ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Киберполигон Ampire

Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак

Атакуют, обязательно атакуют

Кибервойска

Криминал

Наёмники

Кибервойска

Отчёт «Энерджинет»

Диаграмма 9.
Оценка подготовленности выпускников

Диаграмма 8.
Соответствие подготовки выпускников требованиям работодателей

Аналитический отчёт «Об образовании специалистов по информационной безопасности в Российской Федерации», экспертная подгруппа по кибербезопасности НТИ «Энерджинет», декабрь 2021 года

Проактивная позиция

Не можем повлиять

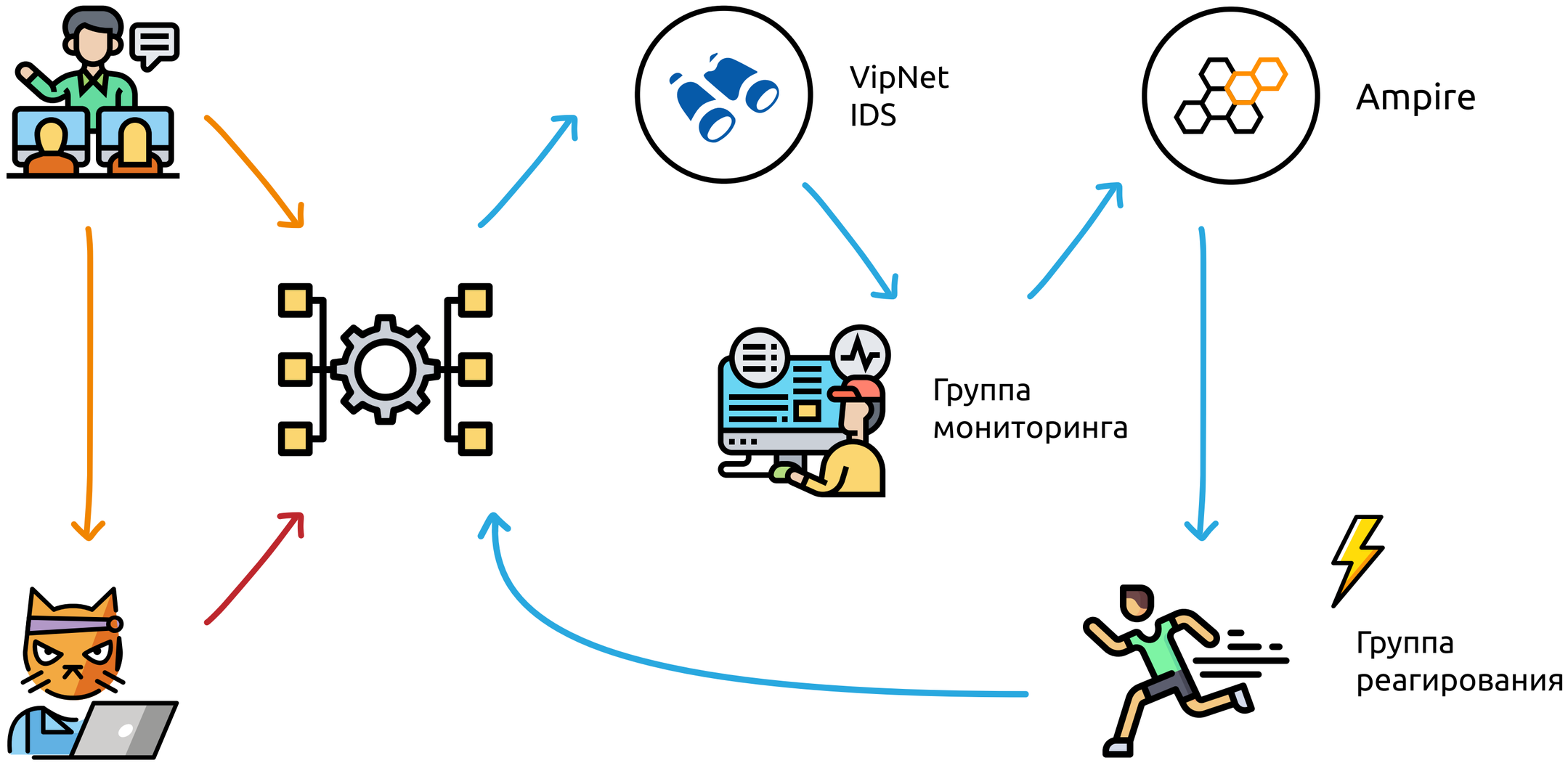
1) Сам факт атаки
2) Квалификация атакующего
3) Инструментарий
4) Объём ресурсов

Можем повлиять

1) Стоимость атаки
2) Скорость реакции
3) Содержание реакции
4) Собственный опыт
5) Планы и изменения

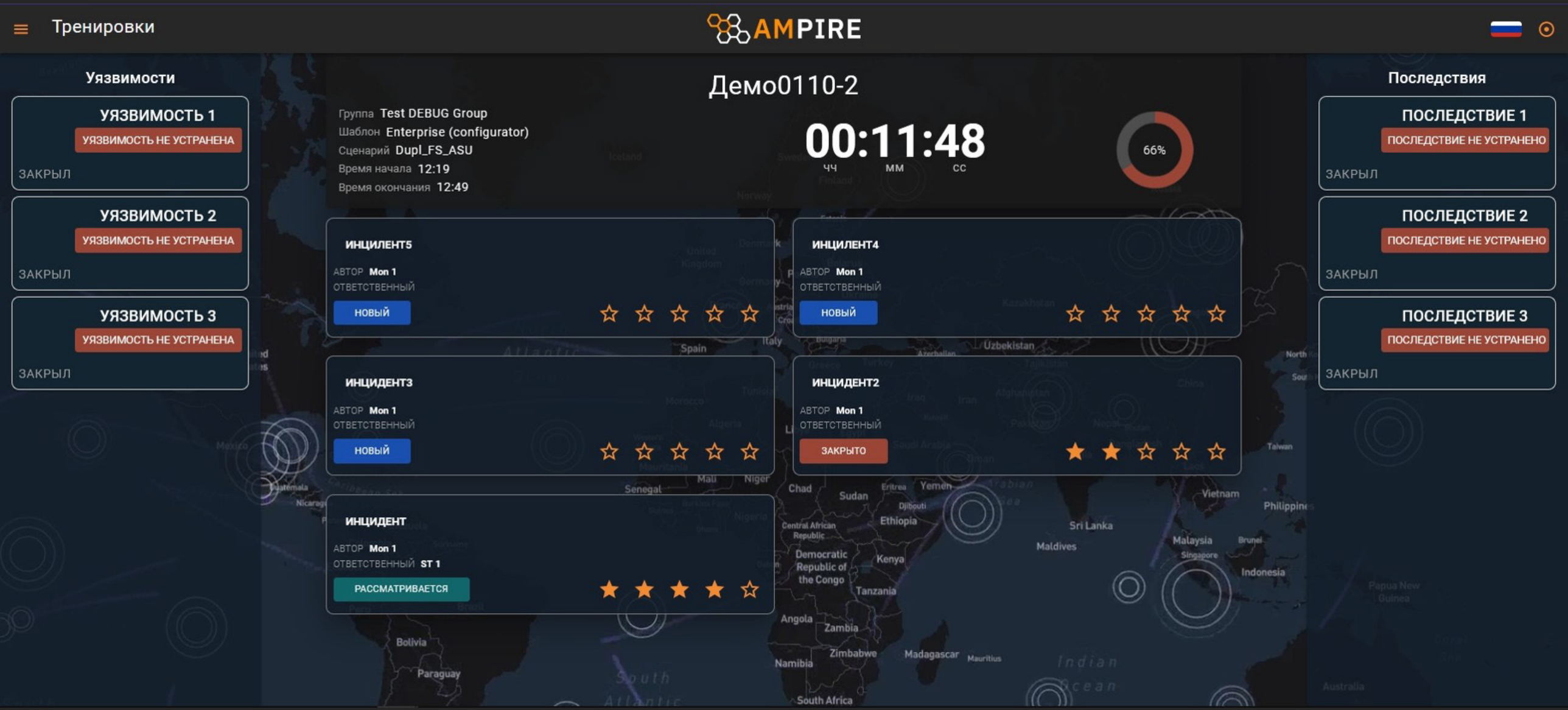
Ampire —
готовый продукт

- Аппаратная часть
- Кодовая база
- Документация
- Процесс поставки и техподдержки
- Прайс


VipNet
IDS
Ampire
Группа
мониторинга
Группа
реагирования

Портал Ampire

- Раздел преподавателя
- Раздел обучаемого
- Подключение к инфраструктуре тренировки
- Система управления инцидентами
- Мультиязычность
- Генератор отчётов


Тренировки
AMPIRE
Уязвимости
УЯЗВИМОСТЬ 1
УЯЗВИМОСТЬ НЕ УСТРАНЕНА
ЗАКРЫЛ
УЯЗВИМОСТЬ 2
УЯЗВИМОСТЬ НЕ УСТРАНЕНА
ЗАКРЫЛ
УЯЗВИМОСТЬ 3
УЯЗВИМОСТЬ НЕ УСТРАНЕНА
ЗАКРЫЛ
Демо0110-2
Группа Test DEBUG Group
Шаблон Enterprise (configurator)
Сценарий Dupl_FS_ASU
Время начала 12:19
Время окончания 12:49
00:11:48
ЧЧ ММ СС
66%
ИНЦИЛЕНТ5
АВТОР Mon 1
ОТВЕТСТВЕННЫЙ
НОВЫЙ
ИНЦИЛЕНТ4
АВТОР Mon 1
ОТВЕТСТВЕННЫЙ
НОВЫЙ
ИНЦИДЕНТ3
АВТОР Mon 1
ОТВЕТСТВЕННЫЙ
НОВЫЙ
ИНЦИДЕНТ2
АВТОР Mon 1
ОТВЕТСТВЕННЫЙ
ЗАКРЫТО
ИНЦИДЕНТ
АВТОР Mon 1
ОТВЕТСТВЕННЫЙ ST 1
РАССМАТРИВАЕТСЯ
Последствия
ПОСЛЕДСТВИЕ 1
ПОСЛЕДСТВИЕ НЕ УСТРАНЕНО
ЗАКРЫЛ
ПОСЛЕДСТВИЕ 2
ПОСЛЕДСТВИЕ НЕ УСТРАНЕНО
ЗАКРЫЛ
ПОСЛЕДСТВИЕ 3
ПОСЛЕДСТВИЕ НЕ УСТРАНЕНО
ЗАКРЫЛ

ОБЩАЯ ИНФОРМАЦИЯ О ТРЕНИРОВКЕ

НАЗВАНИЕ: Занятия по защите БД 22.03.2022

ШАБЛОН: Корпоративная сеть

СЦЕНАРИЙ: Защита базы данных предприятия

ГРУППА: Demo group

СТАТУС ТРЕНИРОВКИ: Активна

01:14:21

ЧЧ ММ СС

ПРОГРЕСС АТАКИ 78 %

Схема шаблона | Скачать методические материалы | Список задач

ДОСТУПНЫЕ РЕСУРСЫ

VipNet IDS HS	10.10.211.121
VipNet IDS NS	10.10.211.122
VipNet TIAS	10.10.211.124
Seconion	10.10.211.123

3/6

Уязвимость 1 — СЕРВЕР НЕДОСТУПЕН — ЗАКРЫЛ:

Уязвимость 2 — УЯЗВИМОСТЬ НЕ УСТРАНЕНА — ЗАКРЫЛ:

Уязвимость 3 — СЕРВЕР НЕДОСТУПЕН — ЗАКРЫЛ:

DRUPALGEDDON 2 — УЯЗВИМОСТЬ УСТРАНЕНА — ЗАКРЫЛ: Анастасия Чиркина

AV — УЯЗВИМОСТЬ УСТРАНЕНА — ЗАКРЫЛ: Пупкин Василий

DEF — УЯЗВИМОСТЬ УСТРАНЕНА — ЗАКРЫЛ:

Создать новый инцидент

Cyber Kill Chain

2/6

ПОСЛЕДСТВИЕ 1 — СЕРВЕР НЕДОСТУПЕН — УСТРАНИЛ:

ПОСЛЕДСТВИЕ 2 — УЯЗВИМОСТЬ НЕ УСТРАНЕНА — УСТРАНИЛ:

ПОСЛЕДСТВИЕ 3 — СЕРВЕР НЕДОСТУПЕН — УСТРАНИЛ:

ПОСЛЕДСТВИЕ — УЯЗВИМОСТЬ УСТРАНЕНА — УСТРАНИЛ: Анастасия Чиркина

ПОСЛЕДСТВИЕ 5 — УЯЗВИМОСТЬ НЕ УСТРАНЕНА — УСТРАНИЛ:

ПОСЛЕДСТВИЕ — УЯЗВИМОСТЬ УСТРАНЕНА — УСТРАНИЛ:

ИНЦИДЕНТЫ

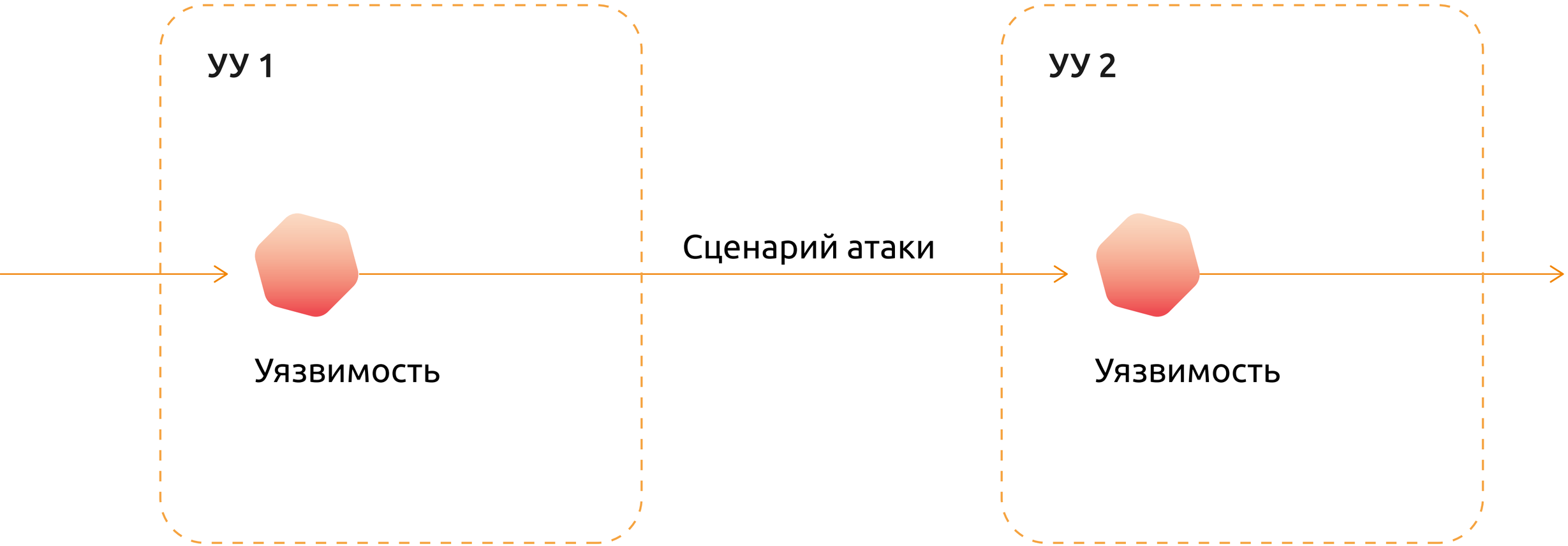
Новые	10 / 22
Рассматриваются	7 / 22
Закрытые	5 / 22

Базовые сценарии киберучений

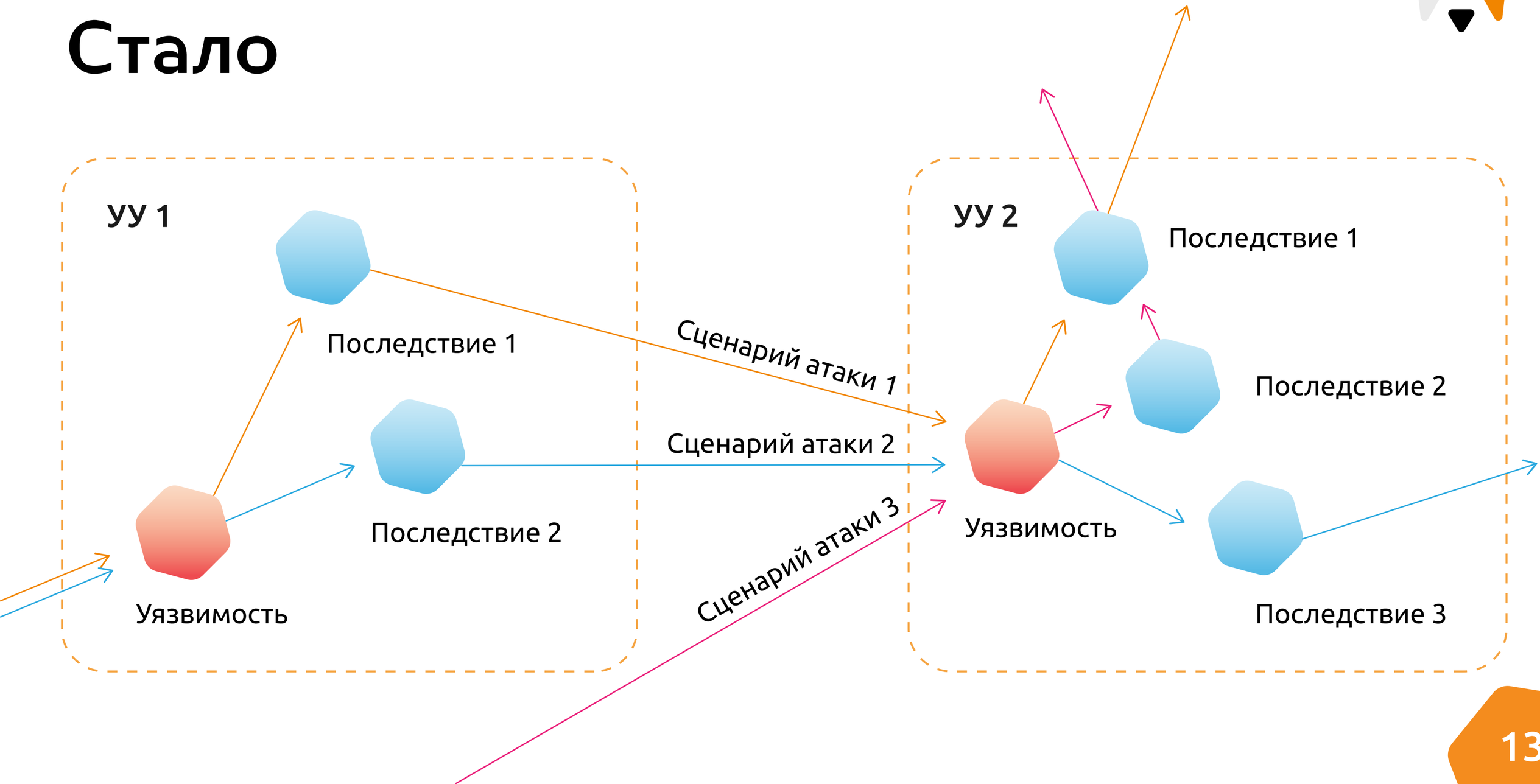
1. Защита базы данных предприятия
2. Защита контроллера домена предприятия
3. Защита файлового сервера предприятия (MS17-010)
4. Защита данных сегмента АСУ ТП
5. Защита научно-технической информации предприятия
6. Защита корпоративного портала от внутреннего нарушителя

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

Было



Стало


УУ 1
Последствие 1
Последствие 2
Уязвимость
Сценарий атаки 1
Сценарий атаки 2
Сценарий атаки 3
УУ 2
Последствие 1
Последствие 2
Уязвимость
Последствие 3

Конфигуратор сценариев

AMPIRE

1 Исходные данные — 2 Вектор атаки — 3 Схема атаки

Введите название сценария

Занятие №1 - атака на веб

Выберите шаблон: Предприятие

Укажите тип нарушителя: Внешний нарушитель

Укажите тип хоста: Хост нарушителя

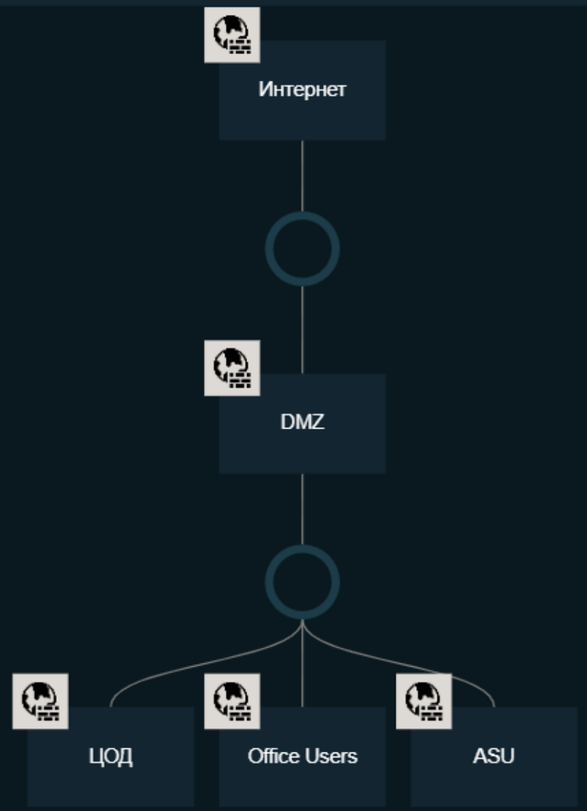
Выберите стартовый сегмент: Интернет

Выберите заражённый хост: Хост отсутствует

Выберите СЗИ

ViPNet IDS NS

- [x] ViPNet IDS NS
- [ ] SecOnion
- [ ] ViPNet TIAS



Список СЗИ

ViPNet IDS NS

СЗИ

- ViPNet IDS NS
- ViPNet IDS HS
- ViPNet TIAS
- IDS/IPS Suricata
- ELK
- Security Onion
- IDS/IPS Snort

И почти любые другие

Типы проводимых занятий

1. Киберучения
2. Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации
3. Противодействие группе реальных нарушителей (концепция Red Team и Blue Team)
4. Лабораторные работы по настройке средств безопасности и прикладных сервисов
5. Киберквесты

Сотрудничаем с ВУЗами

Сотрудничаем
с учебными центрами

Версии поставки

Функциональная характеристика	Academic	Academic Light
Кол-во шаблонов	3	1
Кол-во предварительно сконфигурированных сценариев	15	6
Кол-во поставляемых уязвимых узлов для конфигуратора	10	5
Лицензия MSSP	✓	

В поставку входят

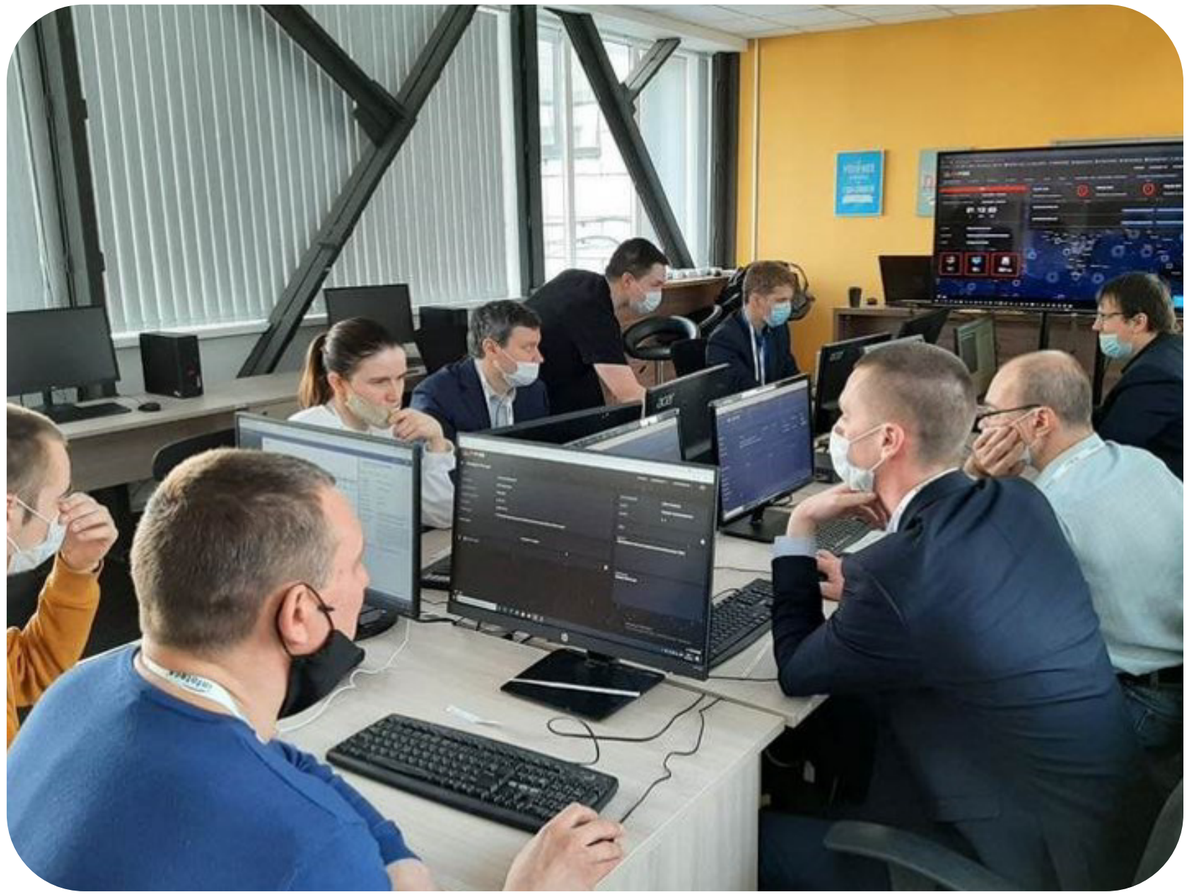
- Программное обеспечение Ampire
- Подготовка преподавателей для работы с комплексом
- Рабочая программа, методические материалы
- Техническая поддержка
- Обновление контента

Комплекс продолжит работать и без техподдержки

Технофест
в Екатеринбурге

Конференция
в Архангельске

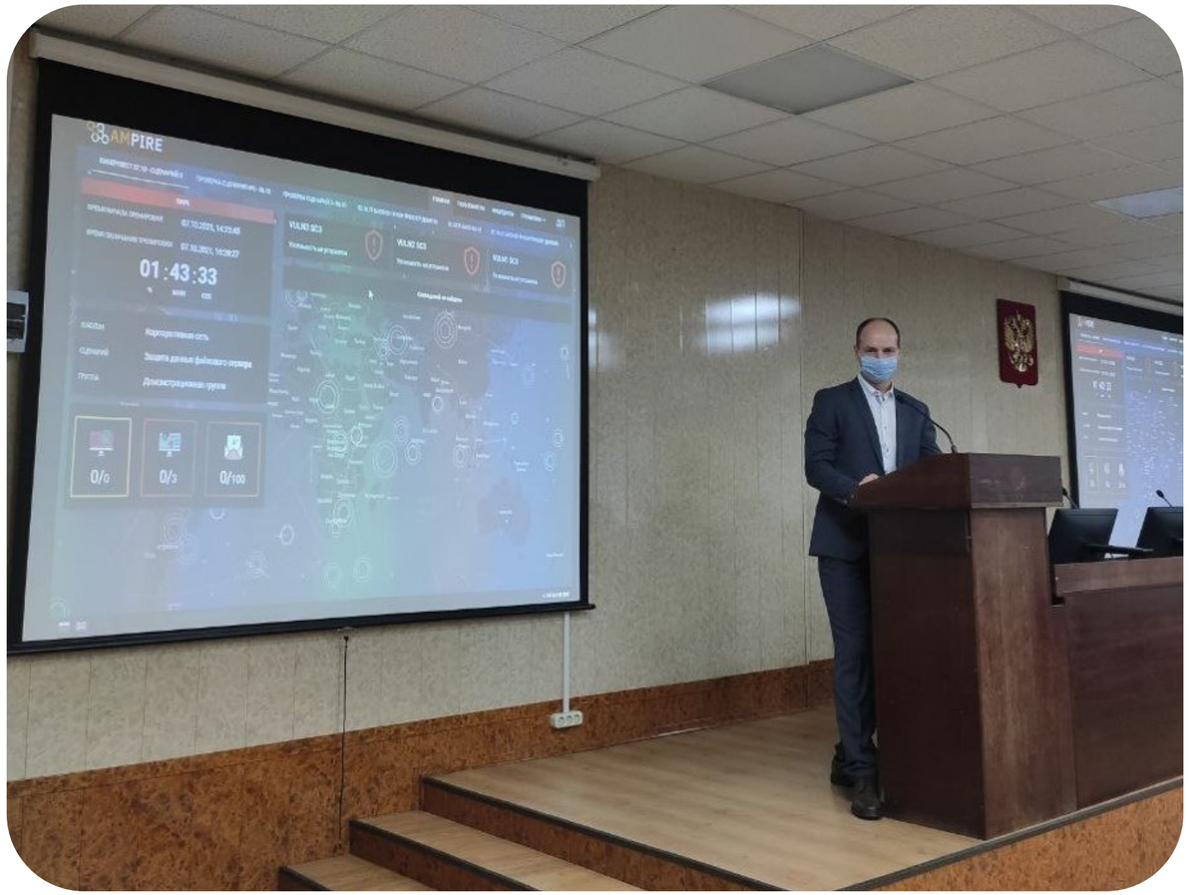
«Будни информационной безопасности»



Соревнования онлайн
в Казани и Якутии

Соревнования по защите информации «Команда безопасности»

Киберквест в МИРЭА
в Москве



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Сергей Нейгер

Директор по развитию бизнеса
«Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru