

Непрерывное взаимодействие с Центром ГосСОПКА

Максим Кувшинов

Руководитель обособленного подразделения
в г. Новосибирск





География офисов АО «ПМ»

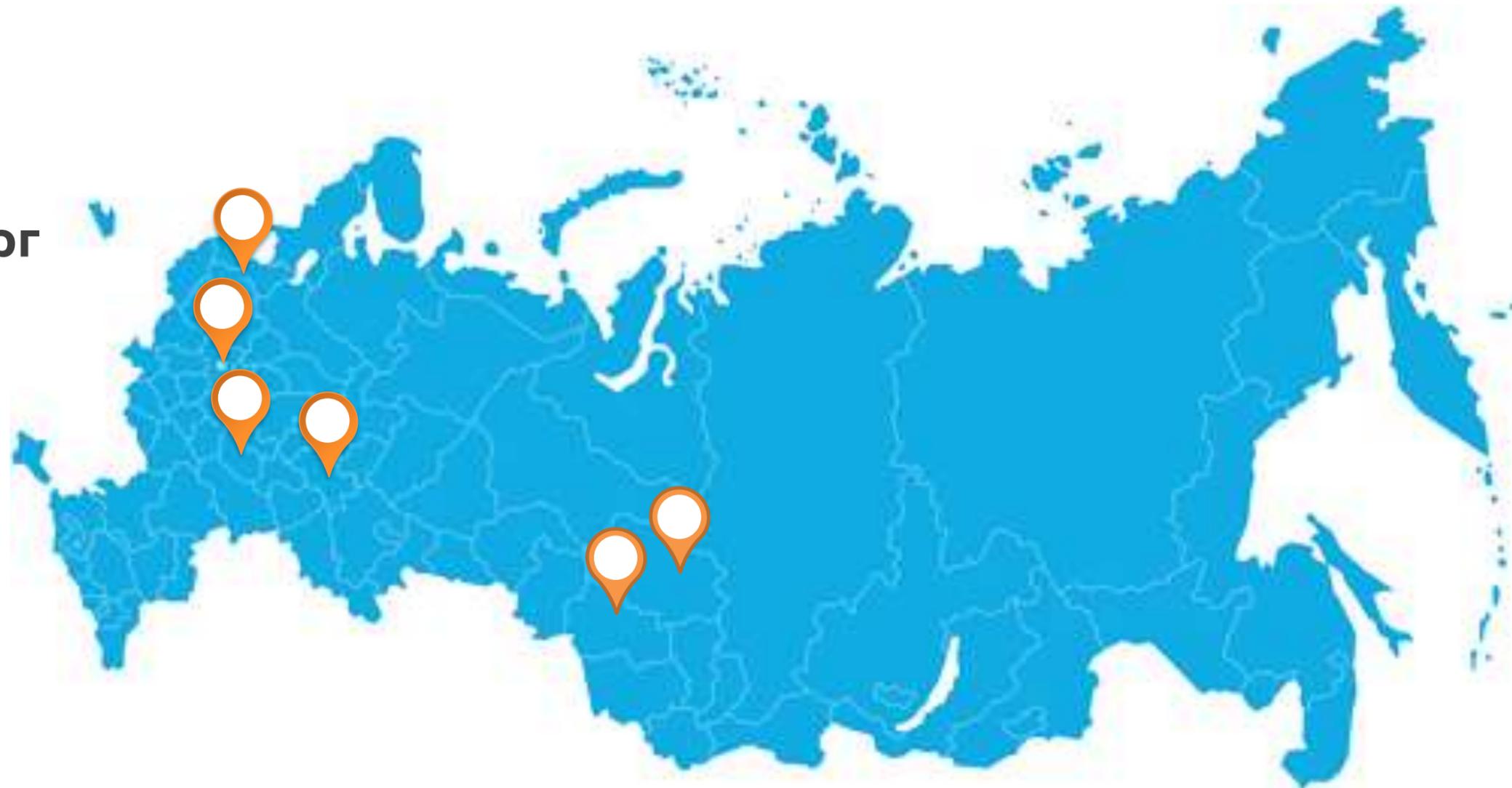
Санкт-Петербург

Москва

Пенза

Новосибирск

Томск



Входим в группу компаний «ИнфоТеКС»



Центр мониторинга (в цифрах)

15 000

Событий в секунду

> 20 000

Конечных агентов

6

Поддерживаем
SIEM/LC

> 400

Сетевых сенсоров
IDS/IPS

> 50

Поддерживаем
ViPNet TIAS

> 150 000

Инфраструктура
узлов

2014

год запуска

с 2017 года

Центр ГосСОПКА
класса А

24/7

режим
сопровождения

Проекты в СФО



Кузбасс

1,2,3 линия



Красноярский
край

2,3 линия



Омская
область

1,2,3 линия



Республика
Тыва

1,2 линия



Холдинг
«Новопорт»

1,2,3 линия



Алтайский
край

1,2 линия



Какие проблемы решает Центр ГосСОПКА?

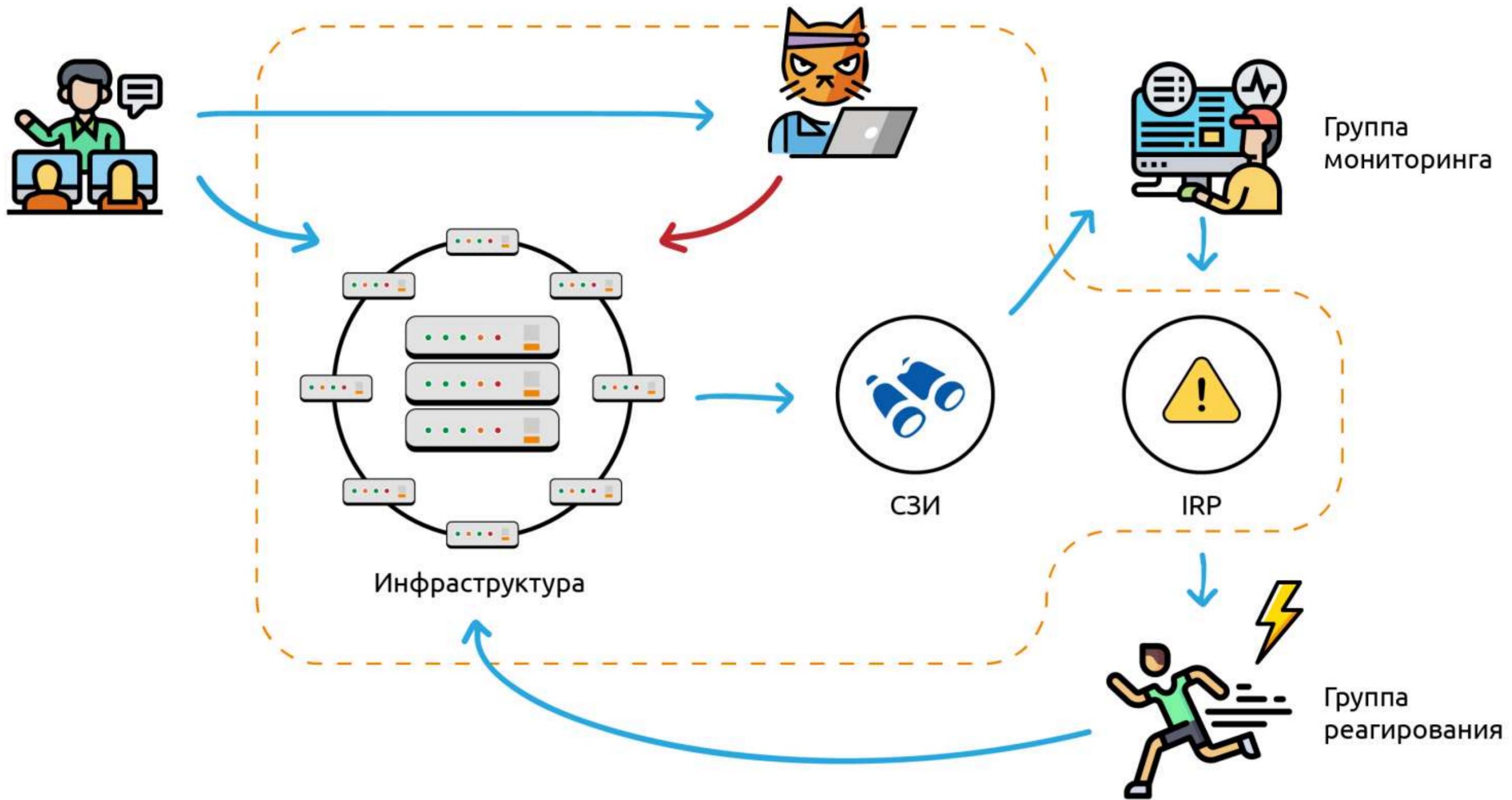
Что входит

- 1) Анализ компьютерных атак (инцидентов)
- 2) Единая Система управления инцидентами
- 3) Тесты на проникновение (Pentest)
- 4) Тюнинг конфигурации WAF/SIEM
- 5) Взаимодействие с НКЦКИ, ФСО России
- 6) TI Feeds (IOC)
- 7) Эксперты-исследователи. База знаний
- 8) Процессы. SLA. Playbook/runbook
- 9) Категорирование объектов КИИ
- 10) **Киберполигон Amprige**

И многое другое

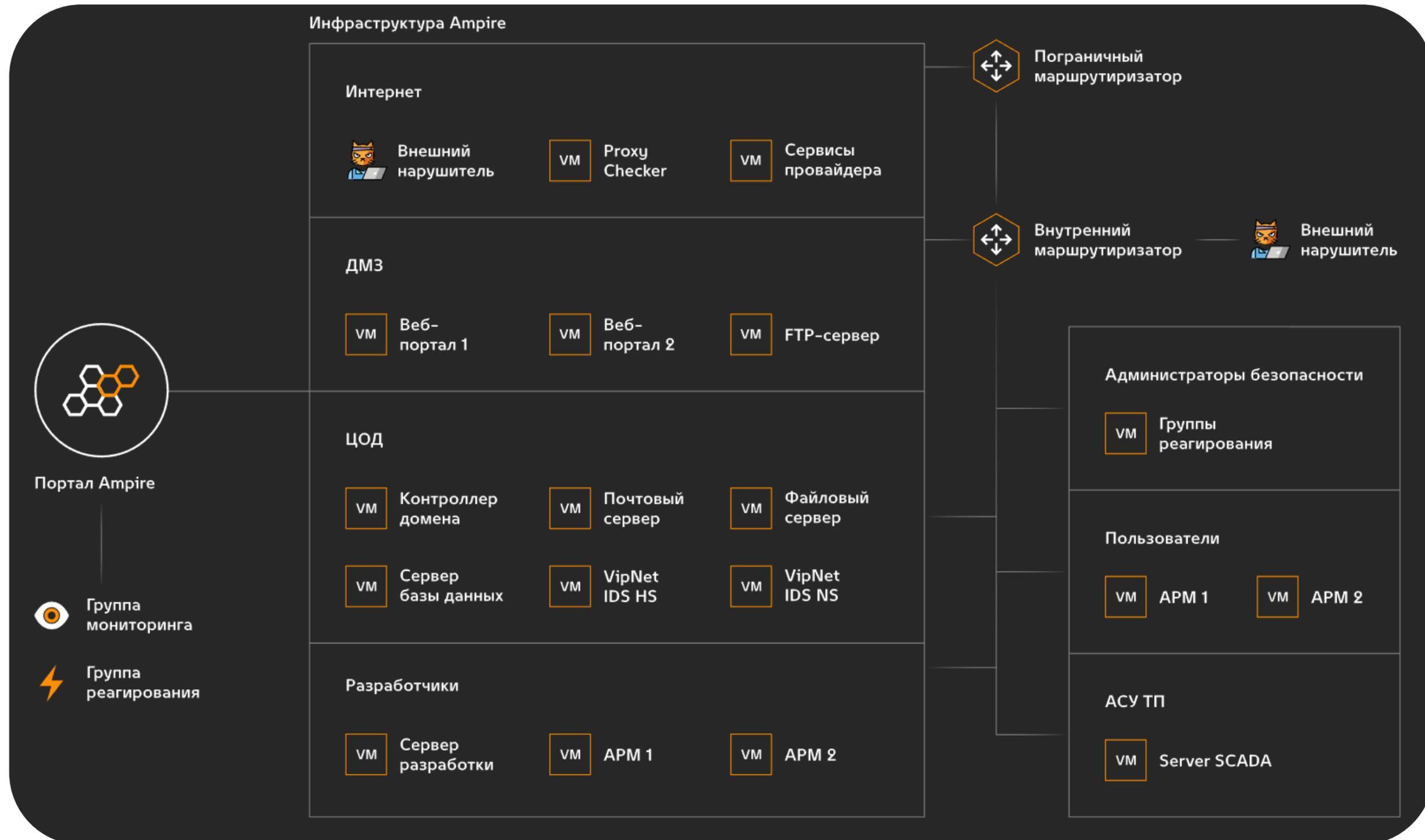
Киберполигон







Шаблон «Предприятие»





Базовые сценарии киберучений

1

Защита базы данных
предприятия

2

Защита контроллера домена
предприятия

3

Защиты файлового сервера
предприятия (MS17-070)

4

Защита данных сегмента АСУ ТП

5

Защита научно-технической
информации предприятия

6

Защита корпоративного портала
от внутреннего нарушителя



Учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.



Правовые **основания**



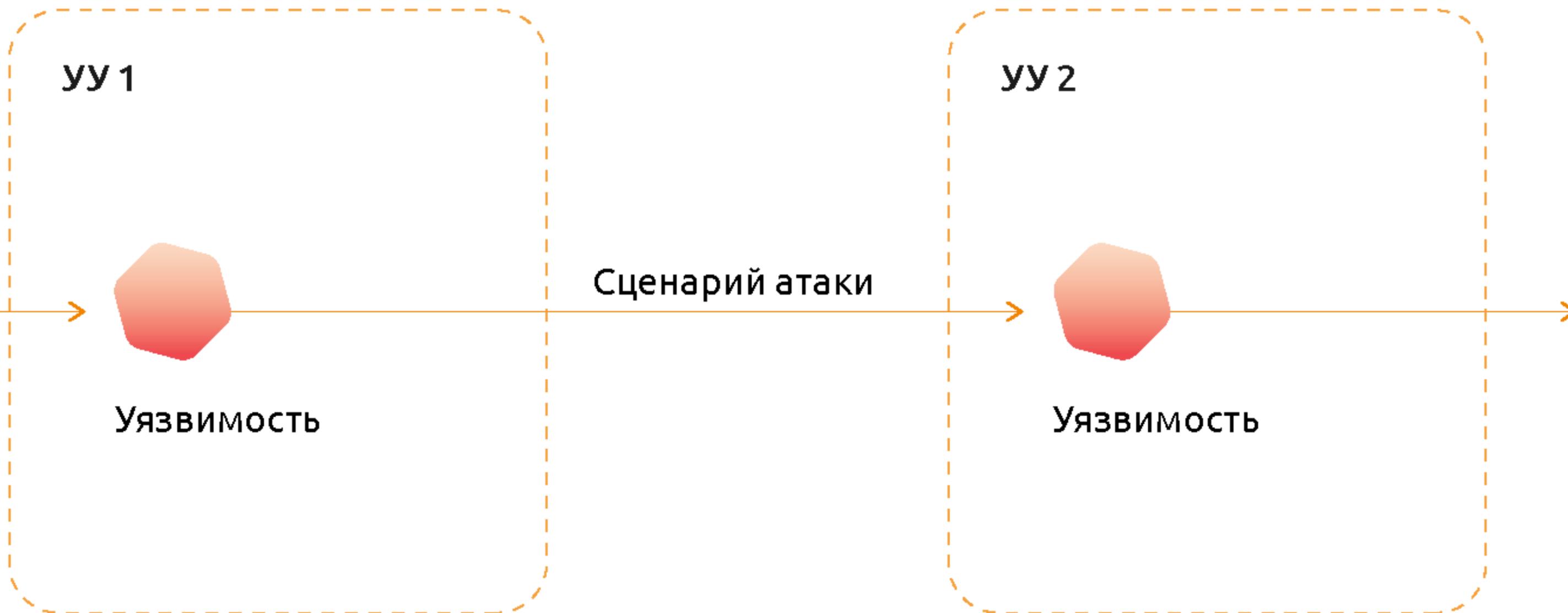
- 1** Указ Президента РФ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
- 2** Федеральный закон «О безопасности критической информационной инфраструктуры» 187-ФЗ.
- 3** Федеральный закон «Об информации, информационных технологиях и о защите информации» 149-ФЗ.
- 4** Концепция ГосСОПКА.



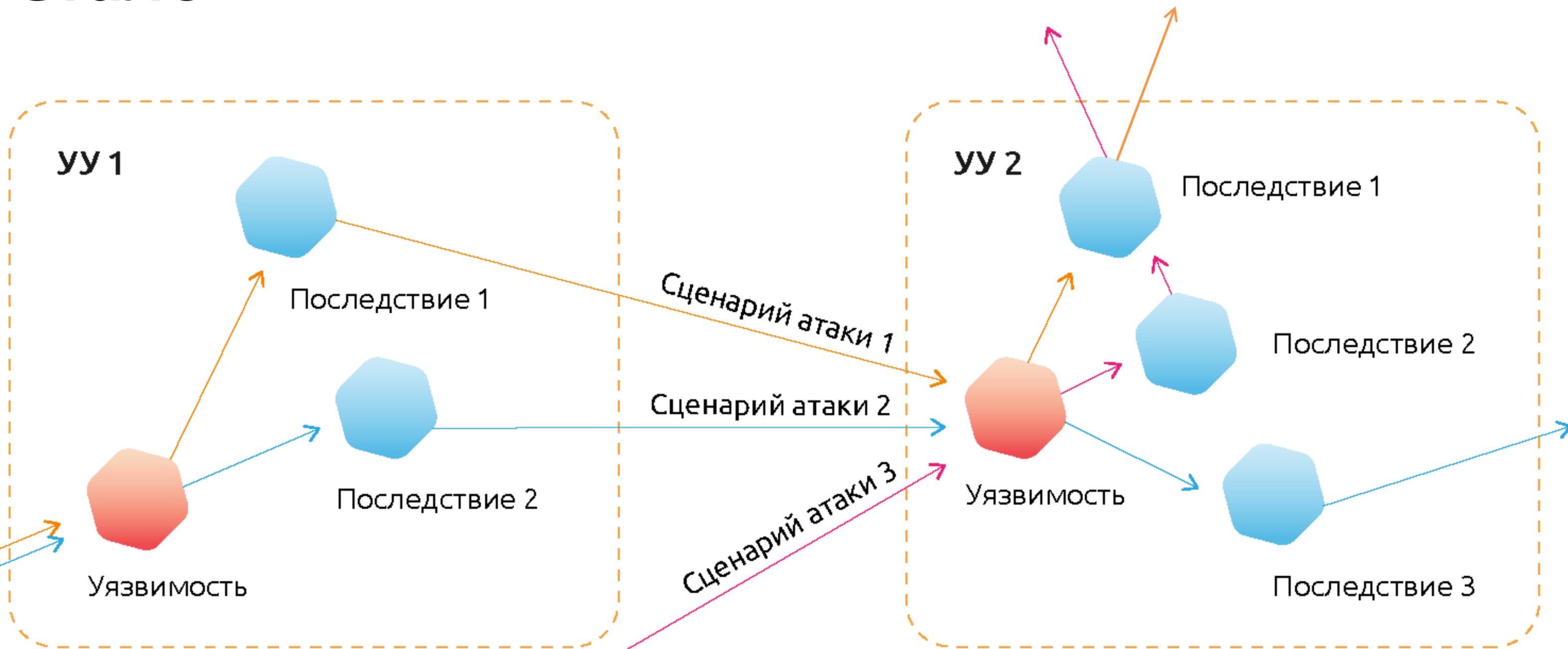
Идея Конфигуратора —
дать возможность преподавателю
самостоятельно подготавливать шаблон
организации и формировать вектор атаки



Было



Стало



ОБЩАЯ ИНФОРМАЦИЯ

ИНЦИДЕНТЫ

УЧАСТНИКИ

СХЕМА ШАБЛОНА

ЛОГИ СОБЫТИЙ АТАКИ

ОБЩАЯ ИНФОРМАЦИЯ О ТРЕНИРОВКЕ

Название тренировки	Квест 29_11
Шаблон	Предприятие (конфигуратор)
Сценарий	Защита SCADA
Группа	test
Статус тренировки	завершена
Доступные действия	скачать отчёт

Начало тренировки 29.11.2022 12:16
 Конец тренировки 29.11.2022 13:11

ПРОГРЕСС АТАКИ 100%



Схема шаблона



Скачать методические материалы

Участники

ГРУППА test	
МОНИТОРИНГ	в сети 0 / 1
РЕАГИРОВАНИЕ	в сети 0 / 2
ЛИДЕР РЕАГИРОВАНИЯ	не в сети



WORDPRESS DUPLICATOR

УСТРАНЕНО



ZEROLOGON

УСТРАНЕНО



IGSS32

УСТРАНЕНО

ИНЦИДЕНТЫ

Новые	0/0
Рассматриваются	0/0
Закрытые	0/0
Цепочки кибератаки	0/1



IGSS32 REVERSE SHELL

УСТРАНЕНО



AD USER

УСТРАНЕНО



WORDPRESS DEFACE

УСТРАНЕНО

ДОСТУПНЫЕ РЕСУРСЫ

Удалённое рабочее место	10.10.211.235
SecOnion	10.10.211.114
ViPNet TIAS	Информация отсутствует
ViPNet IDS NS	10.10.211.128

Стартовые параметры

Шаблон: **Предприятие**
Нарушитель: **Внешний нарушитель**
Стартовый сегмент: **Интернет**
Заражённый хост: **Хост отсутствует**

Список СЗИ

SecOnion

VPNnet IDS NS

ОТКРЫТЬ СХЕМУ ШАБЛОНА

Этап №1

Сегмент: **DMZ**
Узел: **Umbraco**
Уязвимость: **Umbraco**
Последствие: **Umbraco WebShell Backdoor**

Этап №2

Сегмент: **ЦОД**
Узел: **MS Exchange**
Уязвимость: **Exchange ProxyLogon**
Последствие: **Exchange China Chopper**

+ ДОБАВИТЬ

Выберите сегмент

ЦОД

Выберите узел

MS Exchange

Выберите уязвимость

Exchange ProxyLogon

Требуется сканирование

Выберите последствие

Exchange China Chopper

ОТМЕНИТЬ

СОХРАНИТЬ

Техническая зрелость



Единственная учебно-тренировочная платформа, в состав которой входят СЗИ линейки ViPNet

Возможно удалённое подключение к платформе

1

2

Устанавливается непосредственно на инфраструктуре заказчика

3



Целевая аудитория



- **Студенты** с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- **ИБ-специалисты**, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- **ИТ-специалисты**: **новички** и те, кто хотел бы увеличить перечень навыков в резюме.



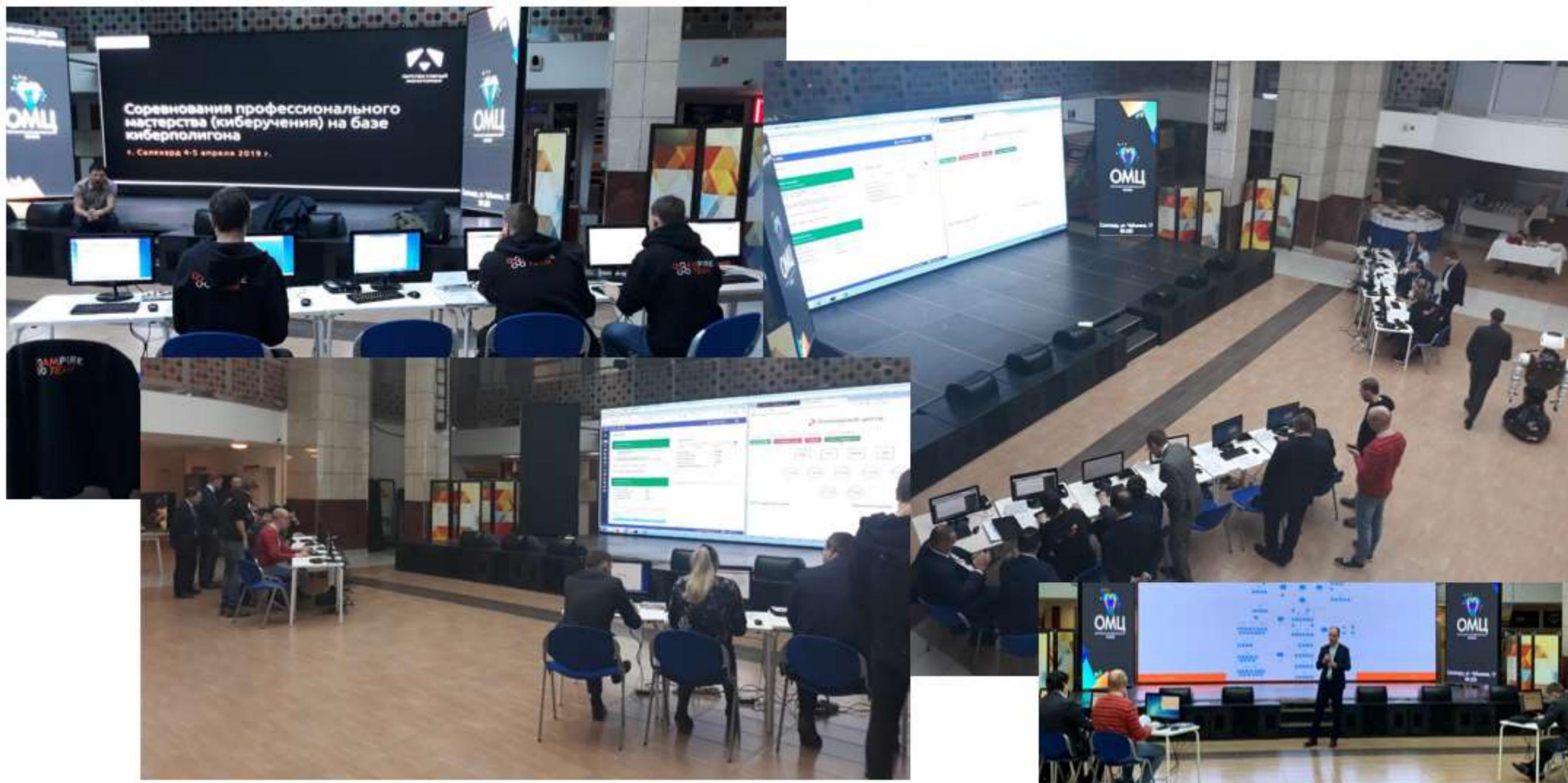
В поставку **входят**

- ✓ Программное обеспечение Amrige
- ✓ Подготовка преподавателей для работы с комплексом
- ✓ Рабочая программа, методические материалы

- ✓ Техническая поддержка
- ✓ Обновление контента

Комплекс продолжит работать и без техподдержки

Киберучения



Спасибо
за внимание!



t.me/pm_public

amonitoring.ru

Максим Кувшинов

Руководитель обособленного
подразделения г. Новосибирск

+7 (495) 737-61-97

Maksim.Kuvshinov@amonitoring.ru