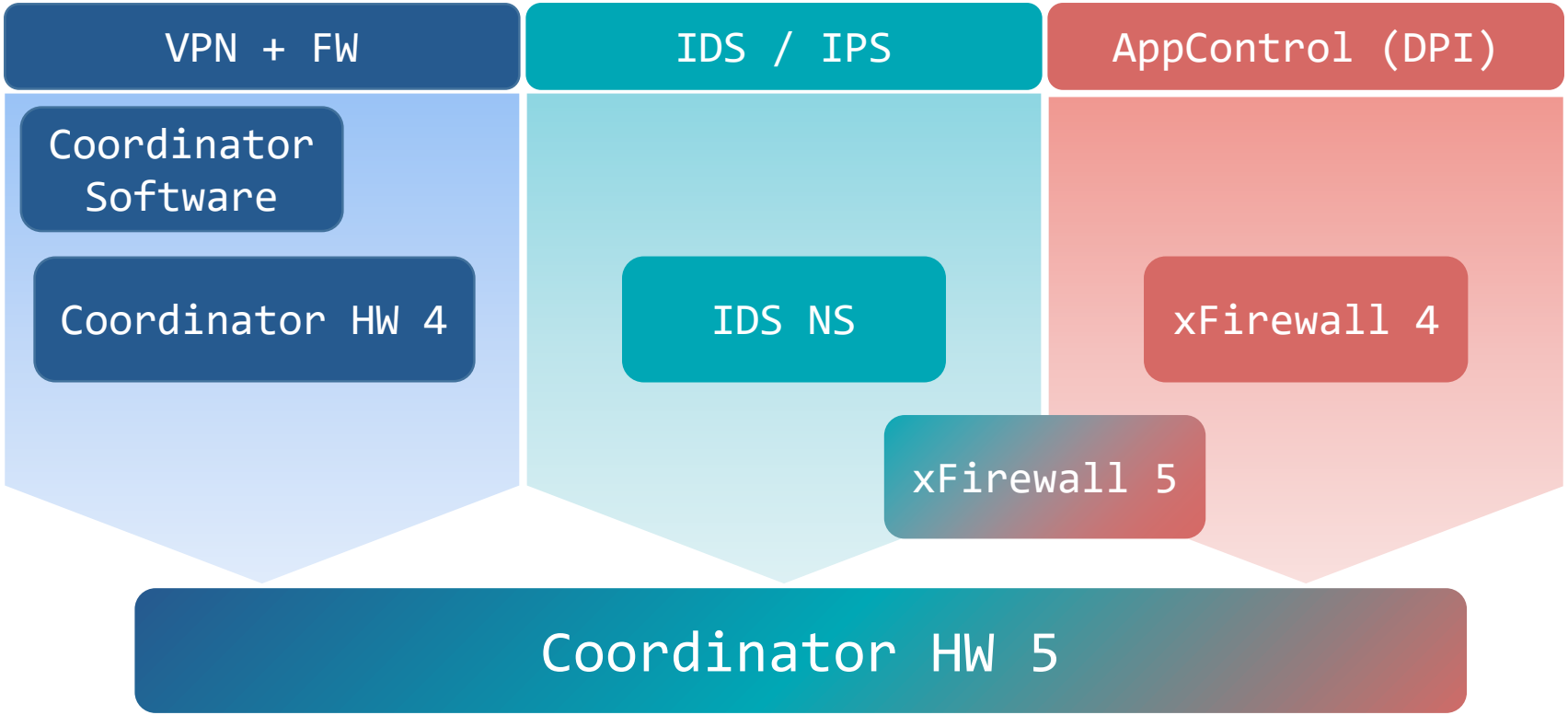
ViPNet Coordinator HW 5

Виталий Беличко

Шлюзы безопасности ViPNet



ViPNet Coordinator HW 5

ТЕХНО infotecs 2022 ФЕСТ

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

ТЕХНО 2022 infotecs ФЕСТ

Сертификация

Требования по сертификации

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса
- СОА класса ВП

ФСТЭК России

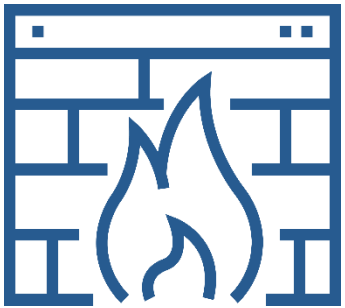
- Межсетевой экран тип «А» и тип «Б» 4 класса
- СОВ уровня сети 4 класса
- 4-й уровень доверия средств защиты информации

ТЕХНО infotecs ФЕСТ 2022

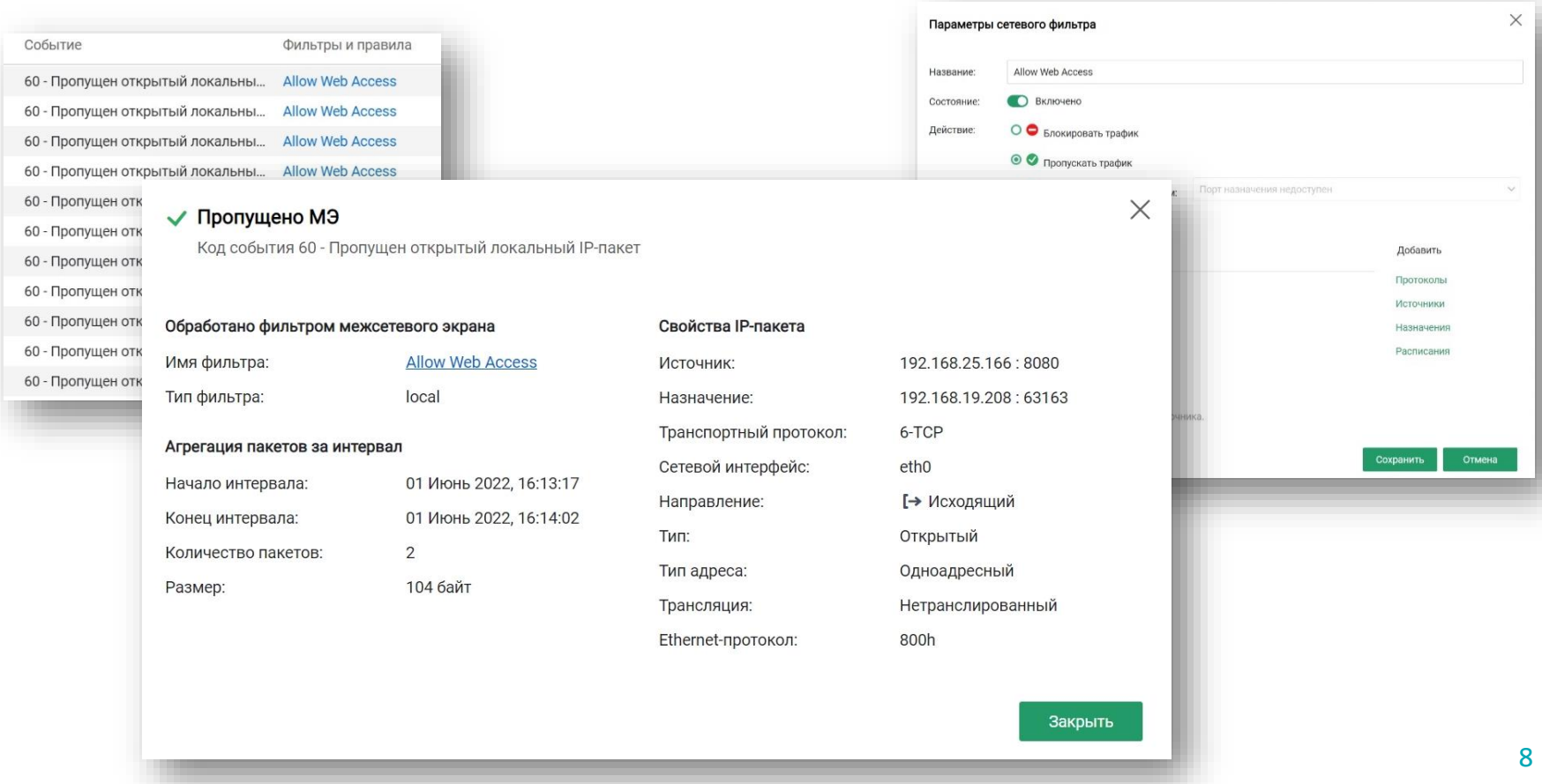
Межсетевое экранирование

Межсетевое экранирование

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



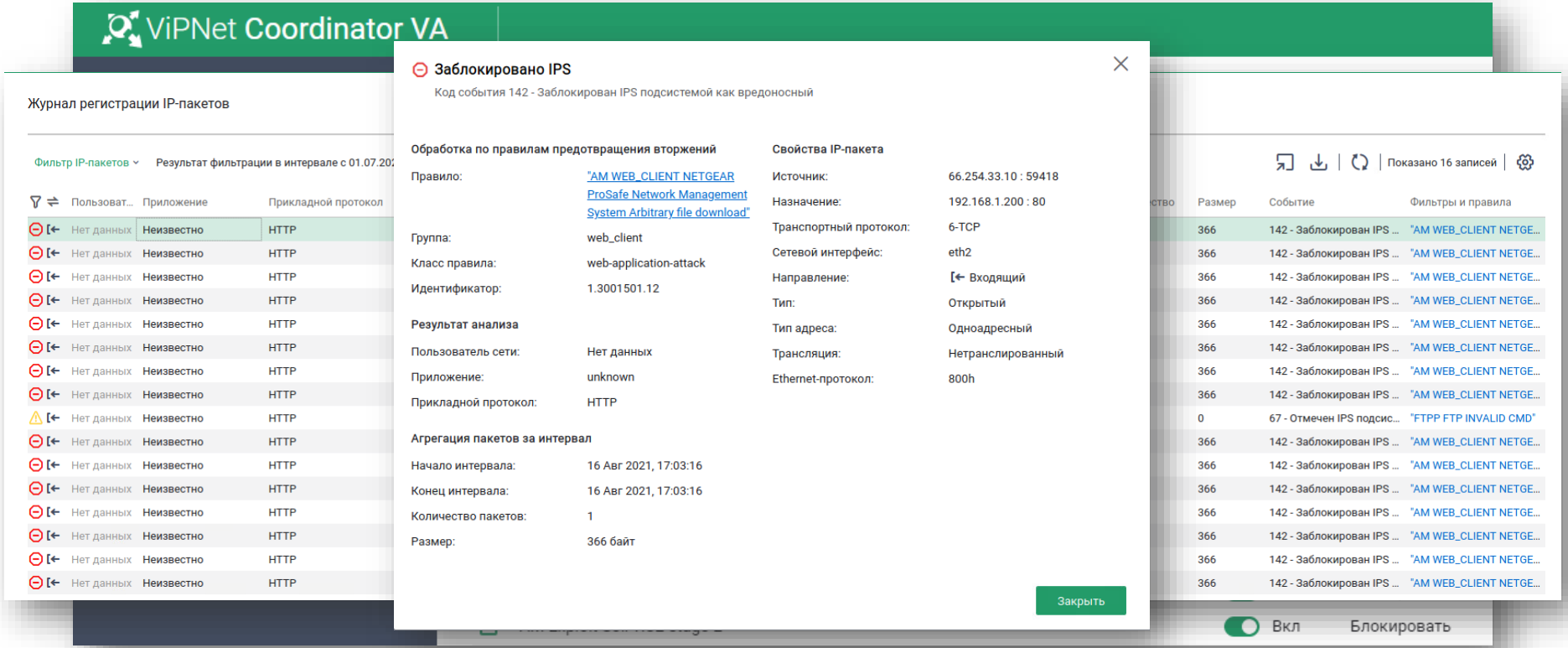
Идентификация правил МЭ



ТЕХНО infotecs 2022 ФЕСТ

Предотвращение вторжений (IDS/IPS)

Предотвращение вторжений



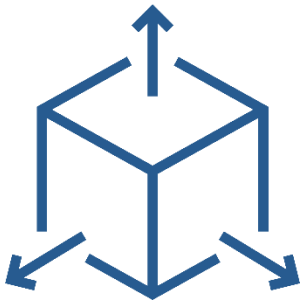
ТЕХНО 2022 infotecs ФЕСТ

Криптография (VPN)

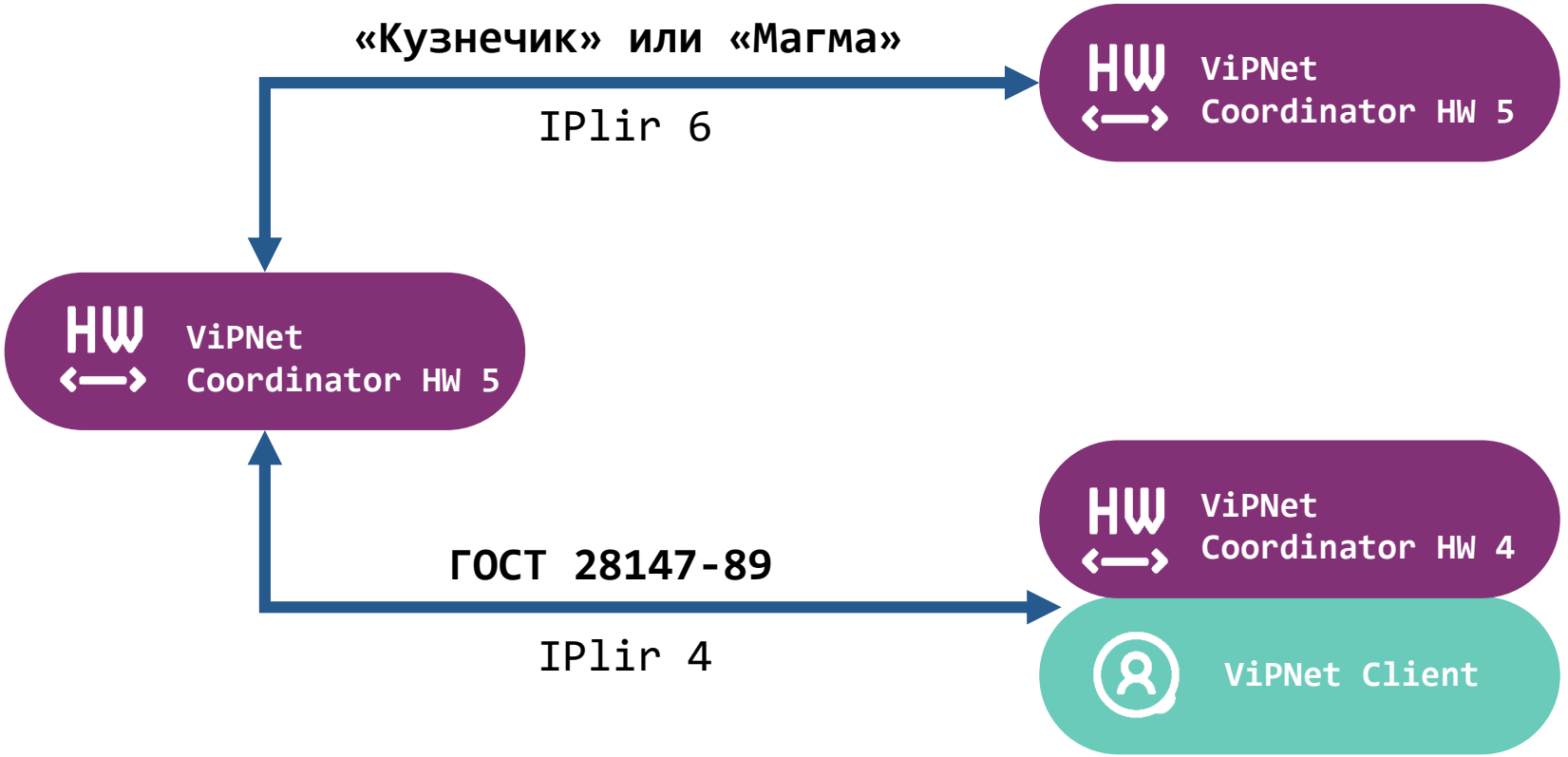
Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPlir 6 – протокол безопасности сетевого уровня

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



Обратная совместимость

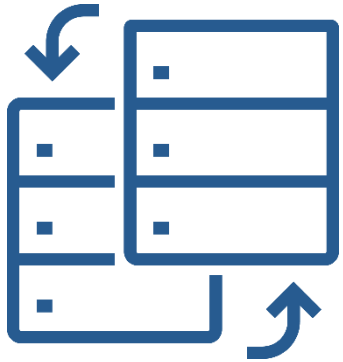


ТЕХНО 2022 infotecs ФЕСТ

Кластер высокой доступности (HA Cluster)

Кластер высокой доступности

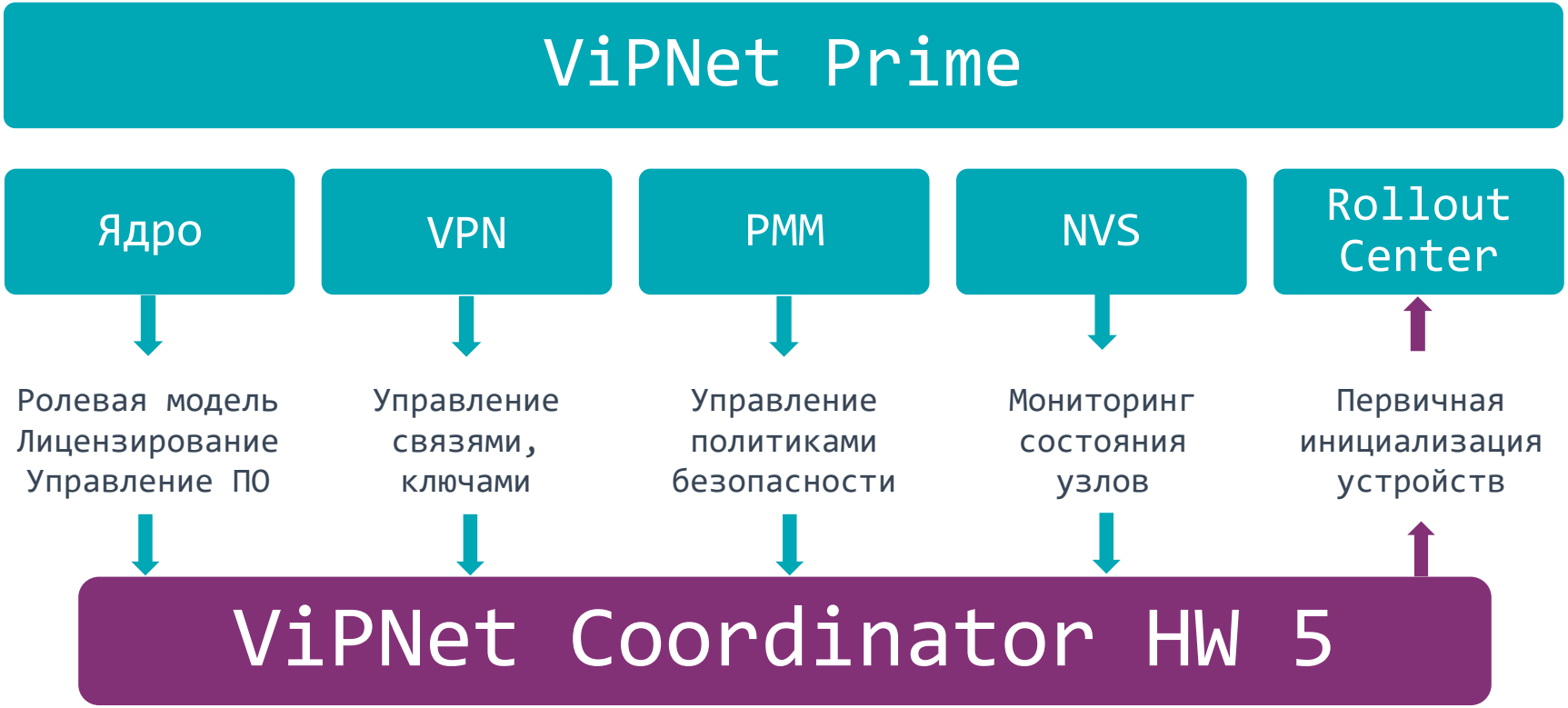
- Быстрое переключение кластера по потере связи и питания
- Синхронизация сессий МЭ в кластере
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- **Минимальное время переключения кластера сократилось до 1 секунды**



ТЕХНО 2022 infotecs ФЕСТ

Управление и мониторинг

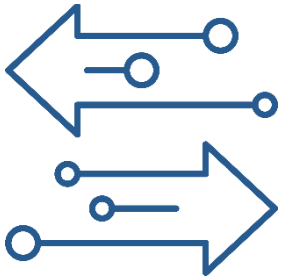
Модули ViPNet Prime



Изменение ролевой модели

ViPNet Coordinator HW 4

- Пользователь
- Администратор узла
- Администратор группы узлов
- Администратор сети



ViPNet Coordinator HW 5

Локальные учетные записи:

- Администратор
- Пользователь (Аудитор)

+

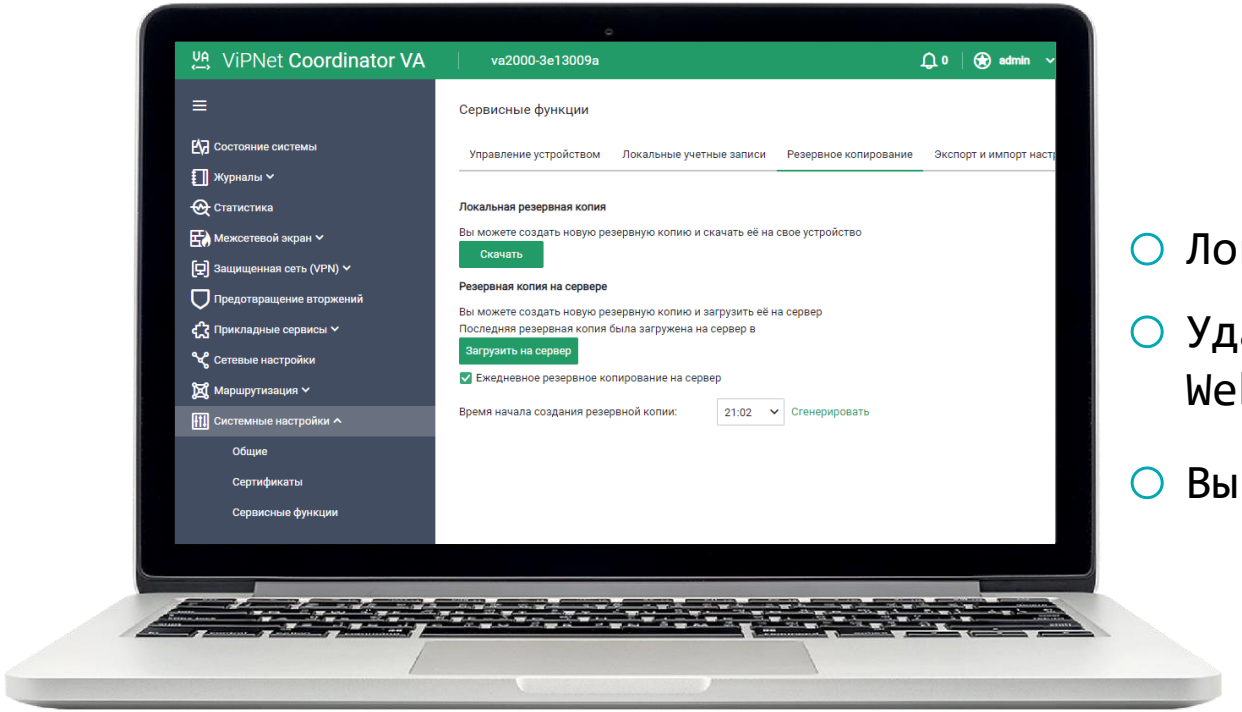
Централизованные учетные записи:

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

Планы развития 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

Резервное копирование

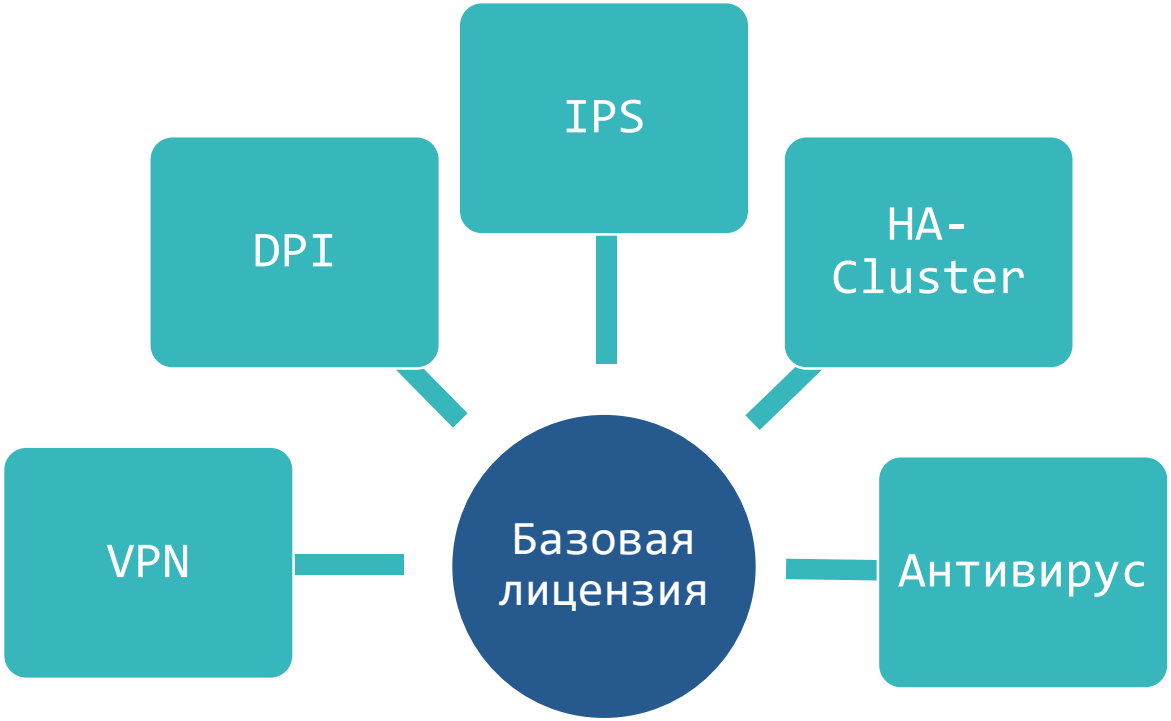


- Локальный экспорт на USB
- Удаленный экспорт через WebUI
- Выгрузка на сервер Prime

ТЕХНО 2022 infotecs ФЕСТ

Лицензирование

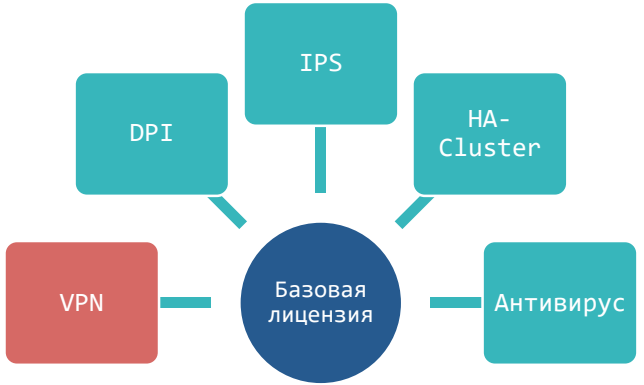
Новая схема лицензирования



HW50/100/1000/2000/5000
VA100/500/1000/2000

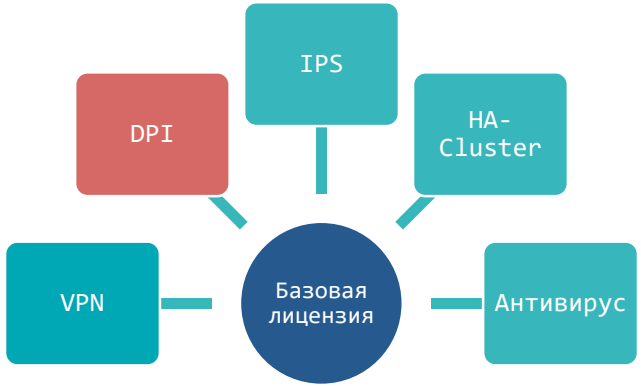
VPN

- **Технологический VPN не лицензируется**
  - Связь с системой управления всегда активна
- **Лицензия на VPN (активация, срок действия)**
  - Туннелирование (L3/L2)
  - Кол-во туннелей не ограничиваем
  - Регистрация ViPNet клиентов



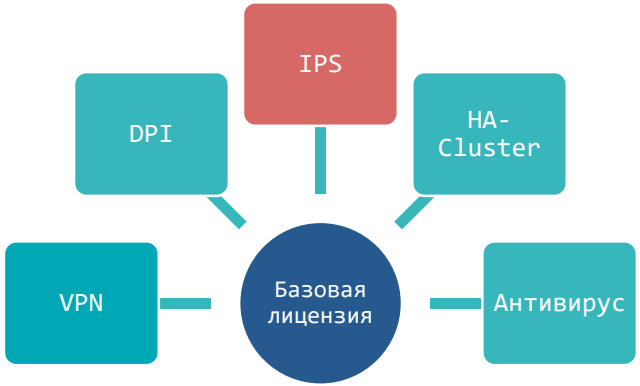
Межсетевой экран

- Межсетевой экран (SPI) не лицензируется (всегда активирован)
- Лицензия на модуль контроля приложений (DPI)
  - Активация, срок действия
- Встроенный прокси-сервер не лицензируем



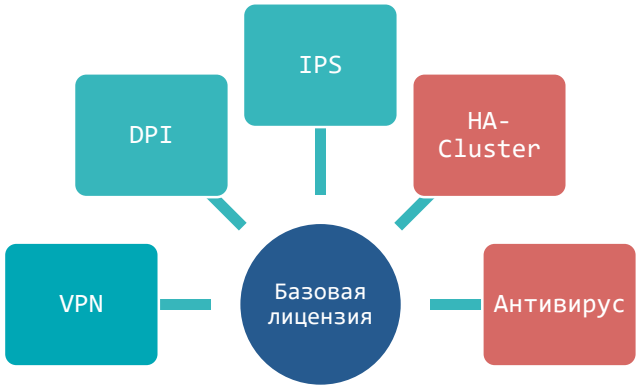
Предотвращение вторжений (IPS)

- **Лицензия на модуль IPS**
  - Активация
  - Срок действия
- **Подписка на обновления БРП**
  - Срок действия



HA-Cluster и антивирус

- Лицензируем на кластер для всех исполнений (HW и VA)
- Подключение внешнего антивируса (ICAP) не лицензируется
- Встроенный антивирус*:
  - Заказчик самостоятельно приобретает лицензию на активацию и обновление



Исполнения

Характеристики старших платформ

Исполнение	Платформа	Интерфейсы (медь)	Интерфейсы (оптика)	Блок питания
HW1000	HW1000 Q7	6x RJ45	-	1x 250 W
HW1000 C	HW1000 Q8	8x RJ45	-	1x 250 W
HW1000 D	HW1000 Q9	8x RJ45	4x SFP	2x 300 W
HW2000	HW2000 Q5	4x RJ45	4x SFP 4x SFP+	2x 300 W
HW5000	HW5000 Q2	4x RJ45	8x SFP+	2x 300 W

- Более производительные CPU
- Увеличен объем RAM (4/16/32/64 Gb)
- Увеличен объем SSD (4 Gb) и HDD (1/2 Tb)

Поддержка аппаратных платформ

ViPNet Coordinator HW50

- HW50 N1/N2/N3/N4/N6 ***
- HW50 A1 NEW

ViPNet Coordinator HW100

- HW100 N1/N2/N3 ***
- HW100 Q1 NEW

ViPNet Coordinator HW2000

- HW2000 Q4
- HW2000 Q5 NEW

ViPNet Coordinator HW1000

- HW1000 Q4/Q5/Q6
- HW1000 Q7/Q8/Q9 NEW

ViPNet Coordinator HW5000

- HW5000 Q1
- HW5000 Q2 NEW

*** - режим VPN only

ViPNet Coordinator VA

- KVM, QEMU-KVM и Libvirt
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox

ТЕХНО infotecs 2022 ФЕСТ

Миграция HW 4 -> HW 5

Миграция HW 4 -> HW 5

ТехноИнфотекс Фест 2022

ViPNet Prime (чистая установка)

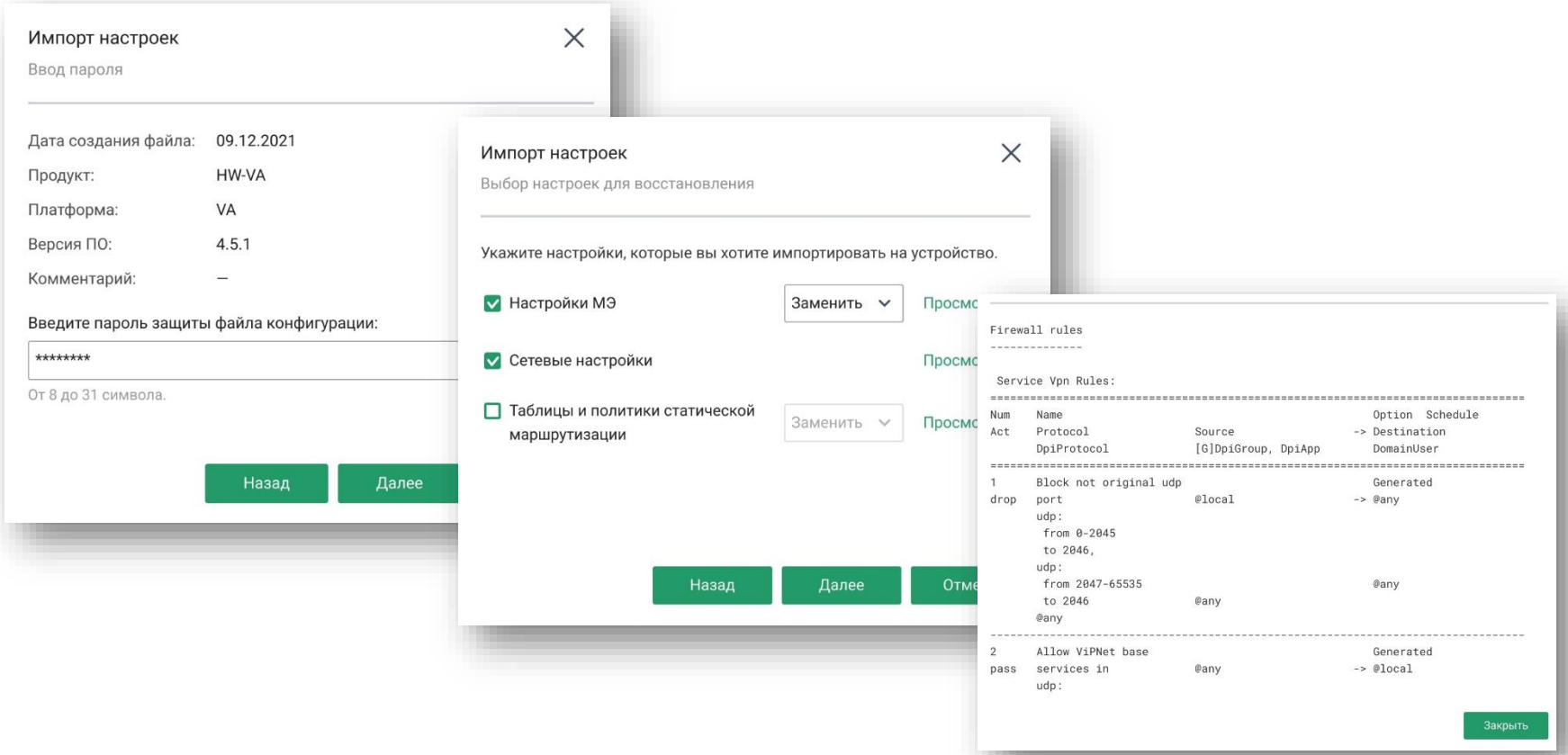
Создаем узел HW 5, настраиваем связи, лицензии, формируем DS5

Снимаем VBE-файл от HW 4 (*если меняется аппаратная платформа*)*

Локально обновляем ПО HW 4.5.2 до HW 5 с удалением VPN конфигурации

Инициализируем DS5 (+VBE). Готово!

Импорт настроек из VBE файла



ТЕХНО 2022 infotecs Фест

Спасибо за внимание!

Беличко Виталий
Ведущий менеджер продукта
e-mail: Vitaly.Belichko@infotecs.ru

Информационный партнер

CYBER MEDIA

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363