GIS DAYS

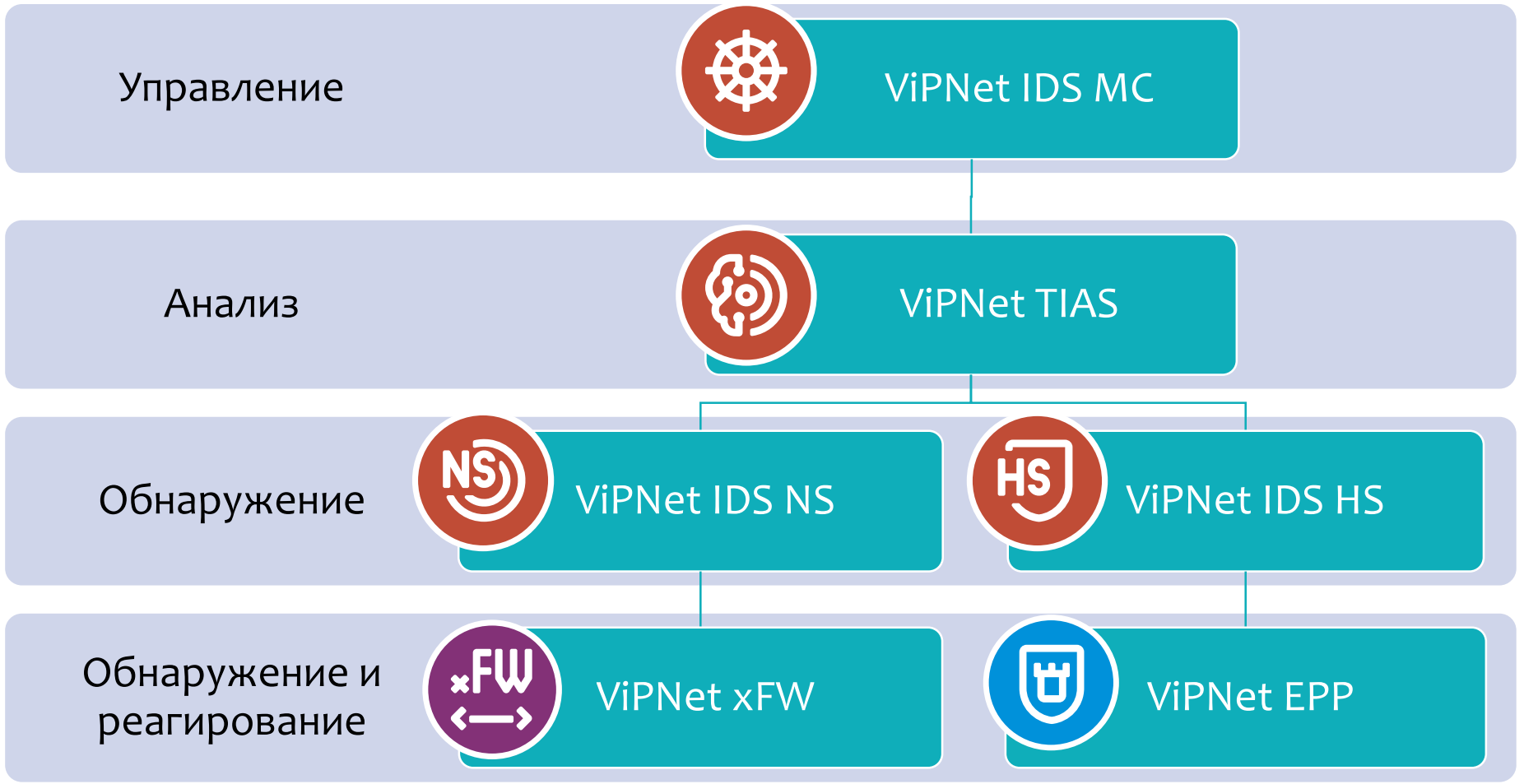
Методы машинного обучения для выявления угроз ИБ и способы их реализации

Старовойт Светлана Геннадьевна
Руководитель направления ИнфоТеКС

План презентации

1. О решении ViPNet TDR
2. Взгляд на обнаружение компьютерных атак сквозь призму ML
3. Комплексное ML-решение для решения ViPNet TDR
4. Процесс разработки ML-модулей
5. Возникающие проблемы и способы их решения

Решение ViPNet TDR

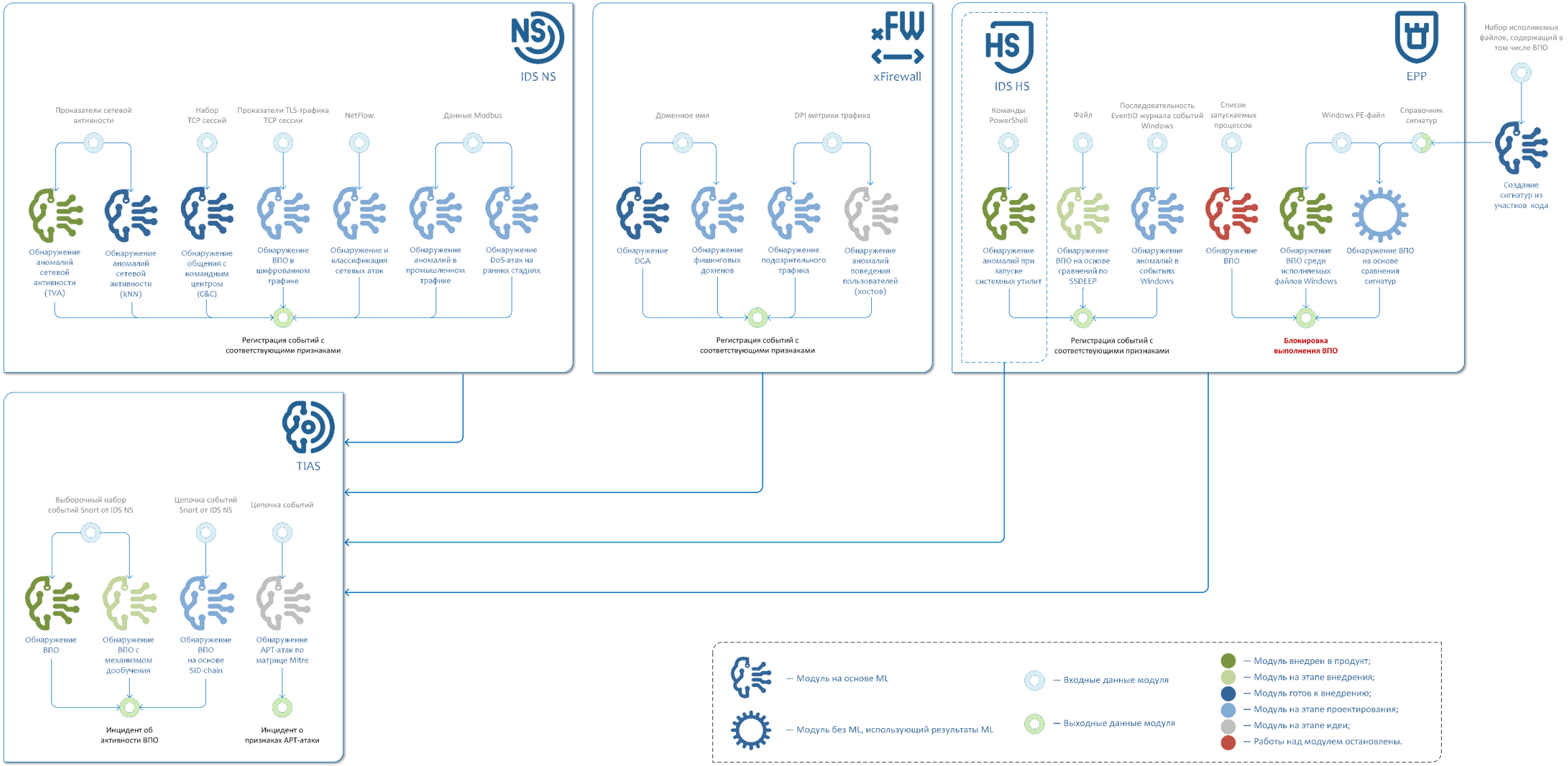


Сила правил и недостатки ML

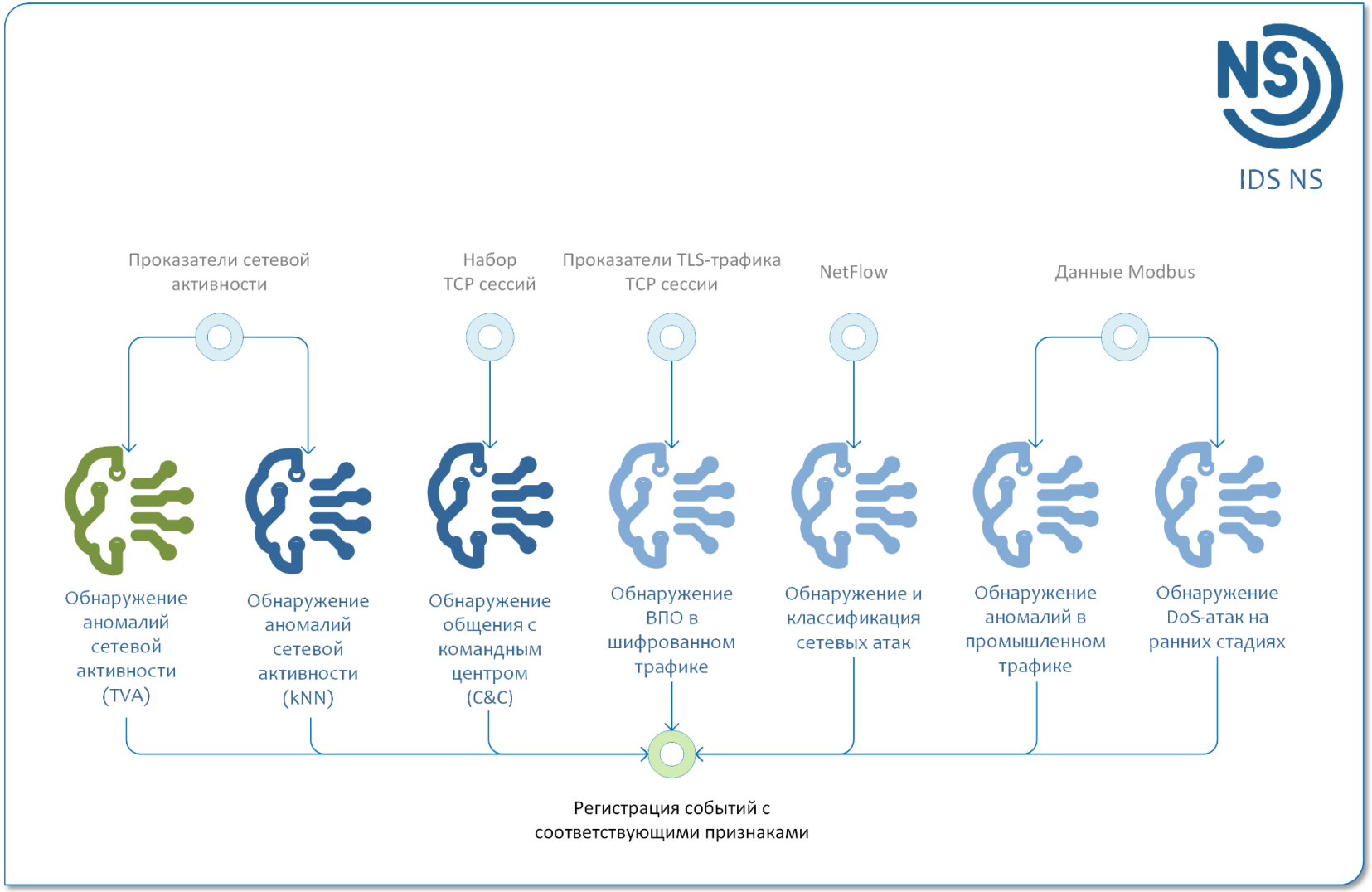
Rules	Критерий	Machine Learning
Высокая	Интерпретируемость результата	Низкая
Высокая вовлеченность	Привлечение эксперта ИБ для поддержки инструмента в актуальном состоянии	Низкая вовлеченность
Отсутствует	Адаптация к новым данным	Высокая

Модели машинного обучения

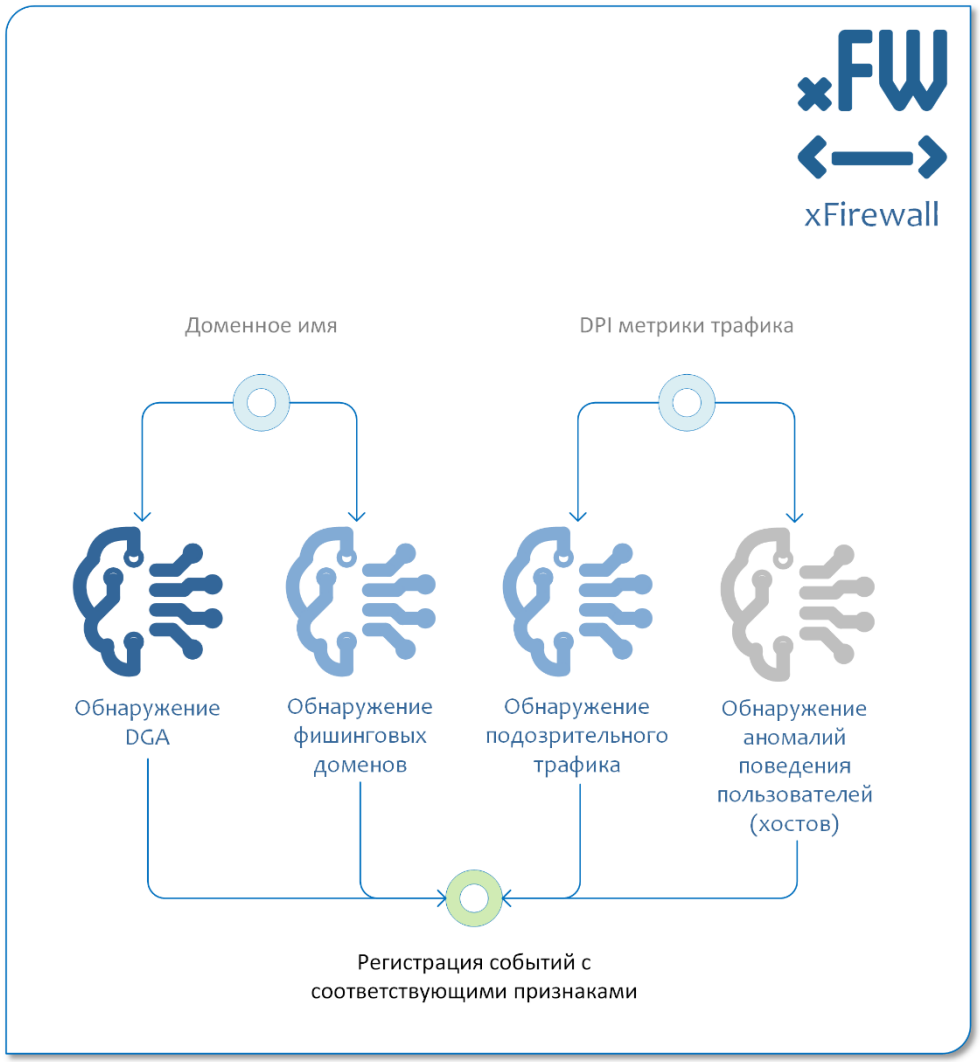
ML-модули в составе продуктов решения



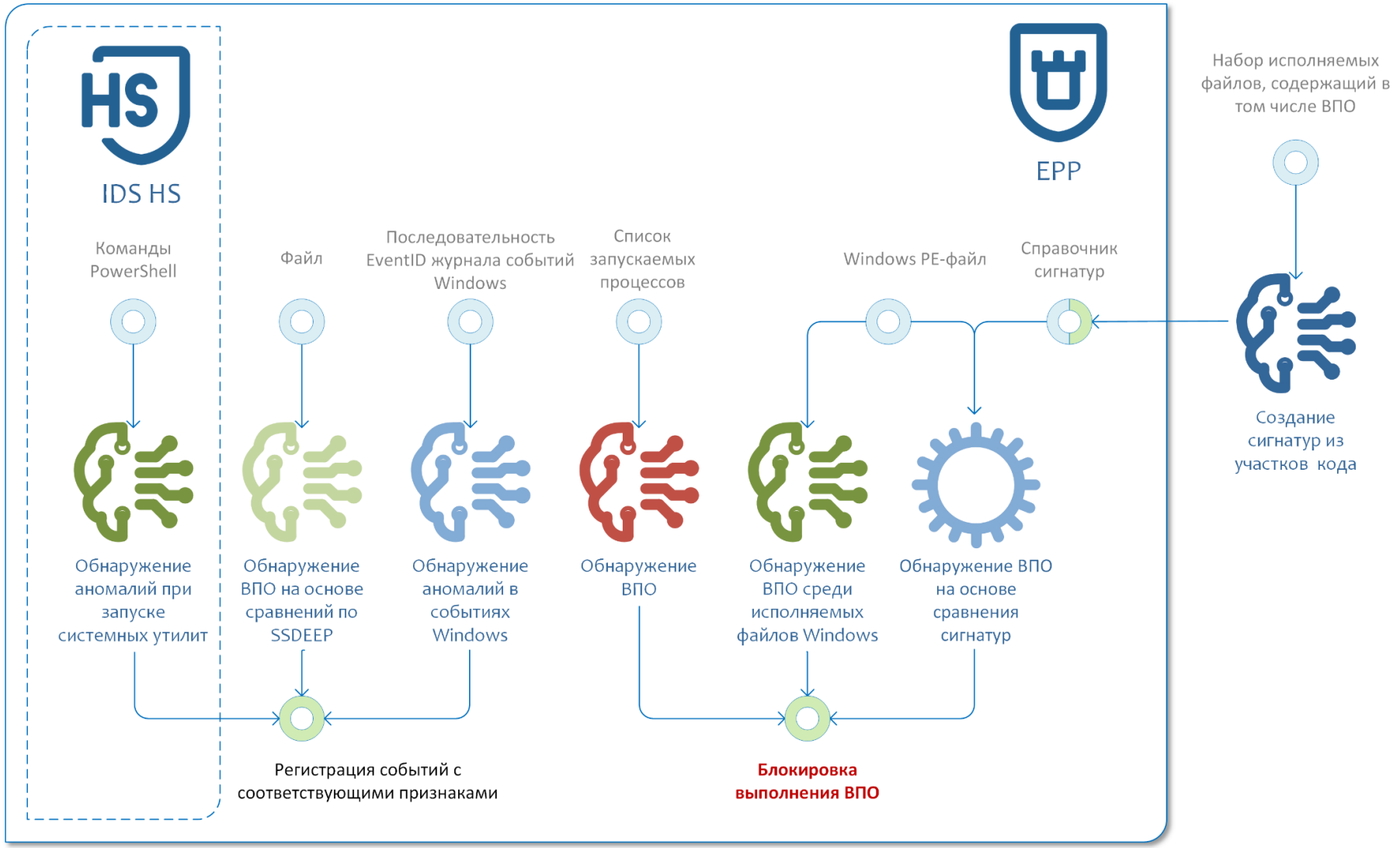
Анализ сетевой активности в IDS NS



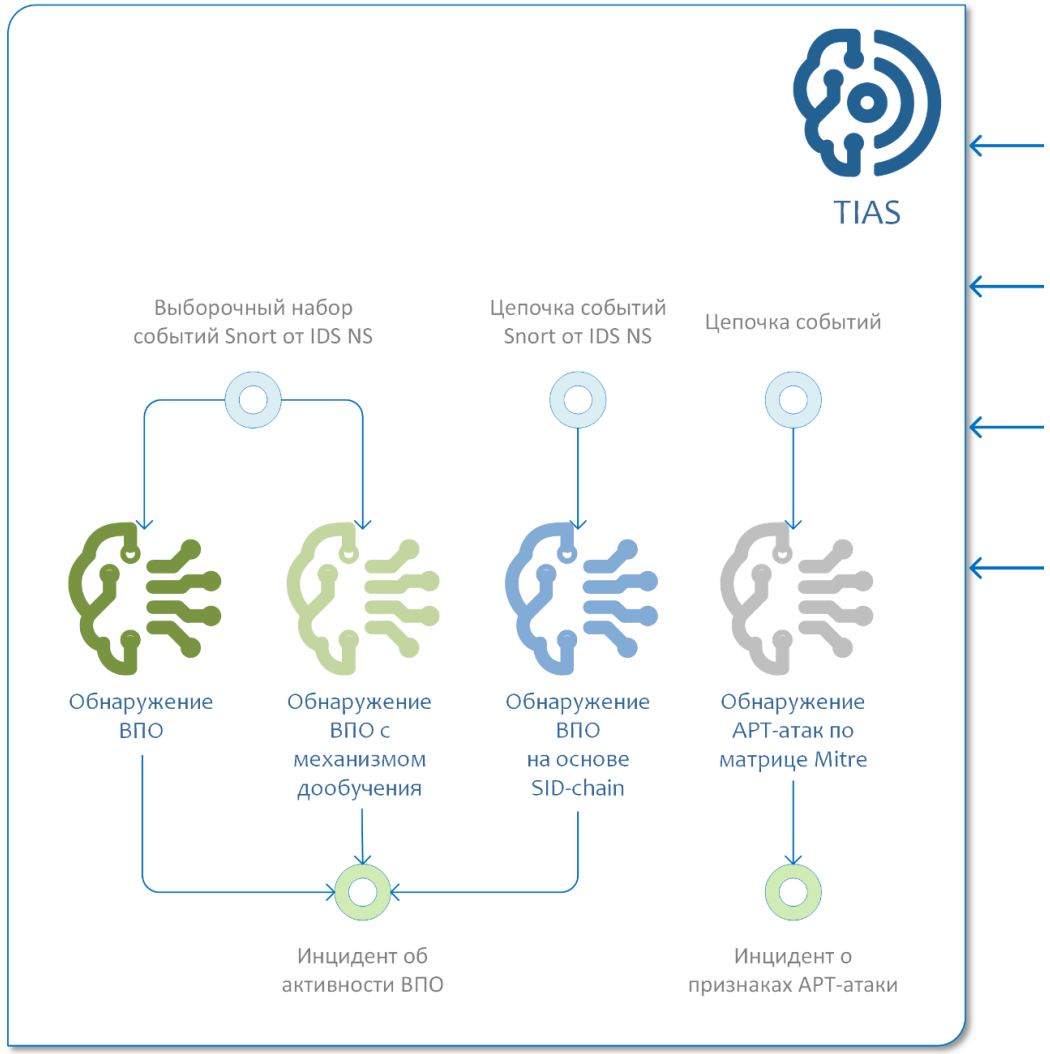
Обнаружение сгенерированных имен в xFirewall

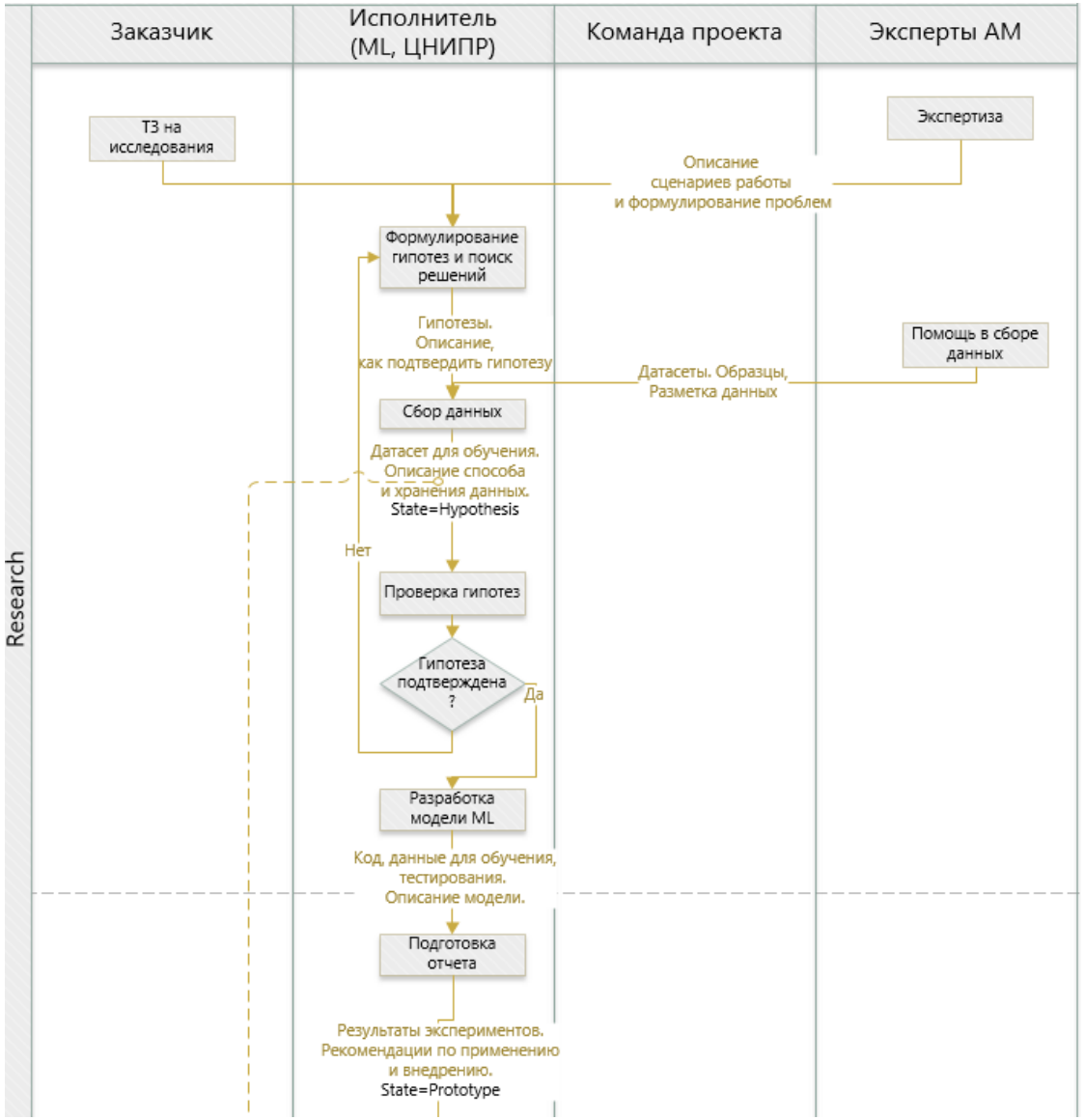


ML-модули в составе EndPoint Protection

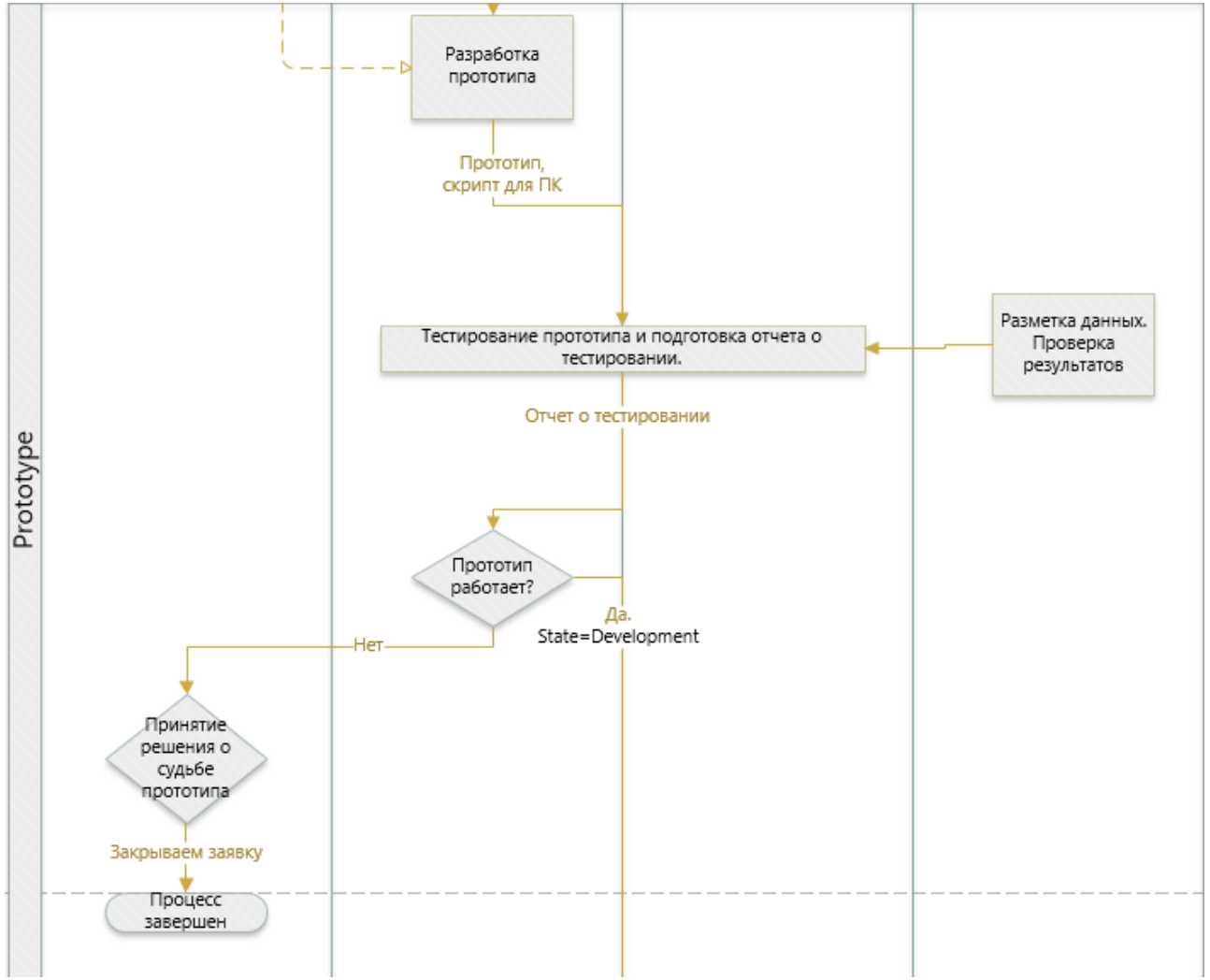


ML-модули в составе TIAS

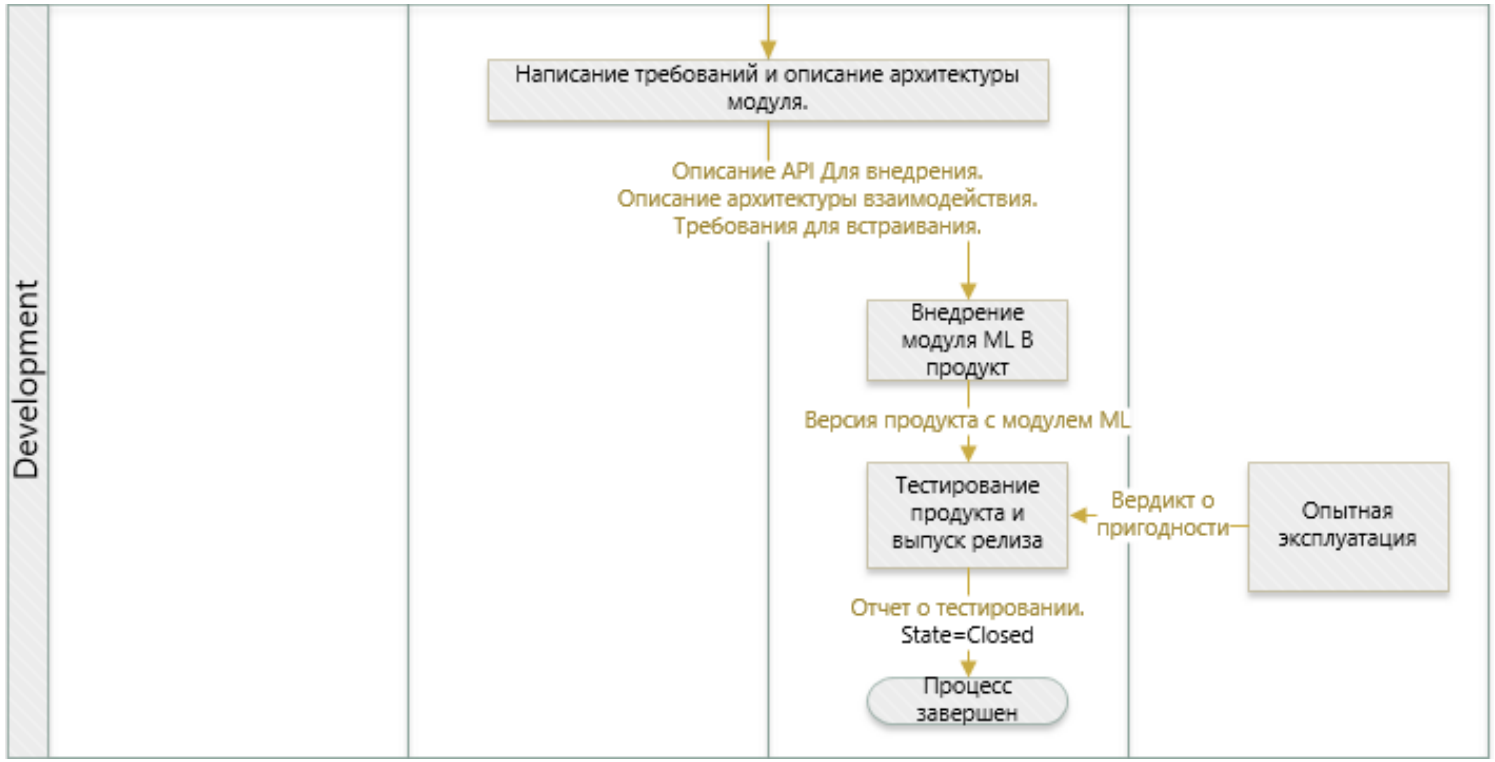




Процессы
шаг 1:
проверка гипотезы



Процессы
шаг 2:
прототипирование



Процессы шаг 3: разработка

Проблемы

Интерпретация результатов

Сбор датасетов

Ресурсоемкость модели

СПАСИБО ЗА ВНИМАНИЕ

https://infotecs.ru/

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363