Защита ведомственных сетей передачи данных, мониторинг информационной безопасности и ГосСОПКА в медицине

infotecs

ViPNet Coordinator HW 4

Криптографическая защита

- Защита каналов передачи данных с использованием алгоритмов ГОСТ
- Защита каналов связи при подключении к сетям общего пользования, в том числе беспроводных каналов связи
- Защищенный доступ удаленных и мобильных пользователей
- Соответствие требованиям ФСБ России

Межсетевое экранирование

- Фильтрация сетевых соединений и поддержка политик безопасности
- Защита периметра
- Сегментация сети, организация DMZ
- Сокрытие адресов и информации о структуре сети
- Соответствие требованиям ФСТЭК России и ФСБ России

Надежность и резервирование

- Отказоустойчивый кластер (High-Availability cluster) с синхронизацией таблицы открытых соединений
- Возможность резервирования каналов MultiWAN (переключение на резервный канал в случае отсутствия связи)
- Резервируемые блоки питания
- 50 тыс. часов наработки на отказ

Сертификаты соответствия

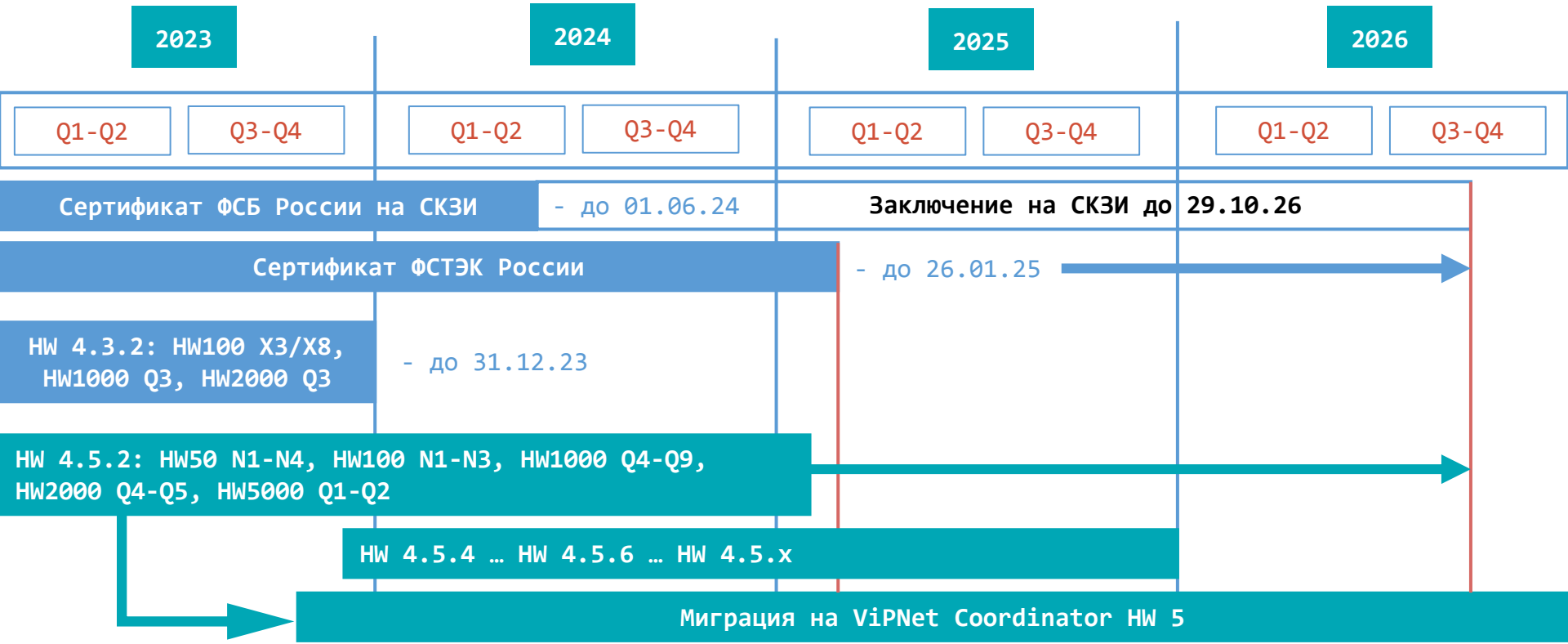
ФСБ России

- СКЗИ класса КС3
- Межсетевой экран 4 класса

ФСТЭК России

- Межсетевой экран типа А 4 класса (ИТ.МЭ.А4.ПЗ)
- Межсетевой экран типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
- 4-й уровень доверия средств защиты информации

Жизненный цикл Coordinator HW 4



ViPNet Coordinator HW 4

Реестр Минцифры России

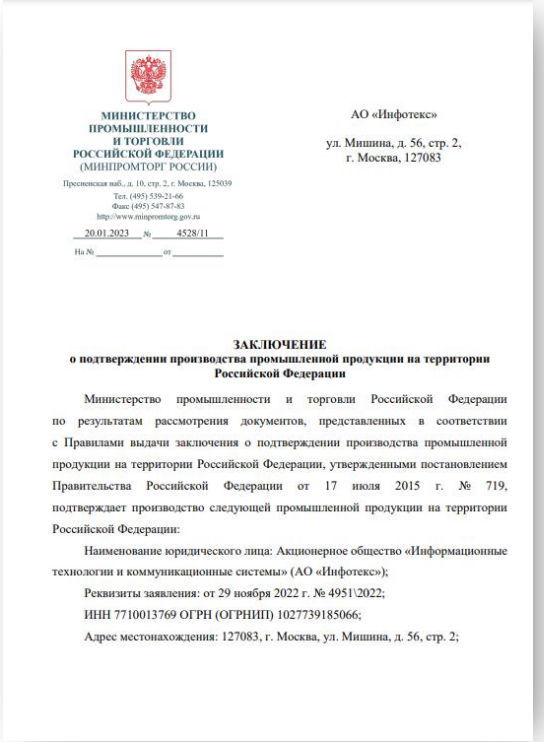
Реестр ПО:

- 03.11 Средства защиты каналов передачи данных, в том числе криптографическими методами
- 03.03 Межсетевые экраны

Реестр ПАК NEW**:**

- 15.10 Программно-аппаратные комплексы защиты каналов передачи данных, в том числе криптографическими методами
- 15.03 Программно-аппаратные комплексы межсетевых экранов

Минпромторг России (ПП РФ № 719)



МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОМТОРГ РОССИИ)

Пресненская наб., д. 10, стр. 2, г. Москва, 125039
Тел. (495) 539-21-66
Факс (495) 547-87-83
http://www.minpromtorg.gov.ru

20.01.2023 № 4528/11
На № _____ от _____

АО «Инфотекс»

ул. Мишина, д. 56, стр. 2,
г. Москва, 127083

ЗАКЛЮЧЕНИЕ
о подтверждении производства промышленной продукции на территории Российской Федерации

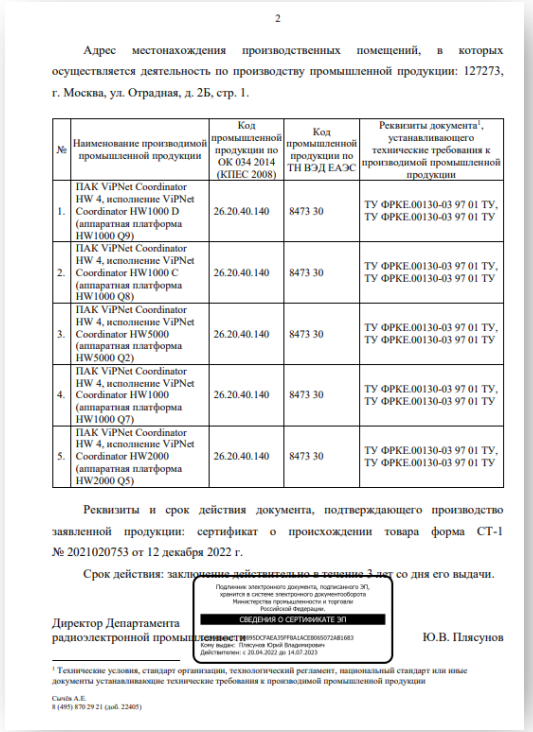
Министерство промышленности и торговли Российской Федерации по результатам рассмотрения документов, представленных в соответствии с Правилами выдачи заключения о подтверждении производства промышленной продукции на территории Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 17 июля 2015 г. № 719, подтверждает производство следующей промышленной продукции на территории Российской Федерации:

Наименование юридического лица: Акционерное общество «Информационные технологии и коммуникационные системы» (АО «Инфотекс»);

Реквизиты заявления: от 29 ноября 2022 г. № 4951\2022;

ИНН 7710013769 ОГРН (ОГРНИП) 1027739185066;

Адрес местонахождения: 127083, г. Москва, ул. Мишина, д. 56, стр. 2;



2

Адрес местонахождения производственных помещений, в которых осуществляется деятельность по производству промышленной продукции: 127273, г. Москва, ул. Отрадная, д. 2Б, стр. 1.

№	Наименование производимой промышленной продукции	Код промышленной продукции по ОК 034 2014 (КПЕС 2008)	Код промышленной продукции по ТН ВЭД ЕАЭС	Реквизиты документа[1], устанавливающего технические требования к производимой промышленной продукции
1.	ПАК ViPNet Coordinator HW 4, исполнение ViPNet Coordinator HW1000 D (аппаратная платформа HW1000 Q9)	26.20.40.140	8473 30	ТУ ФРКЕ.00130-03 97 01 ТУ, ТУ ФРКЕ.00130-03 97 01 ТУ
2.	ПАК ViPNet Coordinator HW 4, исполнение ViPNet Coordinator HW1000 C (аппаратная платформа HW1000 Q8)	26.20.40.140	8473 30	ТУ ФРКЕ.00130-03 97 01 ТУ, ТУ ФРКЕ.00130-03 97 01 ТУ
3.	ПАК ViPNet Coordinator HW 4, исполнение ViPNet Coordinator HW5000 (аппаратная платформа HW5000 Q2)	26.20.40.140	8473 30	ТУ ФРКЕ.00130-03 97 01 ТУ, ТУ ФРКЕ.00130-03 97 01 ТУ
4.	ПАК ViPNet Coordinator HW 4, исполнение ViPNet Coordinator HW1000 (аппаратная платформа HW1000 Q7)	26.20.40.140	8473 30	ТУ ФРКЕ.00130-03 97 01 ТУ, ТУ ФРКЕ.00130-03 97 01 ТУ
5.	ПАК ViPNet Coordinator HW 4, исполнение ViPNet Coordinator HW2000 (аппаратная платформа HW2000 Q5)	26.20.40.140	8473 30	ТУ ФРКЕ.00130-03 97 01 ТУ, ТУ ФРКЕ.00130-03 97 01 ТУ

Реквизиты и срок действия документа, подтверждающего производство заявленной продукции: сертификат о происхождении товара форма СТ-1 № 2021020753 от 12 декабря 2022 г.

Срок действия: заключение действительно в течение 3 лет со дня его выдачи.

Директор Департамента радиоэлектронной промышленности Ю.В. Плясунов

Подписано электронного документа, подписанного ЭП, хранится в системе электронного документооборота Министерства промышленности и торговли Российской Федерации.
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Кому выдан: Плясунов Юрий Владимирович
Действителен: с 20.04.2022 до 14.07.2023

[1] Технические условия, стандарт организации, технологический регламент, национальный стандарт или иные документы устанавливающие технические требования к производимой промышленной продукции

Сычёв А.Е.
8 (495) 870 29 21 (доб. 22405)

МИНПРОМТОРГ РОССИИ

- HW1000 Q7
- HW1000 Q8
- HW1000 Q9
- HW2000 Q5 NEW
- HW5000 Q2

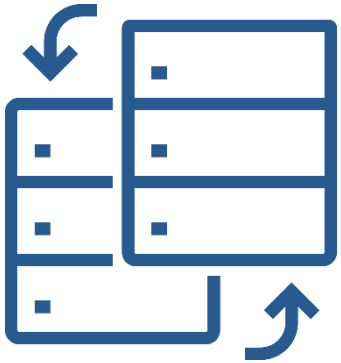
ViPNet Coordinator HW 4.5.2

- Кластер высокой доступности
- Новые возможности мониторинга
- Повышение безопасности сетевых протоколов
- Новые сервисные функции
- Улучшения веб-интерфейса
- Поддержка платформы HW2000 Q5

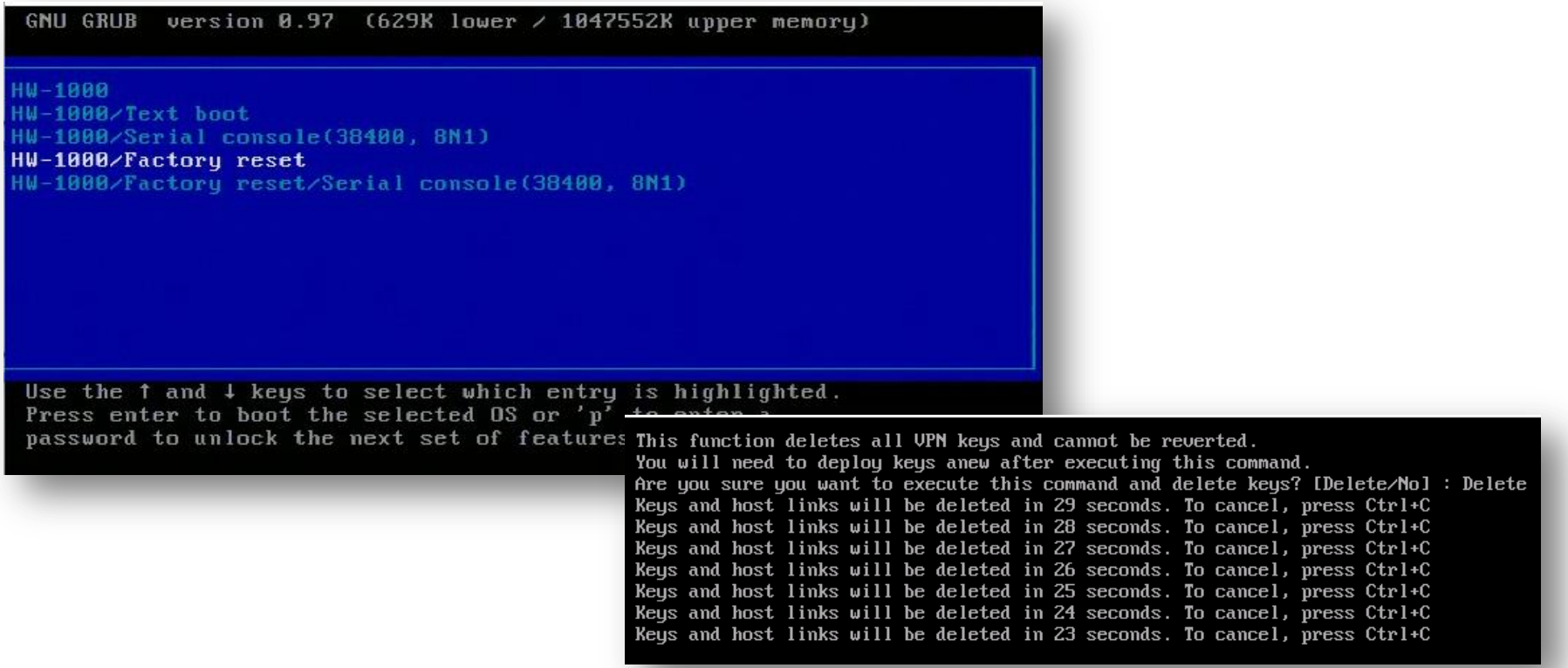
✓ ФСТЭК России сертифицировано
✓ ФСБ России сертифицировано

Кластер высокой доступности

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



Возврат к заводским настройкам



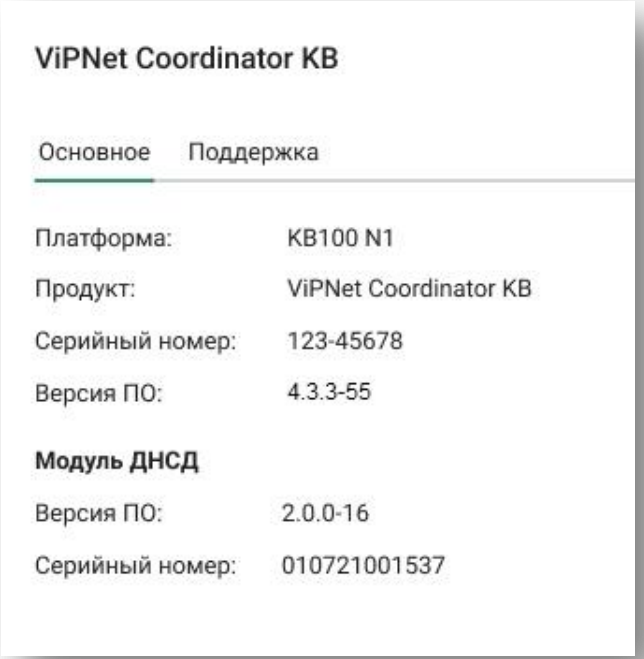
Ближайшие планы развития

- Поддержка новых аппаратных платформ
- Инвентаризация (добавление SN изделия)
- Поддержка беспроводных модулей Wi-Fi и LTE для HW50 / HW100

Инвентаризация

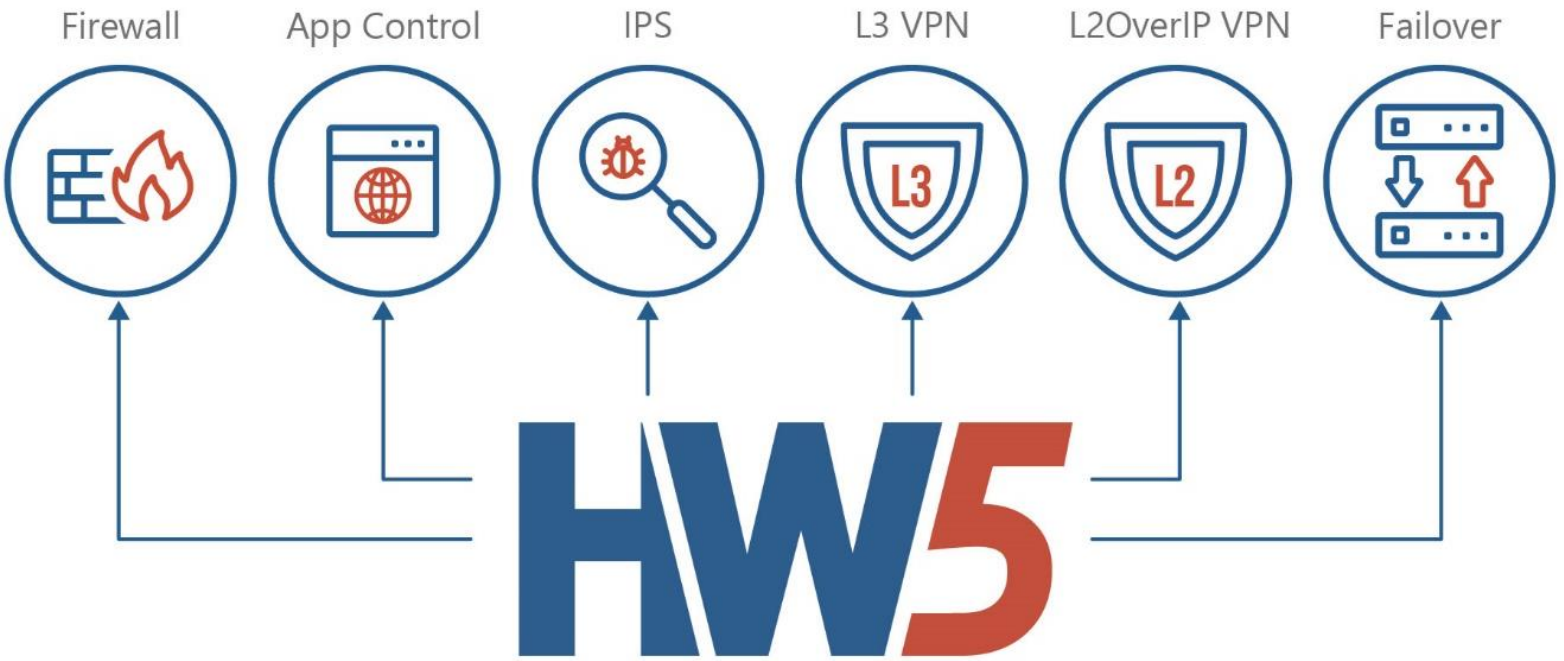
- Добавление серийного номера при производстве и пользователем самостоятельно
- Отображение в CLI, WebUI
- Передача данных по SNMP

```
kb100-3db7000a# version
Product: ViPNet Coordinator KB
Platform: KB100 N1
Serial number: 123-45678
Software version: 4.3.3-154
DNSD version: 2.0.0, build number: 16
DNSD serial number: 010721001537
```

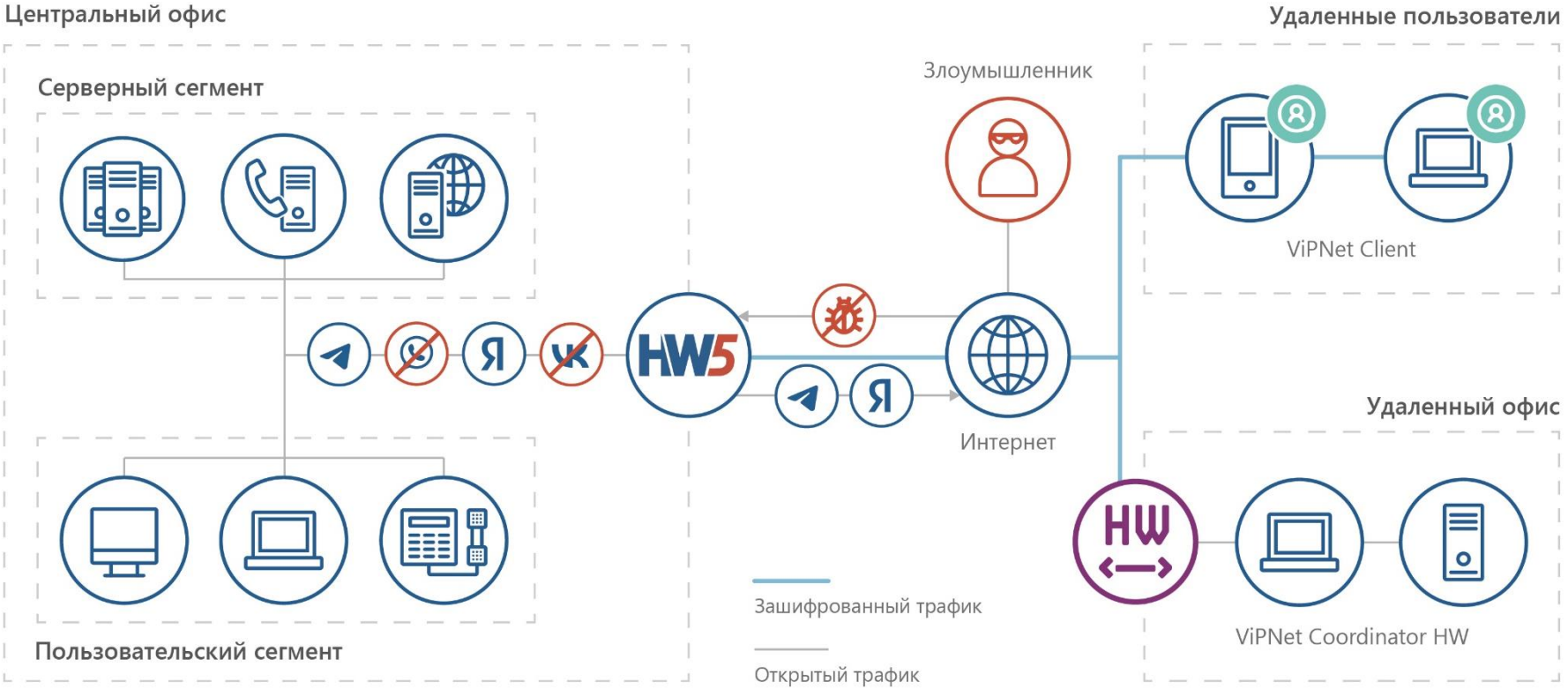


ViPNet Coordinator HW 5

ViPNet Coordinator HW 5



Типовая схема применения HW 5



Требования по сертификации

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

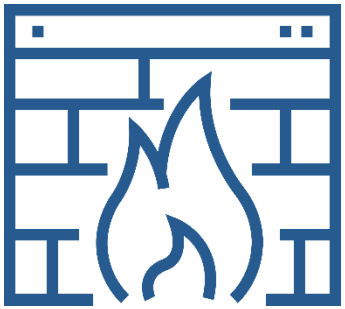
- Межсетевой экран тип «А» и тип «Б» 4 класса
- СОВ уровня сети 4 класса
- 4-й уровень доверия средств защиты информации

Минцифры России

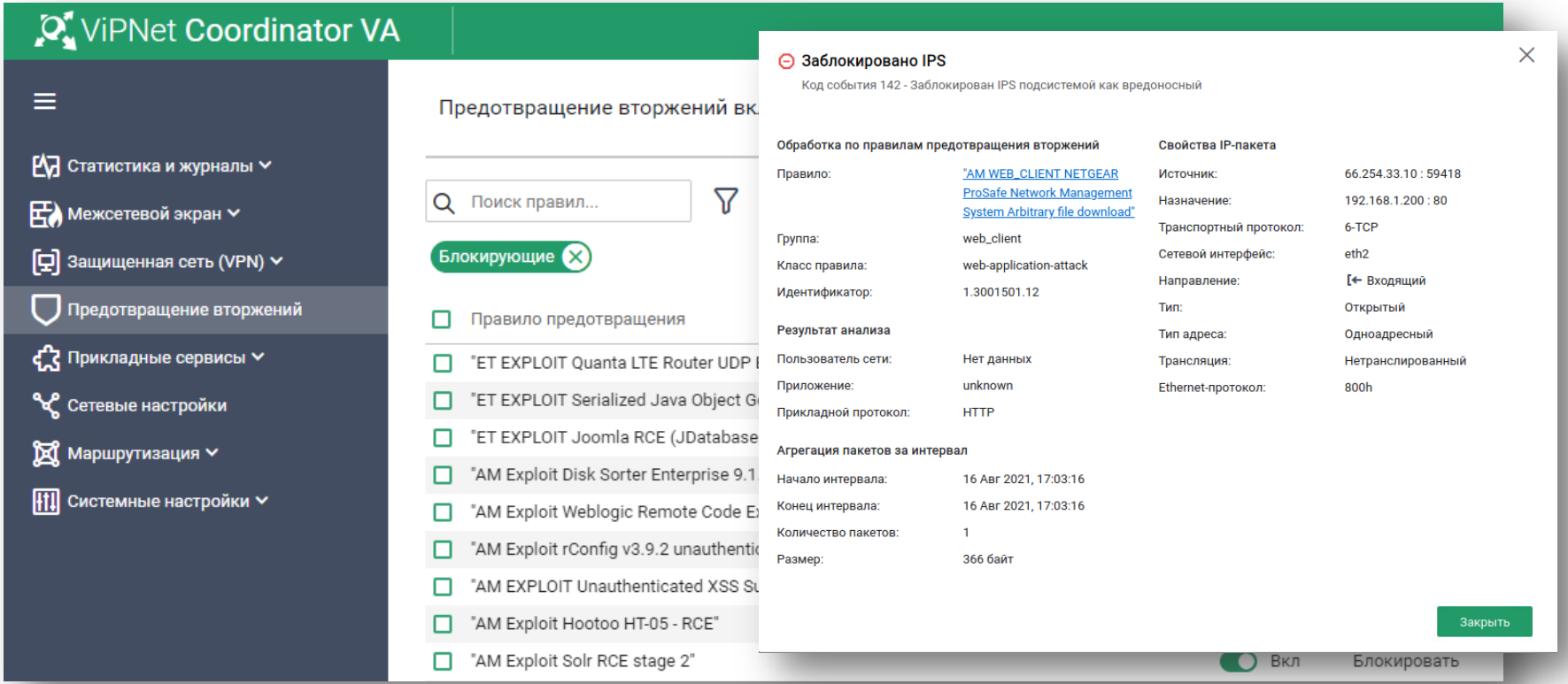
- В реестре российского ПО

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



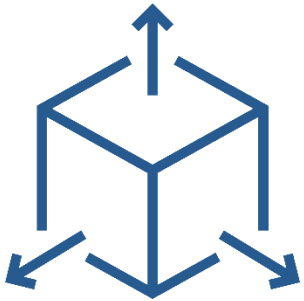
Предотвращение вторжений



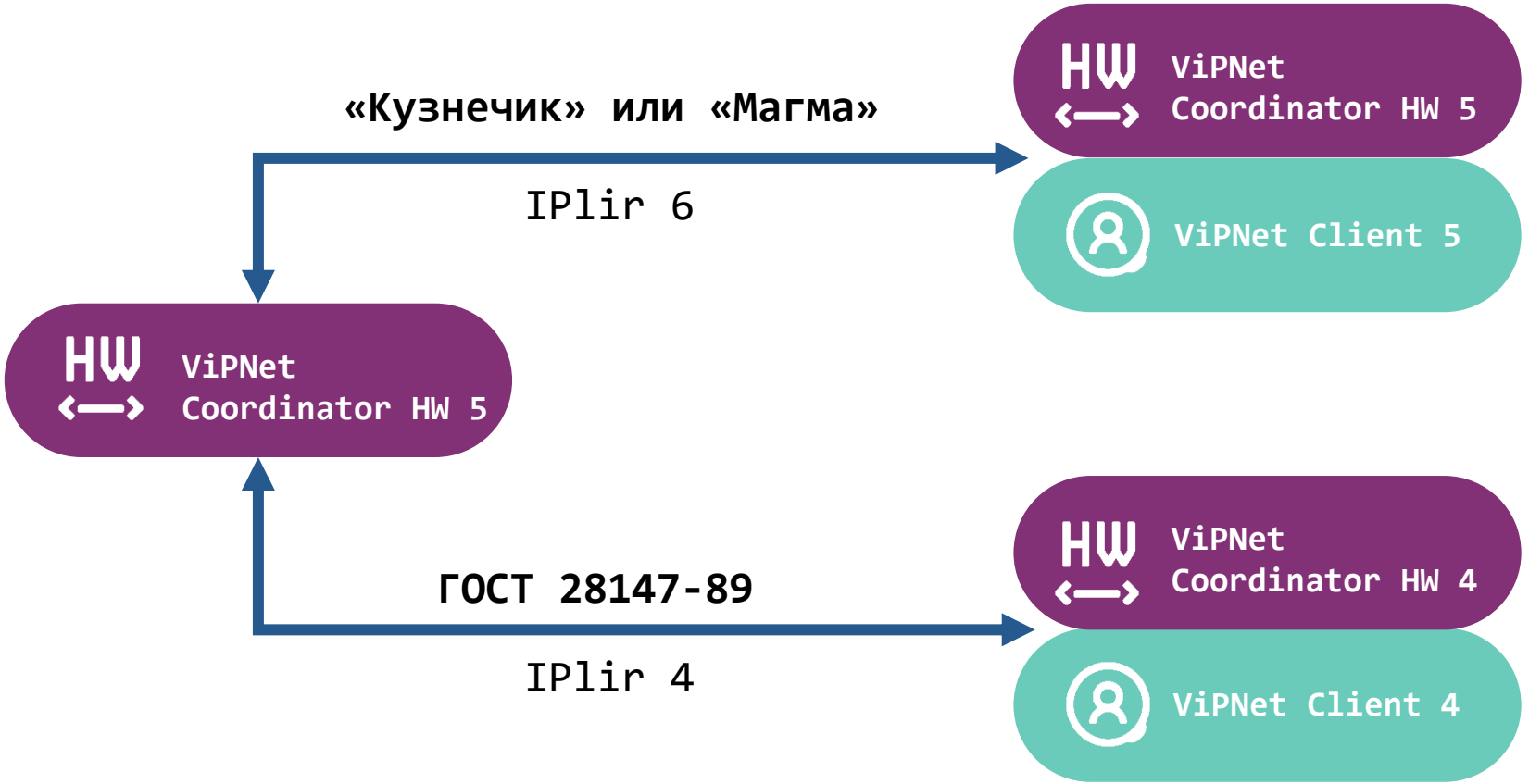
Криптография (VPN)

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

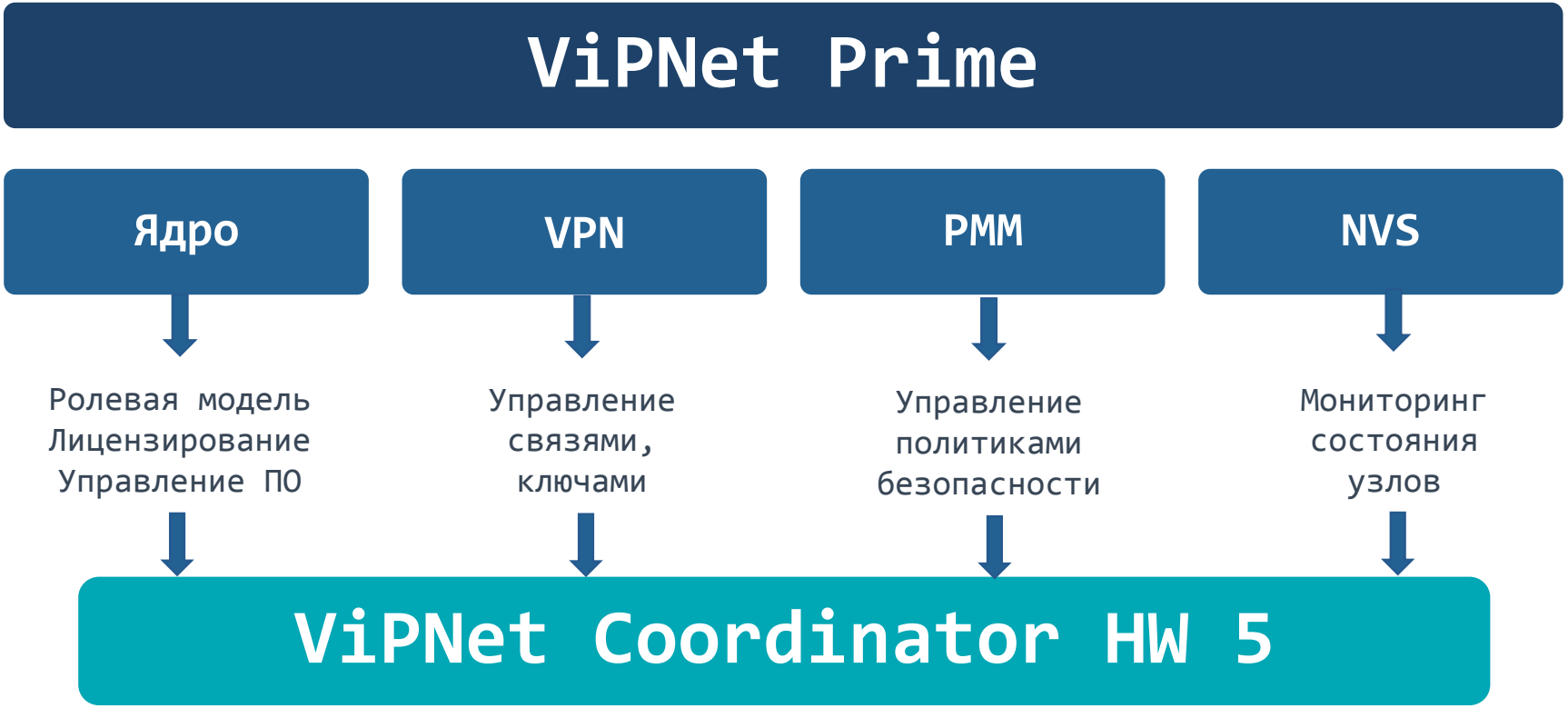
  ТК 26 Р 1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня»



Обратная совместимость



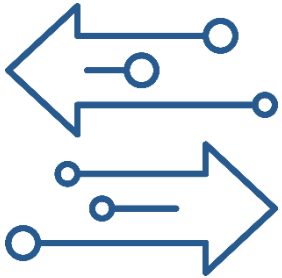
Новая система управления



Изменение ролевой модели

ViPNet Coordinator HW 4

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



ViPNet Coordinator HW 5

Локальные учетные записи:

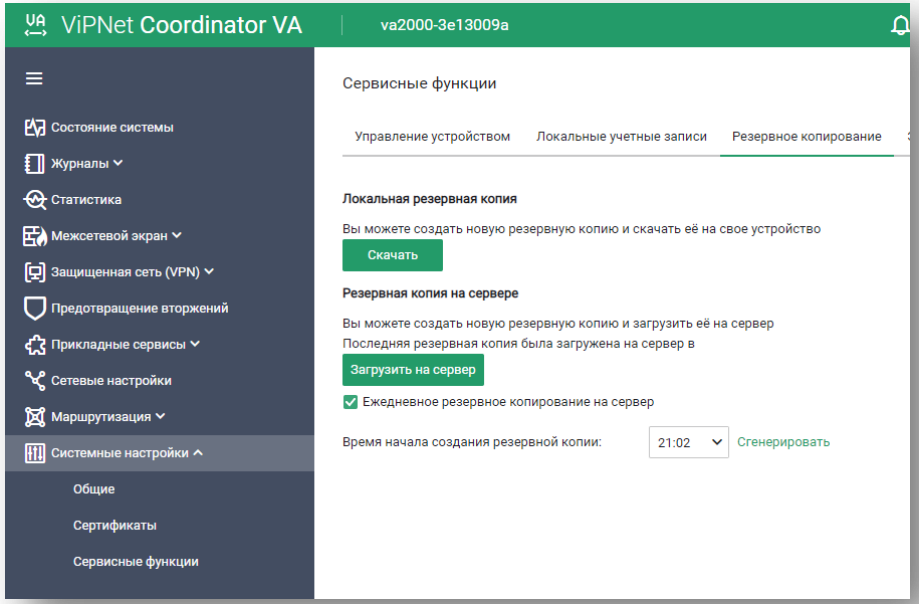
- Администратор
- Пользователь (Аудитор)

+

Централизованные учетные записи:

- Неограниченное количество
- Администратор/Аудитор
- Single Sign-On (SSO)

Резервное копирование



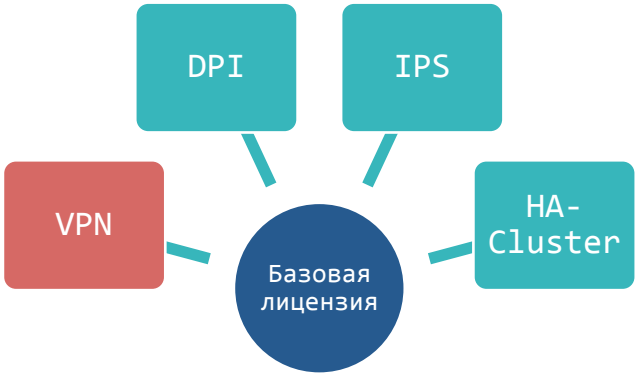
- Локальный экспорт на USB
- Удаленный экспорт через WebUI
- Выгрузка на сервер Prime

Новая схема лицензирования

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

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, Antivirus, ICAP

- Лицензируем на кластер для всех исполнений (HW и VA)
- Внешние подключения по ICAP не лицензируются:
  - Антивирусы
  - Песочницы
  - DLP

Поддержка аппаратных платформ

infotecs

ViPNet Coordinator HW50

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

ViPNet Coordinator HW100

- HW100 N1/N2/N3 *
- HW100 Q1/Q2 NEW

ViPNet Coordinator HW2000

- HW2000 Q4
- HW2000 Q5

ViPNet Coordinator HW1000

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

ViPNet Coordinator HW5000

- HW5000 Q1
- HW5000 Q2

* - режим VPN only

Что такое ГосСОПКА?

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации.

Цель системы — объединить усилия для предотвращения и противодействия кибератакам на критически важные информационные инфраструктуры. Для этого создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который организует сбор и обмен информацией об инцидентах между субъектами КИИ, координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению компьютерных атак.

Нормативные документы в области ГосСОПКА и безопасности КИИ

№ 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

АО «ПМ» сегодня

12
лет на рынке услуг SOC и исследования защищённости

7
лет центр ГосСОПКА (А)

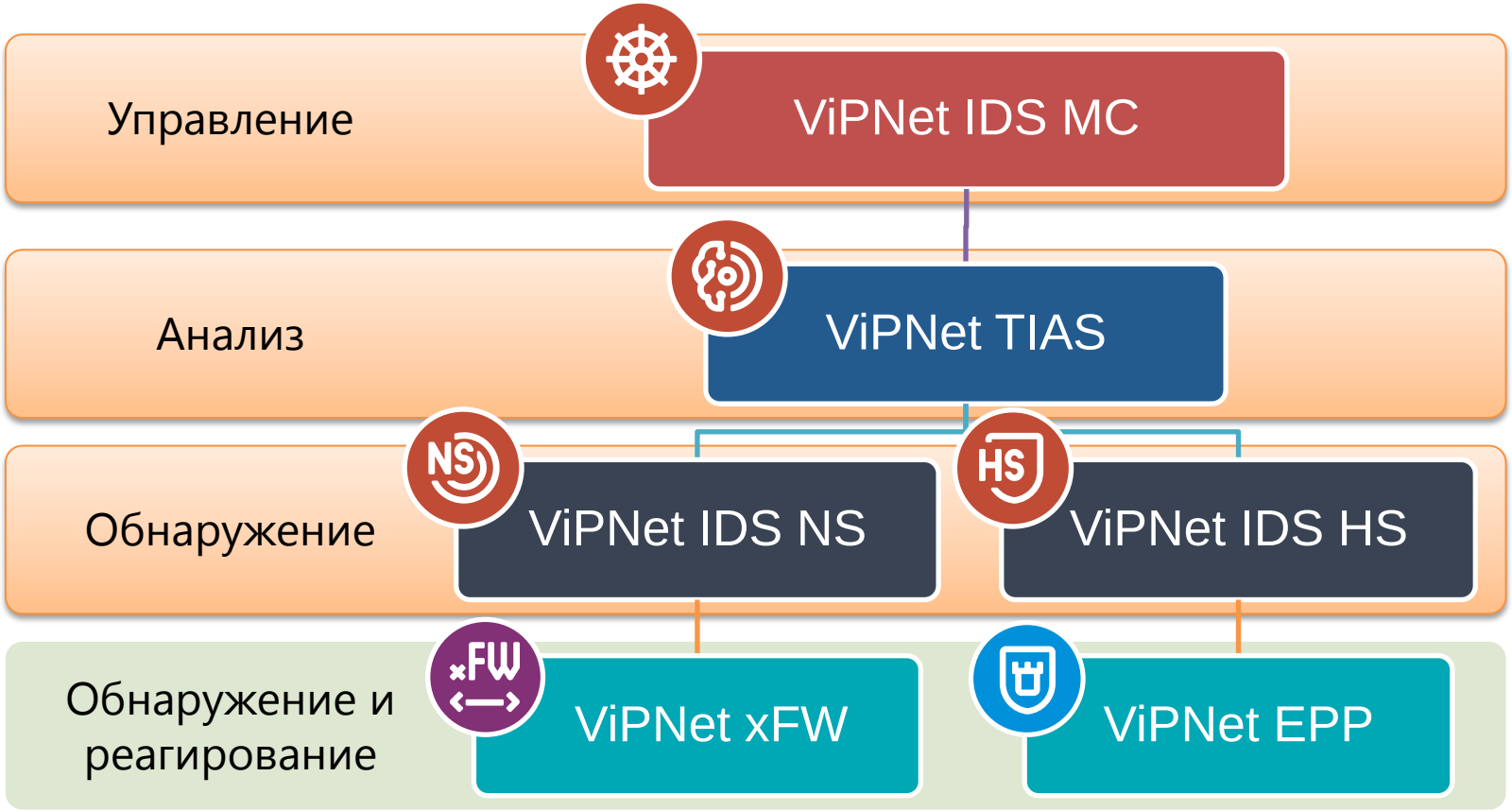
>1600
выполненных ИБ проектов

13
действующих киберполигонов Ampire

300+
проведенных киберучений

3000+
ИБ специалистов прошли обучение на Ampire

Решение ViPNet TDR



Назначение компонентов ViPNet TDR

ViPNet IDS MC

- Управлять инфраструктурой сенсоров
- Осуществлять мониторинг состояния сенсоров

ViPNet TIAS

- Анализировать события ИБ от сетевых и хостовых сенсоров и выявлять инциденты ИБ

ViPNet IDS NS

- Выявлять события, связанные с ИБ в сетевом трафике

ViPNet IDS HS

- Выявлять события ИБ и аномалии поведения на конечных узлах

Сенсоры

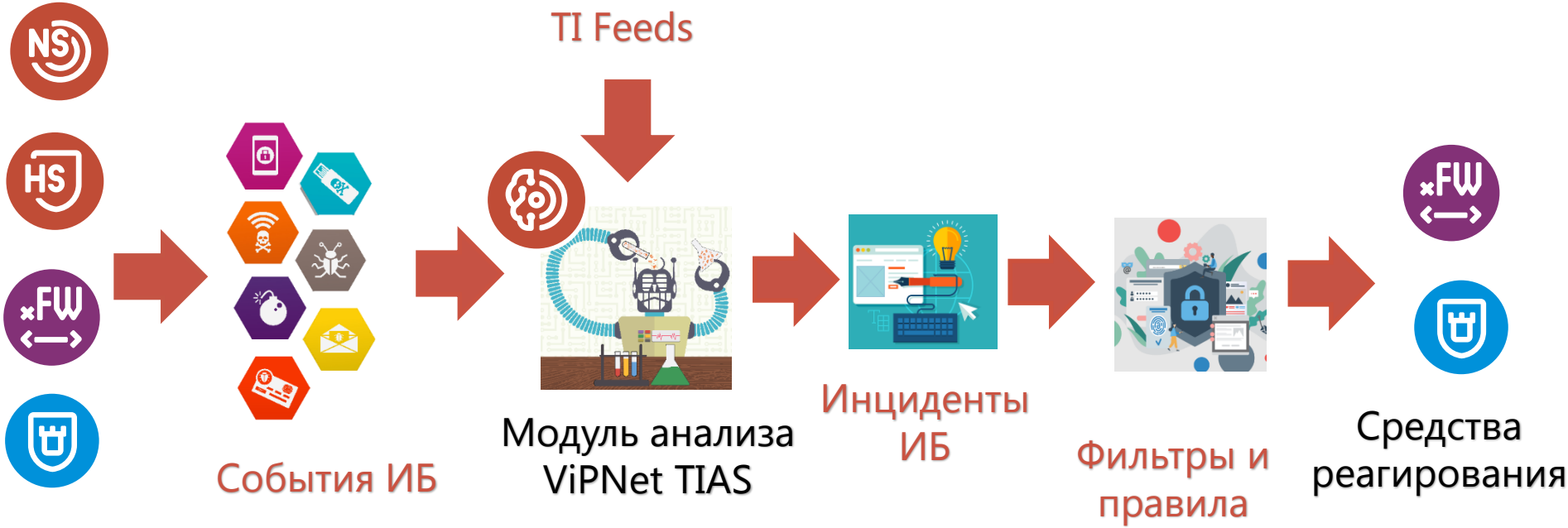
ViPNet IDS NS

✓ Система обнаружения вторжений уровня сети

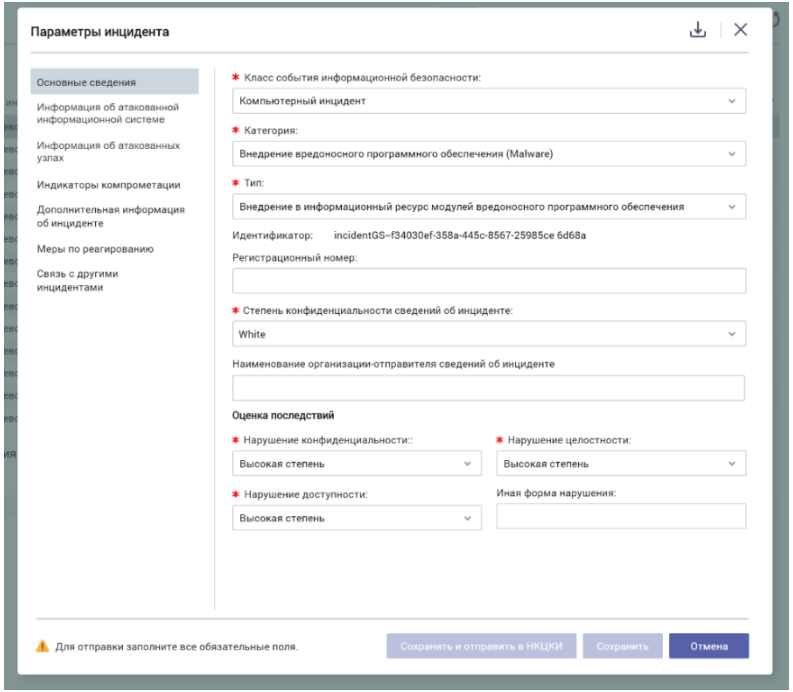
ViPNet IDS HS

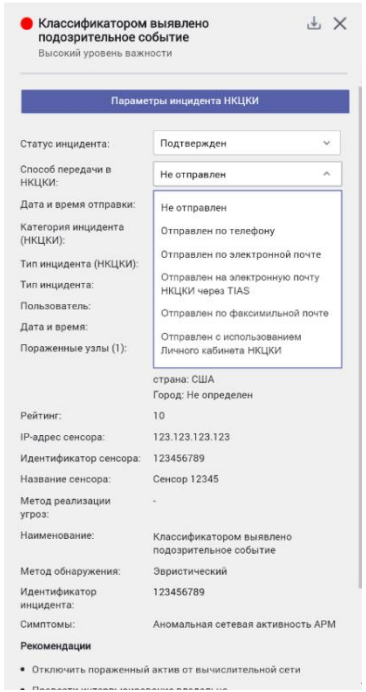
✓ Система обнаружения вторжений уровня узла

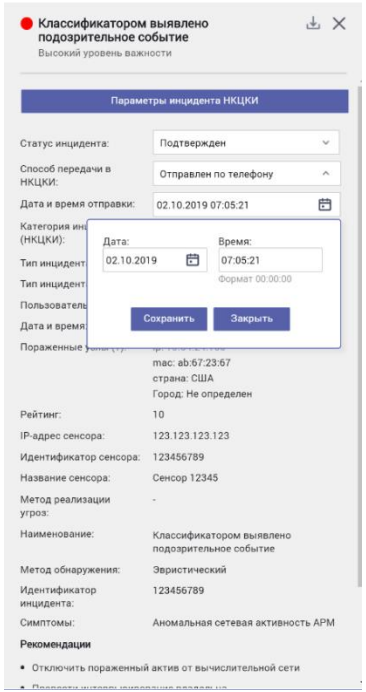
Как это работает?



Передача инцидентов в НКЦКИ ГосСОПКА с помощью ViPNet TIAS







Форензика

- Заключение по результатам расследования
- Документирование инцидента и собранных доказательств
- Результаты анализа причин, развития и последствий инцидента, предположения о виновных лицах
- Рекомендации по недопущению подобных инцидентов в будущем

Каждое подозрительное событие SOC является потенциальным инцидентом ИБ. Аналитики ПМ вручную исследуют и проводят расследование

200+
событий ежедневно

Варианты подключения

Самостоятельное подключение

ГОССОПКА

Субъект ГосСОПКА

- Заключить соглашение с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосСОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ

НКЦКИ

Подключение через корпоративный центр

ГОССОПКА

Корпоративный центр ГосСОПКА

- Заключить соглашение с корпоративным (ведомственным) центром ГосСОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности цента

Объект КИИ

Перечень мероприятий

Класс В

- Взаимодействие с НКЦКИ
- Разработка регламентирующих документов
- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах
- Регистрация атак и инцидентов
- Анализ событий ИБ
- Инвентаризация

Класс Б

- Анализ угроз ИБ
- Составление и актуализация перечня угроз
- Выявление уязвимостей
- Подготовка предложений по повышению уровня защищенности
- Составление перечня инцидентов

Класс А

- Ликвидация последствий
- Анализ результатов ликвидации последствий

Подключаясь к SOC ПМ вы получаете

- Затраты ниже, чем при постройке собственного SOC
- Время реагирования на инциденты – 30 минут
- Актуальные экспертные данные о киберугрозах, которые разрабатываются и поставляются ежедневно
- Квалифицированные сотрудники центра мониторинга, которые углубляют свои знания, совершенствуют навыки, регулярно проходят киберучения на Ampire
- Платформа по сбору, обработке и анализу событий ИБ для выявления атак на ранних этапах и расследования инцидентов
- Удобная аналитика состояния ИБ за счёт информативного и понятного личного кабинета

- Время подключения – от 1 недели
- Подключение к ГосСОПКА – от 1 дня
- Гибридная модель оказания услуг
- Безопасность как сервис (MSSP)

Преимущества КЦ ГосСОПКА as Service

- Оптимизация затрат на ИБ за счёт сервисной модели
- Высокий уровень устойчивости к киберугрозам
- Быстрый старт и масштабируемость
- Качественный сервис вместо длительного интеграционного проекта

Ст. 10 187-ФЗ «системы безопасности ЗОКИИ должны обеспечивать непрерывное взаимодействие с ГосСОПКА.

Подключение к внешнему (коммерческому) центру ГосСОПКА позволяет передать задачи в области обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ специализированной организации.

Кроме того, воспользовавшись услугами внешнего центра ГосСОПКА, организация перекладывает на исполнителя риски несоответствия законодательству РФ в области ведения незаконного предпринимательства (ст. 171 УК РФ) в части ведения деятельности без соответствующих лицензий ФСБ РФ и/или ФСТЭК России.

Спасибо за внимание!

Санников Александр
ООО «КриптоСвязь»
www.infotrust.ru
vpn@infotrust.ru
+7(3412) 918-100