

VIPNet Coordinator IG 5: новое поколение продукта

Марина Сорокина
Руководитель направления

ViPNet Coordinator IG 5



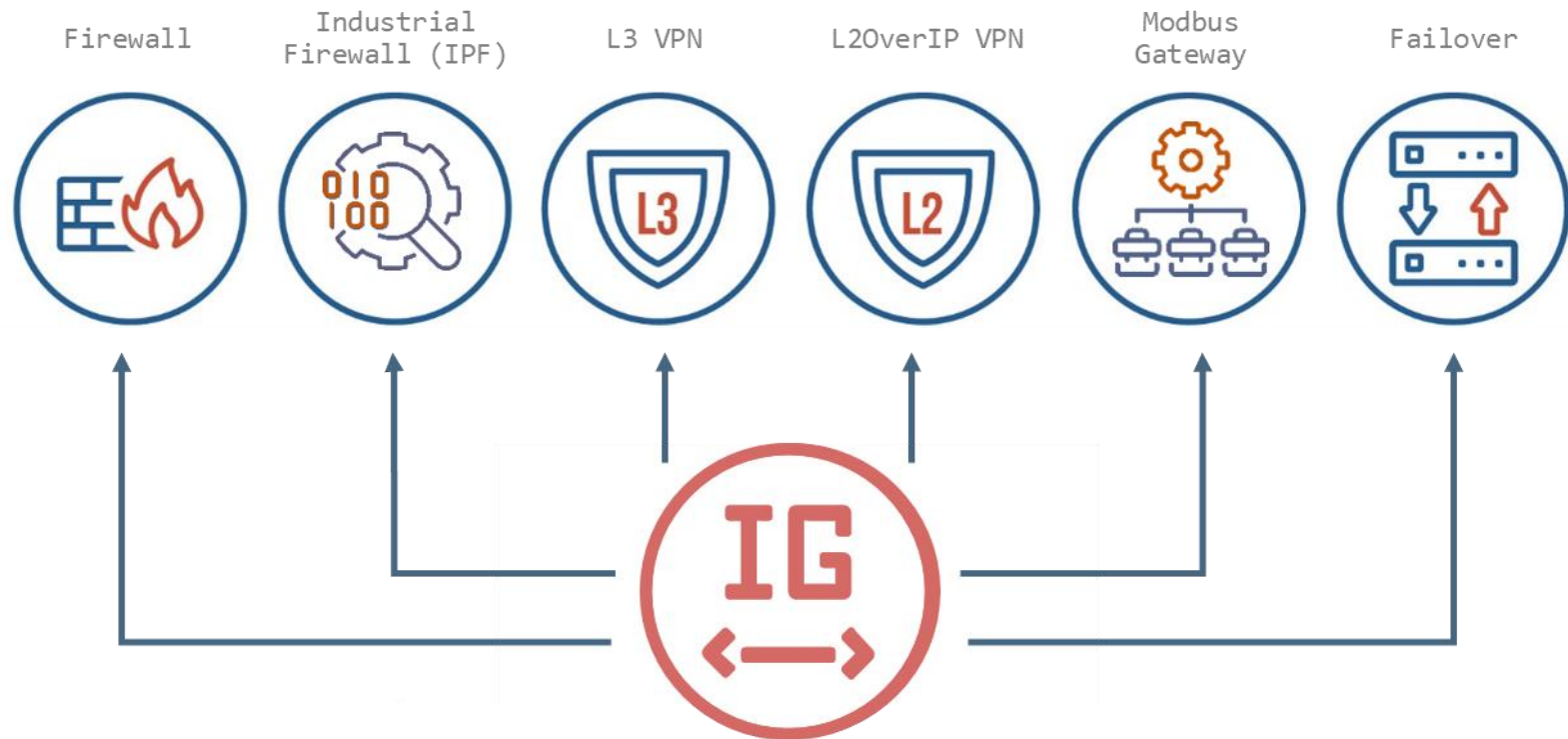
Линейка промышленных межсетевых экранов нового поколения (NGFW). Позволяет защитить промышленную инфраструктуру от несанкционированного доступа, своевременно обнаружить и предотвратить атаки на промышленные сети, организовать защищенные соединения.

ViPNet Coordinator

IG 5.1

ViPNet Coordinator IG 5.1

Выпущен в декабре 2023 г.



ViPNet Coordinator IG 5.1: ИСПОЛНЕНИЯ



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG100 I4

Только в рамках обновления с
Coordinator IG4

Новые поставки и обновление с
Coordinator IG4

Новая система управления

ViPNet Prime

Ядро

Ролевая модель
Лицензирование
Управление ПО

VPN

Управление
связями,
ключами

PMM

Управление
политиками
безопасности

NVS

Мониторинг
состояния
узлов

ViPNet Coordinator IG 5

L3 VPN, L2overIP VPN

Современные КРИПТОГРАФИЧЕСКИЕ Алгоритмы:

- «Кузнечик» и «Магма» (ГОСТ Р 34.12-2015, ГОСТ 34.13-2018)
- «ГОСТ 28147-89» для обратной совместимости

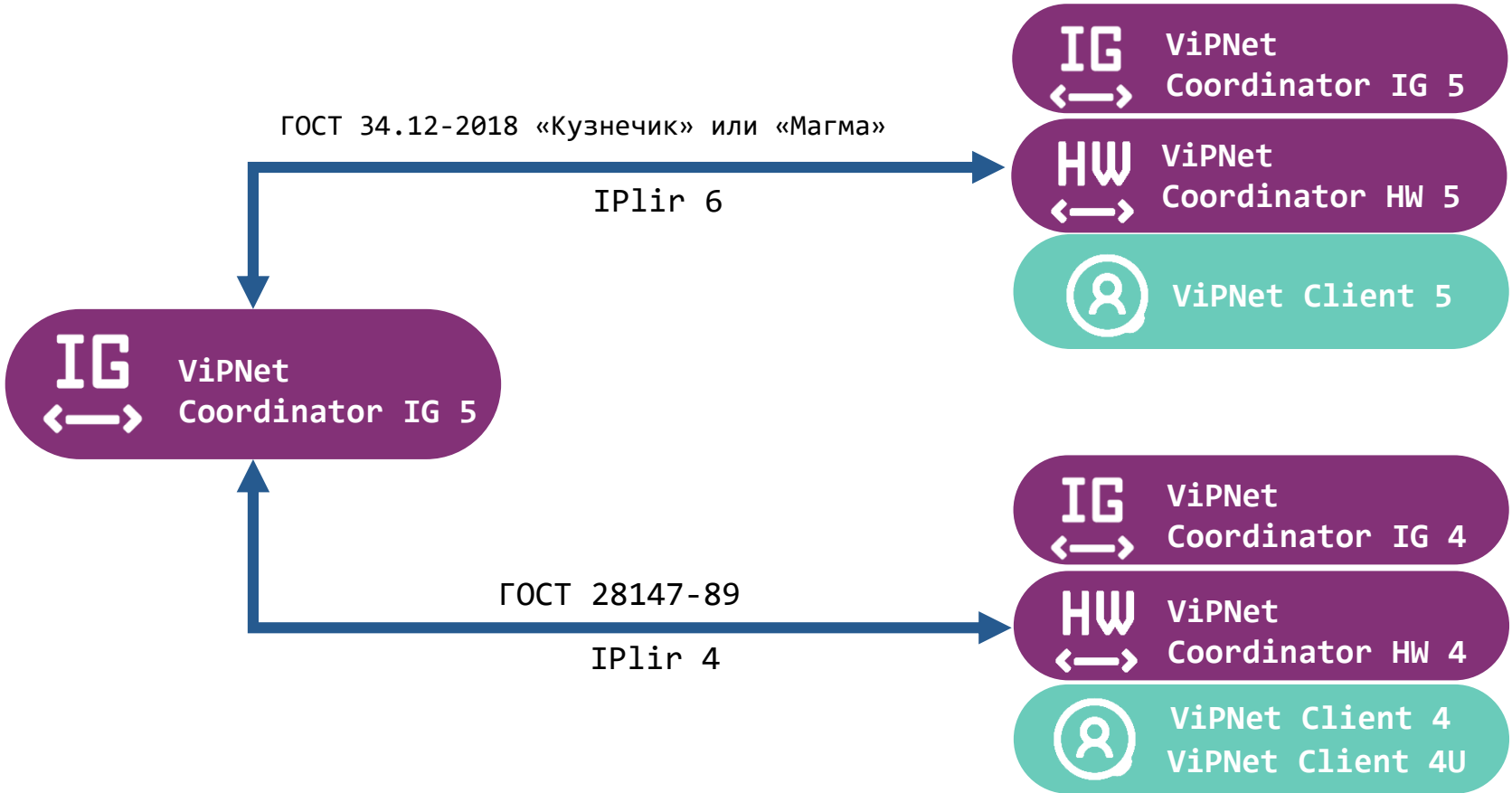
Рекомендованный TK26 КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ:

- IPsec 6 – протокол безопасности сетевого уровня

Сценарии обеспечения ИБ в соответствии с Приказами ФСТЭК России №239 и №31:

- Защита информации при передаче по каналам связи
- Обеспечение доверенных каналов и маршрутов
- Защита беспроводных соединений
- Реализация защищенного удаленного доступа
- Управление сетевыми потоками
- Соккрытие архитектуры и конфигурации автоматизированной системы

Обратная совместимость



Межсетевой экран и промышленный межсетевой экран

Название

Модуль FIREWALL

Назначение

- [+] Фильтрация сетевых соединений
- [+] сокрытие адресов и информации о структуре сети
- [+] Поддержка политик безопасности

Управление политиками

- [+] Локальное
- [+] Дистанционное

Название

Модуль INDUSTRIAL FIREWALL

Состав

- [+] Наборы правил под разные режимы работы системы:
 - [+] штатный режим
 - [+] Регламентное обслуживание
 - [+] специальный режим
- [+] Глубокая фильтрация пакетов промышленных протоколов по полям до уровня команд и их значений (Modbus TCP, МЭК 104)

Межсетевой экран и промышленный межсетевой экран

Сценарии защиты

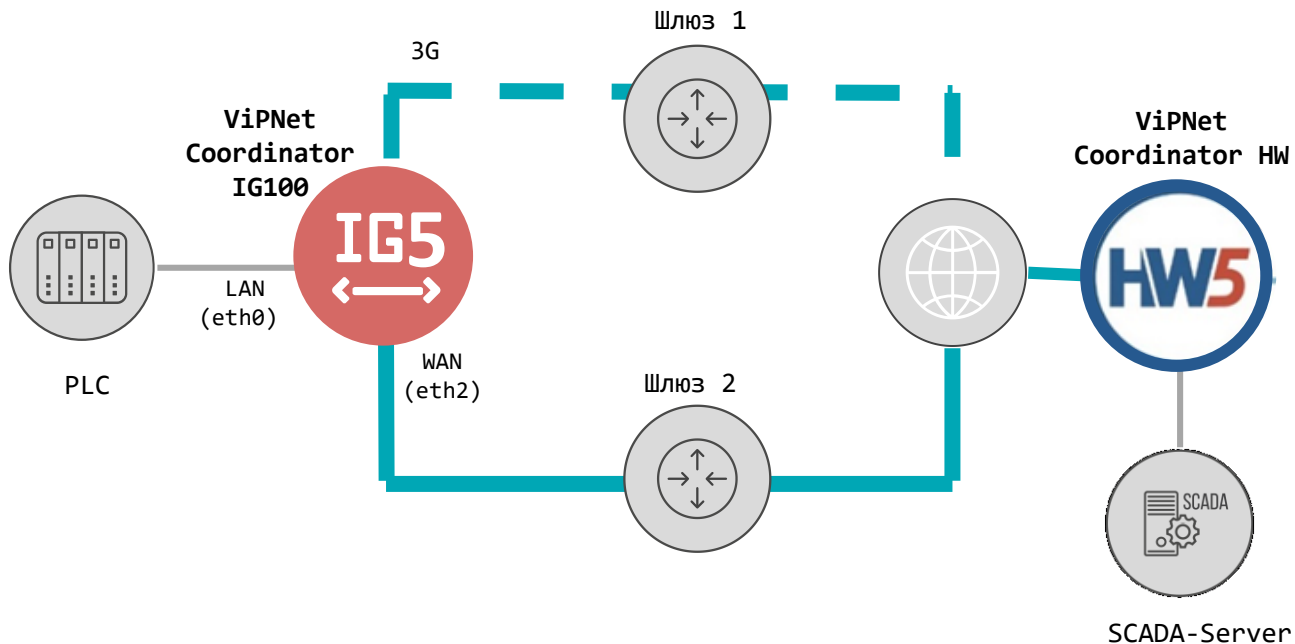
- Ограничение промышленного трафика определением допустимых промышленных протоколов для системы
- Контроль устройств в сети
- Контроль допустимых операций с оборудованием
- Контроль действий пользователей
- Сужение поверхности атак

Кластер высокой доступности



- Быстрое переключение кластера по потери питания
- Быстрое переключение кластера по потери связи, в том числе и для динамических интерфейсов
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- Минимальное время переключения до 1 секунды

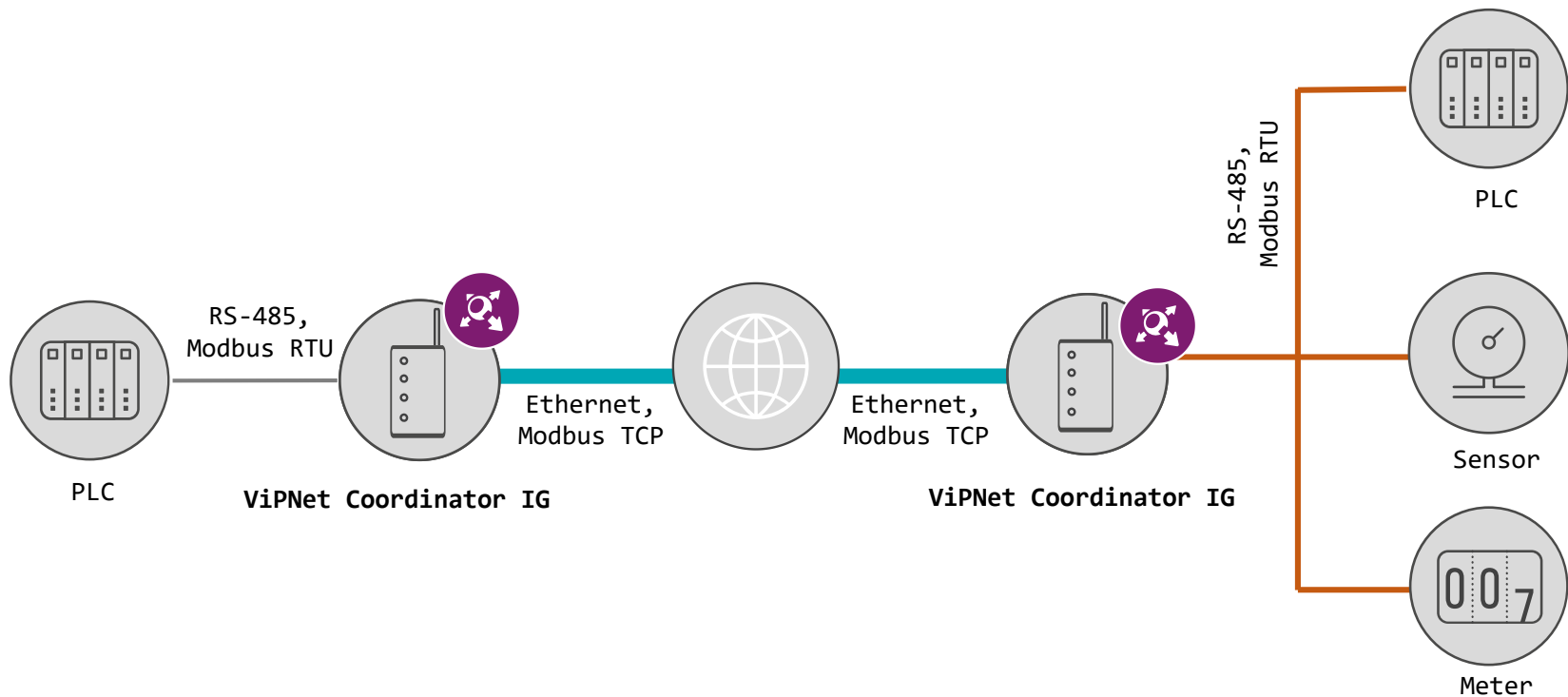
MultiWAN: резервирование каналов



Мониторинг работы каналов:

- Определение доступности шлюзов
- Определение основного шлюза, через который идет работа
- Передача информации по SYSLOG
- Передача информации по SNMP

Шлюз Modbus TCP-RTU и RTU-TCP





Входной сигнал

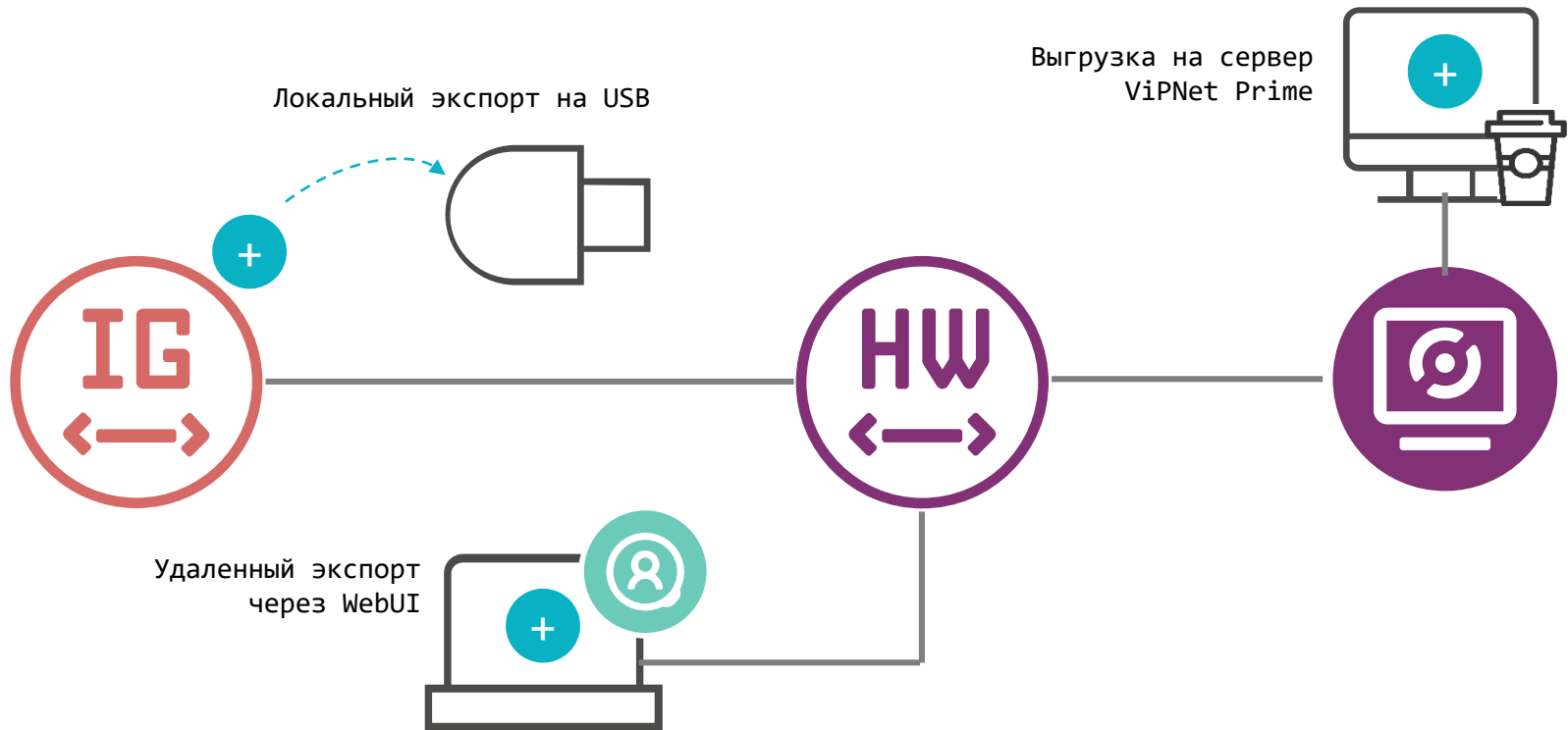
- Датчик вскрытия внешнего шкафа.
- Переключение режима работы МЭ типа Д.
- Сигнал с пользовательского устройства.



Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU.
- Индикатор событий:
 - работа в регламентном обслуживании;
 - работа в штатном режиме;
 - работа в специальном режиме;
 - вскрыт шкаф;
 - сигнал с пользовательского устройства.

Резервное копирование конфигураций



Изменение ролевой модели



Локальные учетные записи:

- Администратор
- Пользователь (Аудитор)

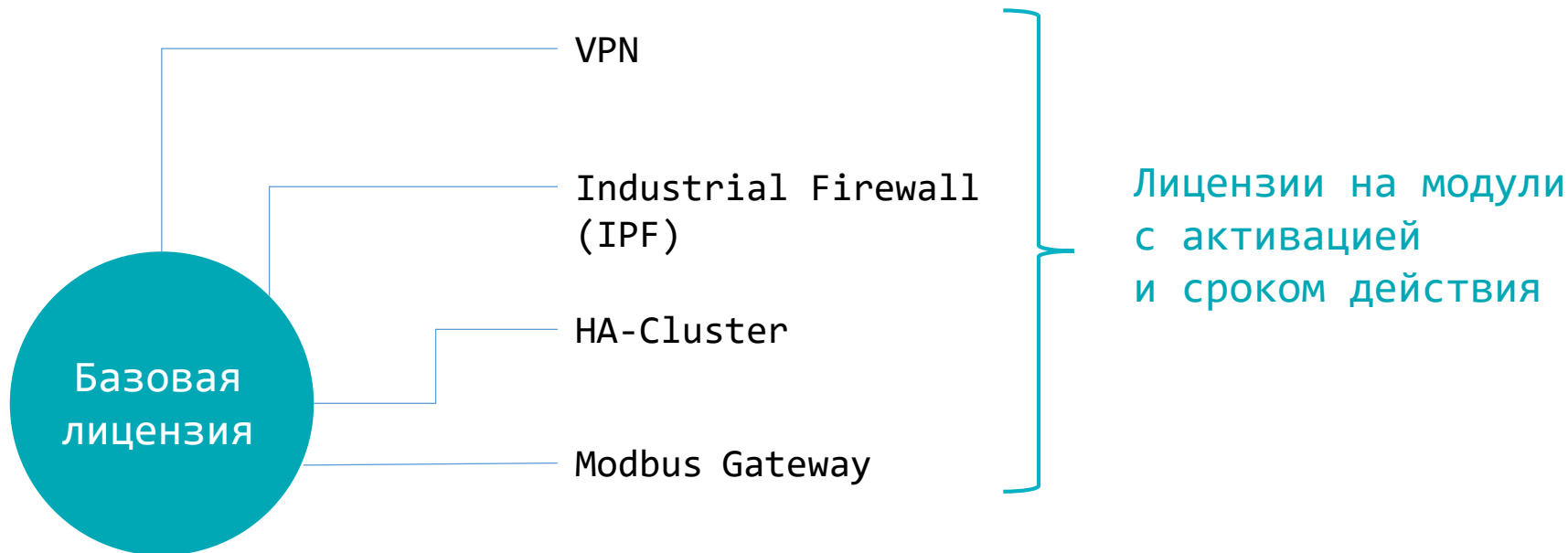
+



Централизованные учетные записи:

- Неограниченное количество
- Администратор/Аудитор
- Single Sign-On (SSO)
- Интеграция с AD через Prime

Новая схема лицензирования



Обновление ViPNet Coordinator IG 4 до ViPNet Coordinator IG 5

Набор лицензий
IG 5
после обновления:

- Базовая
- VPN
- IPF
- Modbus

ViPNet Coordinator IG10 I1

ViPNet Coordinator IG10 I2

ViPNet Coordinator IG100 I1

ViPNet Coordinator IG100 I4



ViPNet Coordinator IG10 I1

ViPNet Coordinator IG10 I2

ViPNet Coordinator IG100 I1

ViPNet Coordinator IG100 I4

ViPNet Coordinator
IG 4.5.1.1

ViPNet Coordinator
IG 5

Сертификация

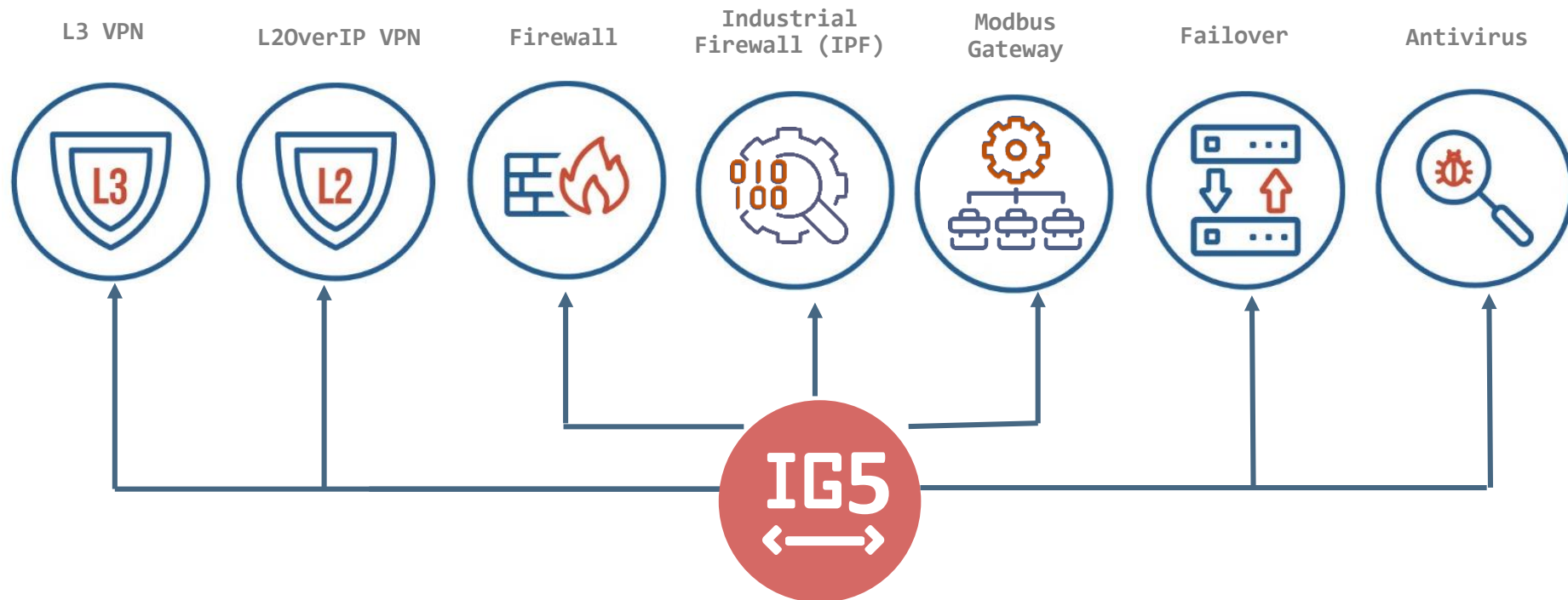


- СКЗИ класса КСЗ по требованиям ФСБ России – тематические исследования, ожидаемые сроки – Q4’ 2024-Q1’2025
- МЭ типа А.4, Б.4, Д.4 и ТДБ 4 класса по требованиям ФСТЭК России – сертификационные работы, ожидаемые сроки – Q1’2025
- внесение в реестр Минцифры (ПО) – ожидаемый срок Q4 2024
- внесение в реестр Минпромторга – ожидаемый срок Q4 2024

ViPNet Coordinator IG 5.2

VIPNet Coordinator IG 5.2

Релиз 5.2.0, план – Q3 2024



ViPNet Coordinator IG 5.2



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5



ViPNet
Coordinator
IG VA



ViPNet Coordinator IG1000 Q1

Обновление
с Coordinator IG4

Обновление
с Coordinator IG4 и отдельная
поставка

НОВЫЕ ИСПОЛНЕНИЯ

VIPNet Coordinator IG1000 Q1

- Форм-фактор: server 1U
- Сетевые интерфейсы:
 - 4 x 1G RJ-45
 - 4 x 1G SFP
- GPIO
- Питание: 2 x 300 Вт с «горячей» заменой
- Рабочая температура - +10°C...+35°C
- Производительность:
 - VPN L2, L3 ~ 2 500 Мбит/с
 - МЭ ~ 2 800 Мбит/с
- Количество соединений ~ 3 000 000



VIPNet Coordinator IG VA

- Форм-фактор: Virtual Appliance
- Среды виртуализации:
 - KVM, QEMU-KVM и libvirt
 - VMWare ESXi 6.7, 7.0
 - VMWare Workstation 15.x, 16.x
 - Oracle VM Server 3.4
 - Oracle VM VirtualBox 6.1.3
 - Microsoft Hyper-V Server 2016/2019
- GPIO через внешний преобразователь USB-GPIO
- Шлюз Modbus через внешний преобразователь USB/RS-485
- Только в целях тестирования



Контент-фильтрация

- Прокси-сервер
 - по параметрам и методам HTTP-запросов;
 - по типам содержимого трафика;
 - по URL;
- Внешний Антивирус*
 - подключение по ICAP
 - обработка входящего и исходящего трафика

The screenshot displays the configuration page for the proxy server and antivirus. At the top, a status message indicates that the proxy server is stopped and that filtering rules are not applied. Below this, there are three tabs: 'Общие настройки', 'Фильтрация открытого трафика', and 'Антивирус'. The 'Антивирус' tab is active. Under the heading 'Внешний антивирус', there is a toggle for 'Инспекция антивирусом' which is currently turned on. Below the toggle, the 'Используемый антивирус' is set to 'external'. There are two fields for 'Сервер обработки исходящих данных' and 'Сервер обработки входящих данных', both of which are currently set to 'Не задано'. At the bottom, there is a dropdown menu for 'Действие при недоступности ICAP' set to 'Пропускать трафик'. A modal window titled 'Настройки внешнего антивируса' is open, showing the configuration for the external antivirus. It has two input fields for 'Сервер обработки исходящих данных', both containing the value 'icap://192.168.1.45:1344/'. The 'Действие при недоступности ICAP' dropdown is also visible in the modal, set to 'Пропускать трафик'. At the bottom of the modal are 'Сохранить' and 'Отмена' buttons.

*Только для исполнений IG100 I4 и IG1000 Q1

Выборочное логирование правил МЭ

Параметры сетевого фильтра ✕

Название:

Состояние: Включено

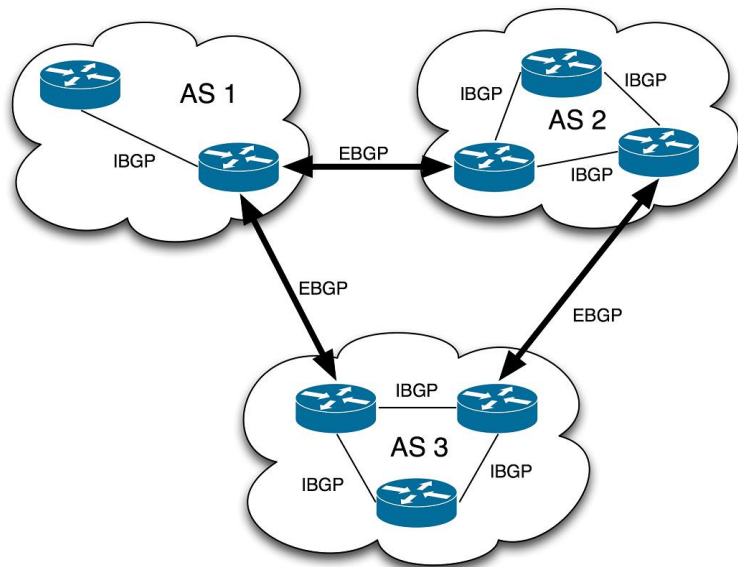
Действие: Блокировать трафик

Пропускать трафик

Отклонять трафик с ответом:

Регистрировать IP-пакеты

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)

Два шлюза Modbus TCP/RTU

Независимое
использование
интерфейсов RS-485 и
RS-232 для шлюзов
Modbus

▼ Шлюз 1, Modbus
RS-485-1, скорость: 115200 бод

Остановить Настроить Удалить

Линия (2), RTU-to-TCP

▼ Шлюз 2, Modbus
RS-232-1, скорость: 115200 бод

Остановить Настроить Удалить

Общие настройки

Состояние: ● Работает

Автоматический запуск: Включен

Режим работы: RTU-to-TCP

Запись событий в журнал: Важные сообщения

TCP-порт: 5065

Настройки интерфейса

Последовательный интерфейс: RS-232

Скорость ТТУ, бод: 115200

Контроль бита четности: even

Время ожидания запроса, мс: 1500

Время ожидания ответа, мс: 1500

Маршруты

SlaveID	IP-адрес	TCP-порт	Интервал, мс	Описание
1	192.168.25.182	65535	1500	TCP Slave 1
3	192.168.25.1	24358	1500	
5	192.168.25.141	24358	1800	TCP
6	188.52.125.08	24358	1200	

Инвентаризация

- Добавление серийного номера при производстве и пользователем самостоятельно
- Отображение в CLI, WebUI
- Передача данных по SNMP

```
igl100-2c670009> version
Product: ViPNet Coordinator IG
Platform: IG100 I1
Serial number: 201906027
License: IG100
Software version: 5.2.0-4424
```

Coordinator IG100

Основное Лицензия

ViPNet Coordinator IG100 5.2.0-4060

© 2023, АО «ИнфоТекс»

Веб-сайт: www.infotecs.ru

E-mail: soft@infotecs.ru

Телефон для регионов России: 8 800 250-0-260

Телефон для Москвы: +7 495 737-61-92

Платформа: IG100 I1

Версия ПО: 5.2.0-4060

Серийный номер: 201906027

[Лицензионное соглашение](#)

Перенос настроек с любой платформы

Импорт настроек

Ввод пароля

Дата создания файла: 09.10.2023

Продукт: VIPNet Coordinator IG

Платформа: IG100 П

Версия ПО: 5.1.0-354

Комментарии:

* Введите пароль защиты файла конфигурации:

.....

Назад Далее Отмена

Импорт конфигурации

Выбор настроек

Выберите настройки, которые вы хотите импортировать.

- Настройки сети**
 - Сетевые интерфейсы ⚠ Результат
 - Статическая маршрутизация и политики ⚠ Результат
 - Маршрутизация OSPF Результат
 - Обнаружение недоступных шлюзов Результат
- Профиль безопасности**
 - Правила фильтрации и трансляции, группы объектов ⚠ Результат
 - Трансляция протоколов DNS, FTP, H.323, SCCP, SIP Результат
 - Обнаружение и предотвращение вторжений Результат
 - Идентификация пользователей сети ⚠ Результат
 - Активирован Результат
- Системные настройки**
 - Веб-интерфейс Результат
 - Сертификаты Результат
 - SNMP ⚠ Результат
 - Другие настройки Результат
- Промышленная безопасность**
 - Шлюз Modbus Результат
 - Фильтры промышленных протоколов Результат
 - Порты ввода и вывода (GPIO) Результат
 - N и L2OverIP ⚠ Результат
 - твые службы Результат

Назад Далее Отмена

firewall

Firewall rules

Service Vpn Rules:

Num	Name	Option	Schedule
Act	Protocol	Source	-> Destination
	DpiProtocol	[G]DpiGroup, DpiApp	DomainUser
1	Block not original udp port		Generated
Drop	udp: from 0-2045 to 2046	@local	-> @any
	udp: from 2047-65535 to 2046	@any	@any
2	Allow VIPNet base services in		Generated
Pass	udp: to 2046	@any	-> @local
	2048 to 2048	@any	@any
	2050 to 2050	@any	@any

Отмена

ViPNet Coordinator IG 4

VIPNet Coordinator IG 4.5.1.1

- Фильтрация промышленного протокола МЭК 60870-5-104
- Кластер высокой доступности
- Динамические интерфейсы в кластере (сняты ограничения)
- Новые возможности мониторинга
- Новые аппаратные платформы IG100 I4 и IG100 I5



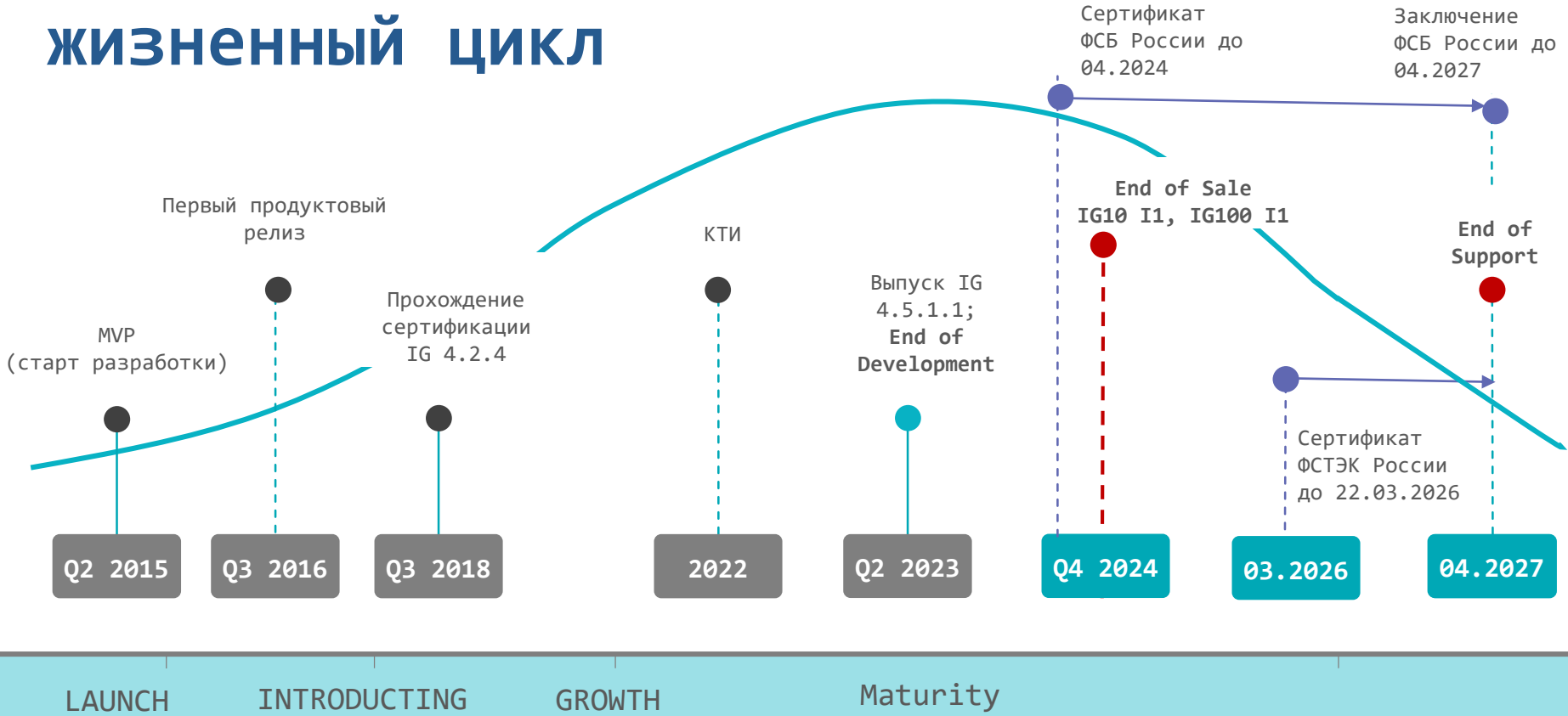
- ✓ Релиз выпущен
- ✓ ФСТЭК России - контроль изменений завершен
- ✓ ФСБ России - контроль изменений завершен (оформление сертификата)

Обновлен статус в реестре РЭП



- ПАК ViPNet Coordinator IG в едином реестре российской радиоэлектронной продукции (реестр РЭП) (от 14.05.2024):
 - ViPNet Coordinator IG10 I1 – реестровая запись [10533948](#);
 - ViPNet Coordinator IG10 I2 – реестровая запись [10533947](#);
 - ViPNet Coordinator IG100 I1 – реестровая запись [10533946](#);
 - ViPNet Coordinator IG100 I4 – реестровая запись [10533945](#);
 - ViPNet Coordinator IG10 I5 – реестровая запись [10533944](#).

VIPNet Coordinator IG 4: ЖИЗНЕННЫЙ ЦИКЛ





СПАСИБО ЗА ВНИМАНИЕ

Марина Сорокина

Marina.Sorokina@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363