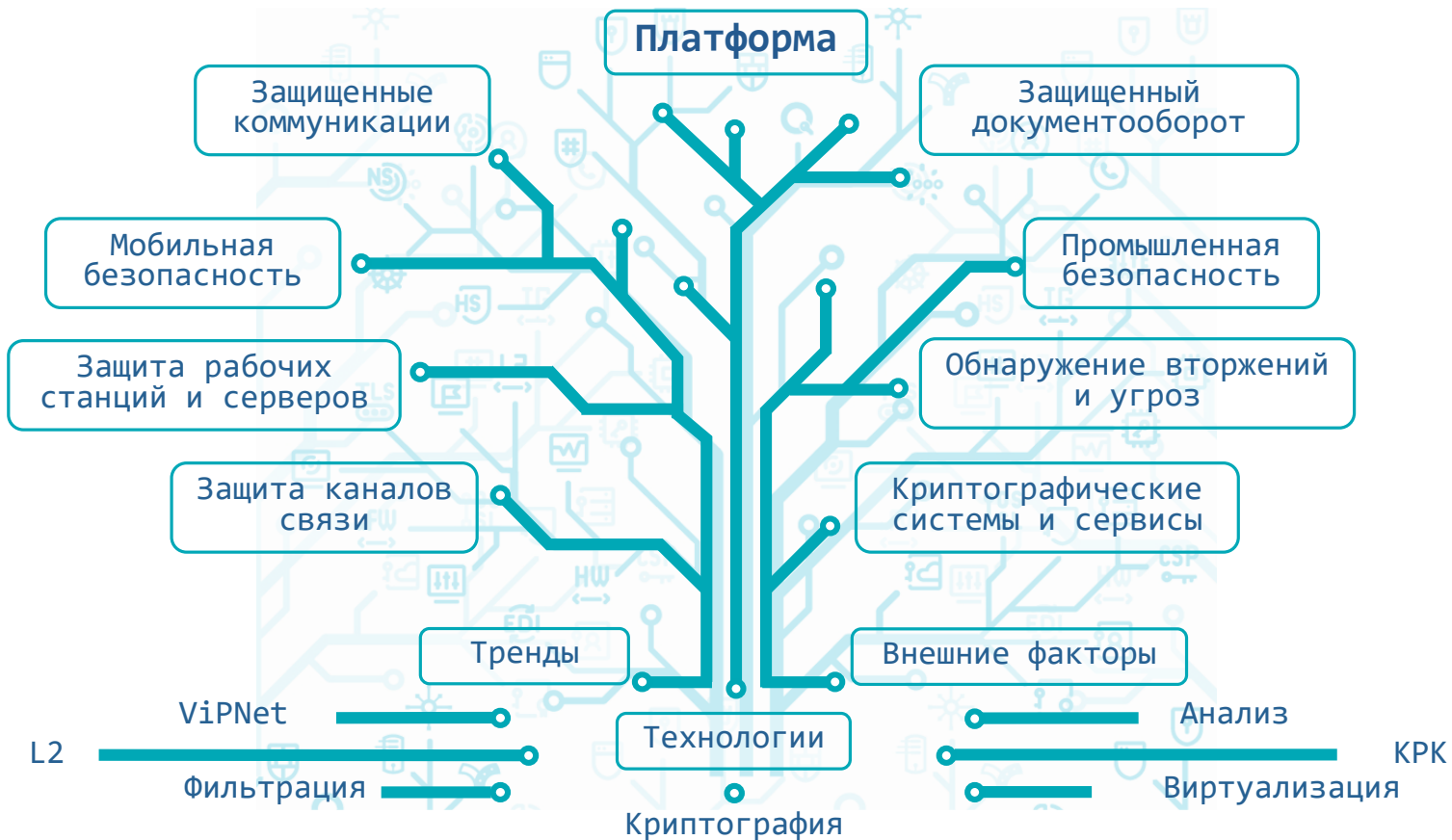
ИнфоТеКС: актуальные вопросы

Хабаров Иван


infotecs



Экосистема ViPNet

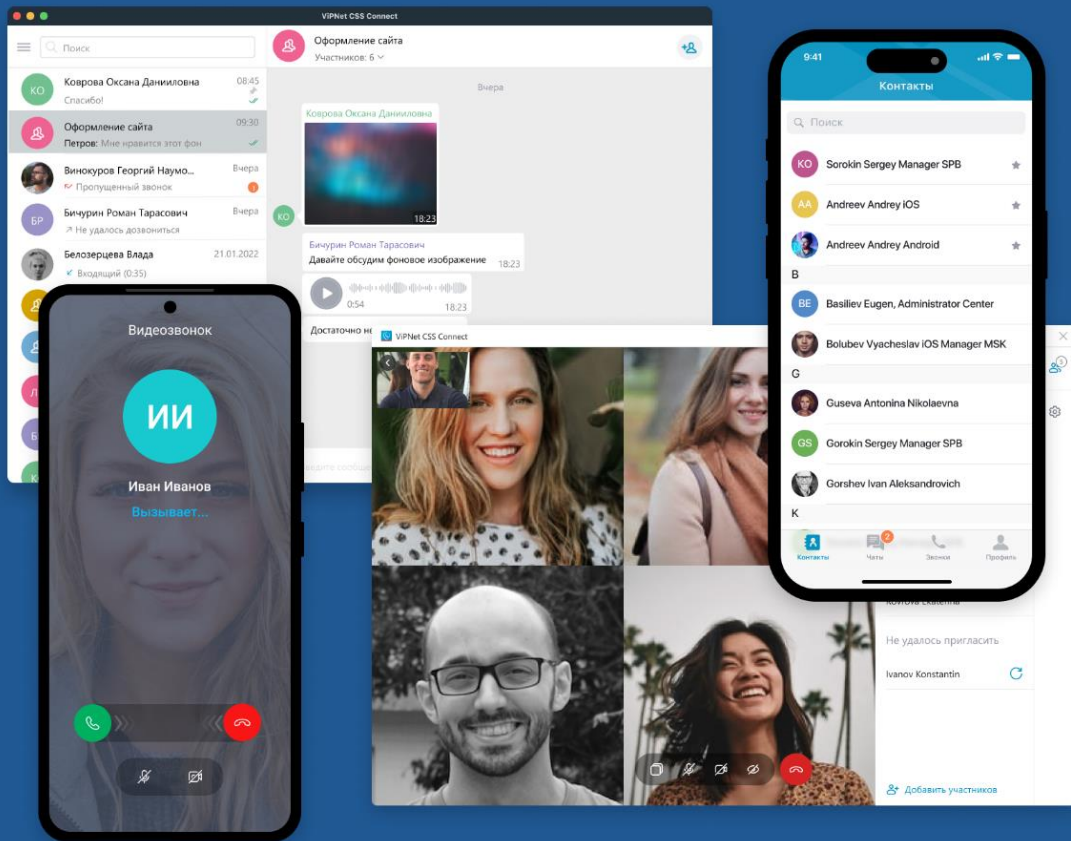


The logo for infotecs, featuring the word "infotecs" in a dark blue, lowercase sans-serif font. A red curved line is positioned above the "i" and "o".

infotecs

Корпоративный мессенджер

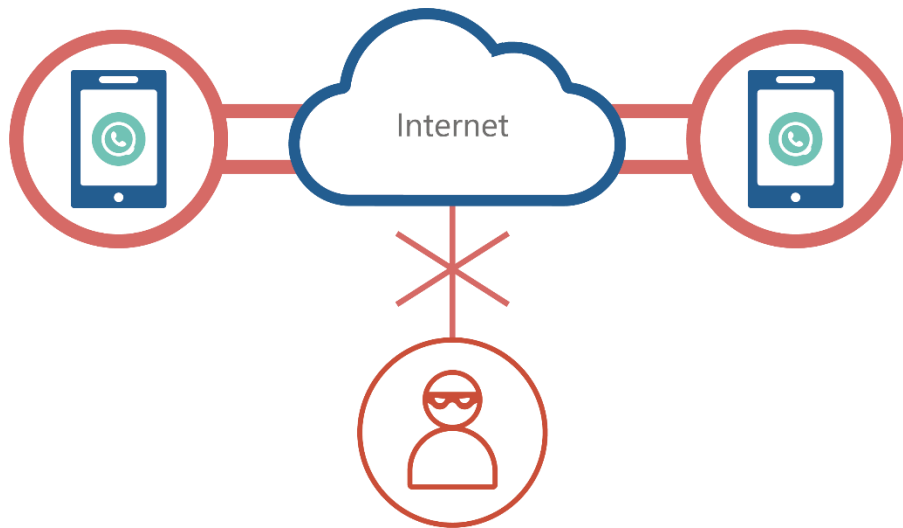
ViPNet CSS Connect ВОЗМОЖНОСТИ



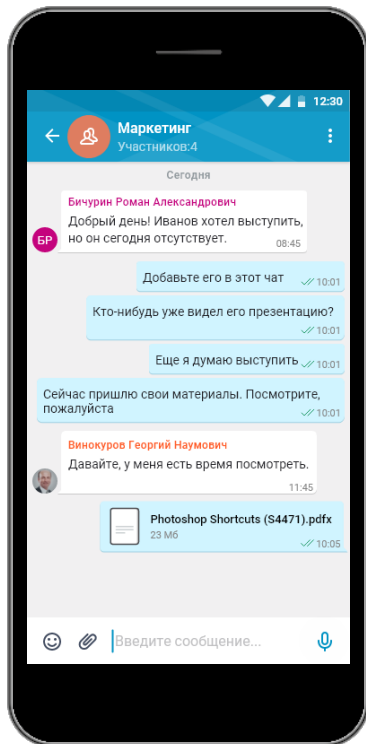
ViPNet CSS Connect обеспечивает голосовые коммуникации, видеосвязь, отправку текстовых сообщений и файлов со стационарных компьютеров, ноутбуков и мобильных устройств, а также интеграцию с SIP телефонией и ВКС

Абонентское шифрование точка-точка

Все коммуникации осуществляются по защищенным каналам связи, в том числе при передаче в локальной сети, что исключает возможность перехвата защищаемой информации как внешними, так и внутренними нарушителями



VIPNet CSS Connect. Возможности



VIPNet CSS Connect позволяет защищенно обмениваться сообщениями и файлами в личных чатах с другими пользователями приложения благодаря прямому обмену шифрованными данными без использования промежуточных серверов

Также вы можете:

- редактировать и удалять сообщения
- вставлять файлы и изображения из буфера обмена
- перетаскивать файлы из других чатов
- комментировать сообщения
- искать сообщения по конкретному чату и по всем чатам

и многое другое

Интеграция с SIP инфраструктурой



VIPNet CSS Connect обладает возможностью интеграции с инфраструктурой доверенных SIP-серверов заказчика, что позволяет встроить его в существующую систему IP-телефонии

Данные в вашей корпоративной сети – это только ваши данные

СообщенияЗвонки

Ваши данные принадлежат вам

Корпоративные сообщения, звонки и видеозвонки не покидают вашу защищенную корпоративную сеть

Видеозвонки



Защищенный смартфон

Hardened Smartphone

Защищенный смартфон Hardened Phone

Мощный, безопасный и конфиденциальный смартфон для корпоративных клиентов



Создан на основе защищенной ОС GrapheneOS

Доверенные приложения

Производительные аппараты

Постоянный доступ через VPN

Защита от удаленного доступа

Безопасный корпоративный мессенджер

Защита от физического доступа

Мониторинг с использованием алгоритмов машинного обучения

Защита от слежки

Доработка под желания заказчика

Защита каналов СВЯЗИ

4G - 5G

4 поколение - до конца 2025 г
(в реальности и дольше)

5 поколение появится в рынке в 2024 г
(для новых информационных систем)

С 2025 г можно будет мигрировать сети в
максимально возможном бесшовном режиме
(будет цикл вебинаров по миграции начиная с этого года)

The logo for infotecs, featuring a red curved line above the word "infotecs" in a dark blue sans-serif font.

VIPNet Coordinator HW 5

Новое поколение
ШЛЮЗОВ
безопасности

The logo for infotecs, featuring a red curved line above the word "infotecs" in a dark blue, lowercase sans-serif font.A large teal circle containing the word "Prime" in a white, bold, sans-serif font, centered within the circle.

Prime

Принципы системы управления следующего поколения

01

Единая система управления

Для всех решений ViPNet

02

Безопасность вездеЕдиная область объектов
(узлы, пользователи, приложения...)

03

Интегрированное управление

Взаимодействие подсистем

04

Прозрачность

Точное понимание происходящего

05

Управление доступом

Гибкая ролевая модель

06

Скорость управления

Эффективная эргономика UI, автоматизация

07

Стандартизация

Протоколы и API

08

Масштабируемость

Под любые задачи

09

Доверие

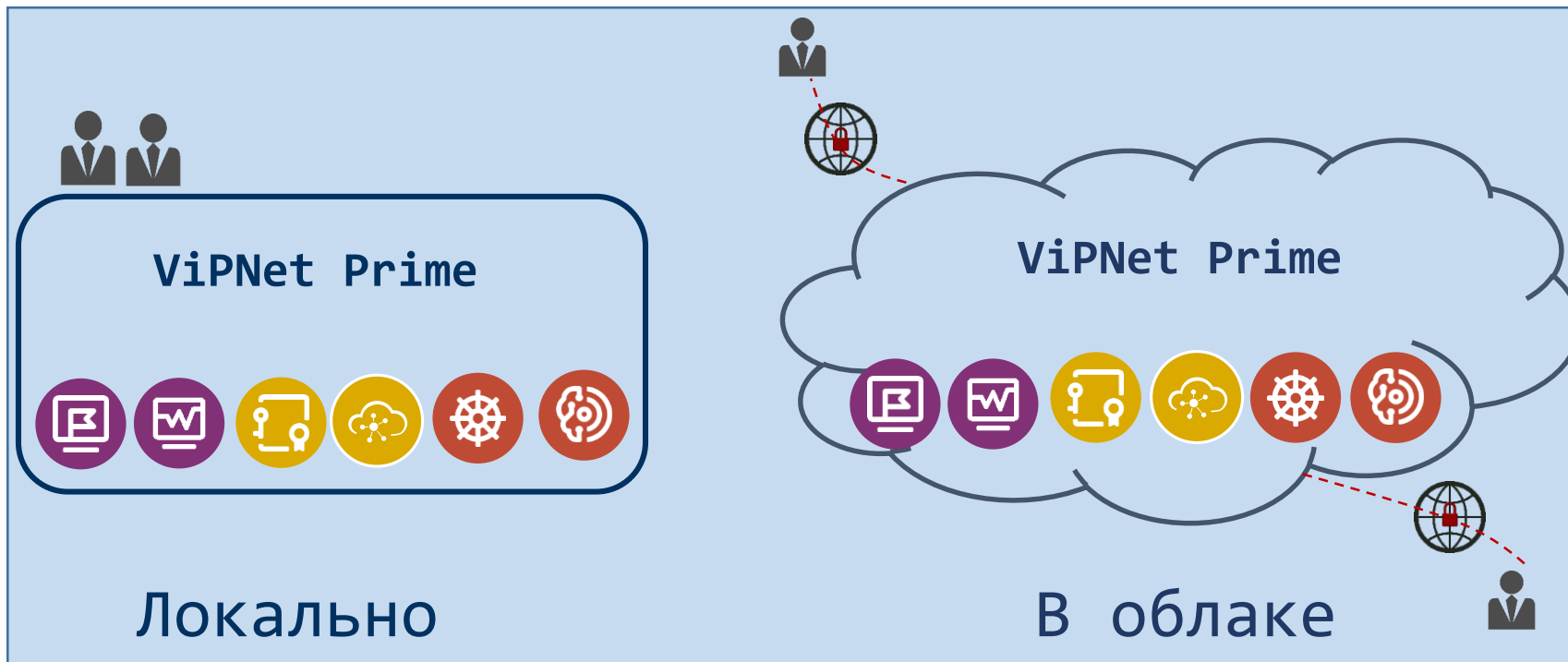
Сертификация, безопасность, Linux

10

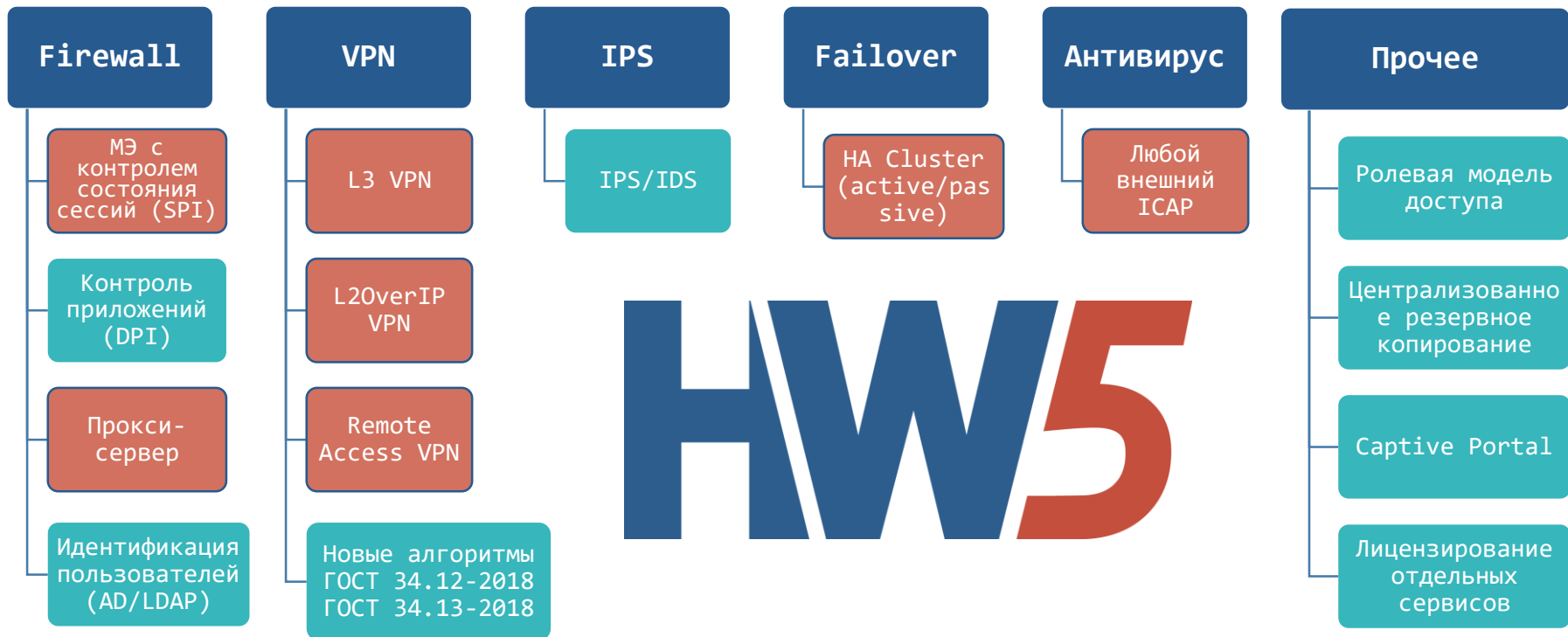
Поддержка сервисной модели

Мультиарендный доступ и контроль

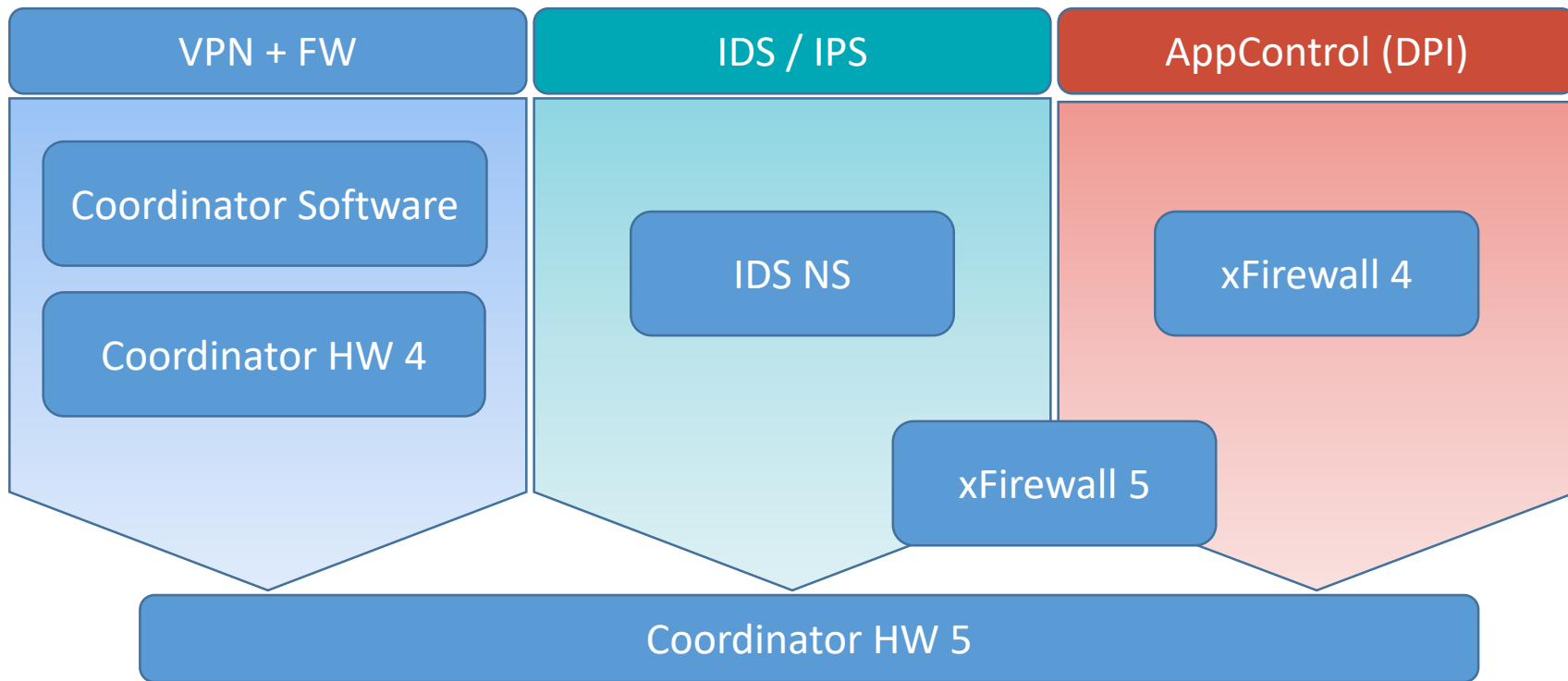
Принципы системы управления следующего поколения



ViPNet Coordinator HW 5



Шлюзы безопасности ViPNet



Требования по сертификации

ФСБ России

- СКЗИ класса КСЗ
- СКЗИ класса КС1 (исполнение VA)
- Межсетевой экран 4 класса
- СОА класса ВП

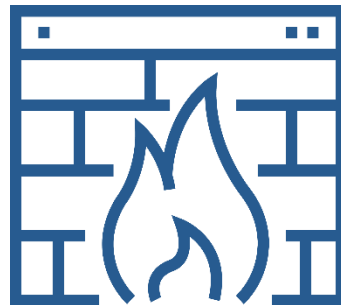
ФСТЭК России

- Межсетевой экран тип «А» 4 класса
- Межсетевой экран тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации



Межсетевое экранирование

- Внедрение технологии DPI (контроль приложений)
- Идентификация пользователей с использованием:
 - Microsoft Active Directory
 - Captive Portal с LDAP каталогом
- Повышение производительности МЭ
- Единый идентификатор правил МЭ



Предотвращение вторжений (IDS/IPS)

















Предотвраще ние вторжений (IDS/IPS)

Предотвращение вторжений (IDS/IPS)

 VIPNet Coordinator VA

Журнал регистрации IP-пакетов

Фильтр IP-пакетов ▾ Результат фильтрации в интервале с 01.07.2021

Пользоват...	Приложение	Прикладной протокол
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP
 ← Нет данных	Неизвестно	HTTP

Заблокировано IPS

Код события 142 - Заблокирован IPS подсистемой как вредоносный

Обработка по правилам предотвращения вторжений

Правило: ["AM WEB_CLIENT NETGEAR ProSafe Network Management System Arbitrary file download"](#)

Группа: web_client
Класс правила: web-application-attack
Идентификатор: 1.3001501.12


Результат анализа

Пользователь сети: Нет данных
Приложение: unknown
Прикладной протокол: HTTP





Агрегация пакетов за интервал

Начало интервала: 16 Авг 2021, 17:03:16
Конец интервала: 16 Авг 2021, 17:03:16
Количество пакетов: 1
Размер: 366 байт

Свойства IP-пакета

Источник: 66.254.33.10 : 59418
Назначение: 192.168.1.200 : 80
Транспортный протокол: 6-TCP
Сетевой интерфейс: eth2
Направление:  Входящий
Тип: Открытый
Тип адреса: Одноадресный
Трансляция: Нетранслированный
Ethernet-протокол: 800h

Закрыть

   | Показано 16 записей | 

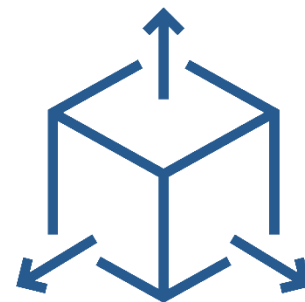
Размер	Событие	Фильтры и правила
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
0	67 - Отмечен IPS подис...	"FTPP FTP INVALID CMD"
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...
366	142 - Заблокирован IPS ...	"AM WEB_CLIENT NETGE...

Вкл Блокировать

Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPsec – протокол безопасности сетевого уровня

TK 26 P 1323565.1.034-2020 «Информационная технология.
Криптографическая защита информации. Протокол безопасности
сетевого уровня»



Развитие ролевой модели

Система

- Системные и сетевые настройки
- Прикладные сервисы

МЭ

- Управление фильтрами
- Задание правил трансляции

VPN

- Работа с ключевой информацией
- Управление VPN сервисами

IPS

- Управление БРП
- Работа с событиями



Спасибо за внимание!

Иван Хабаров
ivan.khabarov@infotecs.ru
+7-909-807-35-05

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363



В любой не понятной ситуации
решение это ViPNet

Иван Хабаров

ivan.khabarov@infotecs.ru

+7 909 807-35-05

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363