

Amrige – российская учебно-тренировочная платформа для проведения киберучений

Сергей Нейгер,
Директор по развитию бизнеса,
«Перспективный мониторинг»



Главный вопрос



- Что, если вы не являетесь профессиональным игроком на рынке ИБ?
- Что, если у вас нет департамента ИБ или выделенных специалистов ИБ?
- Что, если нужно оценивать навыки специалистов?

Как подготовиться и теоретически, и **практически** к киберугрозам?



Что такое **Ampire**



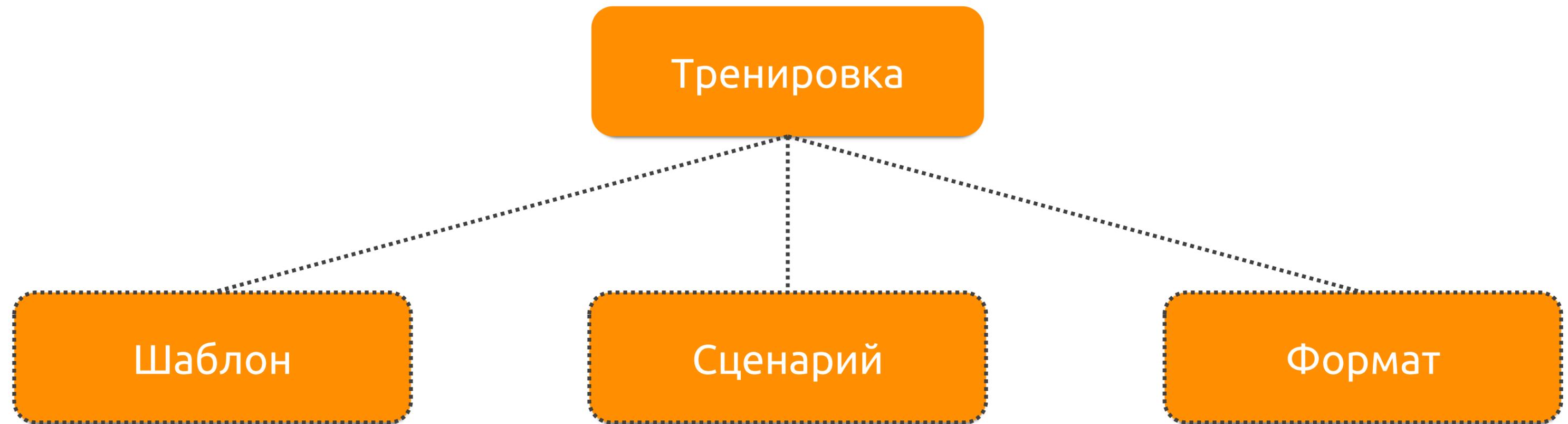
The screenshot displays the AMPiRE web interface. At the top, there is a navigation menu with 'Главная' and the AMPiRE logo. The main dashboard features a world map and four summary cards: 'Шаблонов 5', 'Сценариев 215', 'Активных тренировок 8', and 'Тренировок пройдено 1113'. Below this is a 'Тренировки' section with filters for 'ВСЕ', 'ТЕКУЩИЕ', and 'ЗАВЕРШЕННЫЕ'. Two training exercises are listed:

- Готова к запуску** Киберучения, Москва
 - Формат тренировки - BlueTeam
 - Сценарий - 1.Защита базы данных предприятия
 - Группа - Учебная группа МГ-182
 - Шаблон - Офис
 - Длительность - 90
 - Лидер - Иванов Андрей
- Запущена** Отработка уязвимостей в CMS
 - Формат тренировки - BlueTeam
 - Сценарий - Deface веб-сайта
 - Группа - Поток А2
 - Шаблон - Офис (Конфигуратор)
 - Длительность - 60
 - Лидер - Сергеев Михаил
 - Уязвимостей устранено: 0/3
 - Последствий устранено: 0/3
 - Количество инцидентов: 0

Учебно-тренировочная платформа

Отработка навыков противодействия киберугрозам

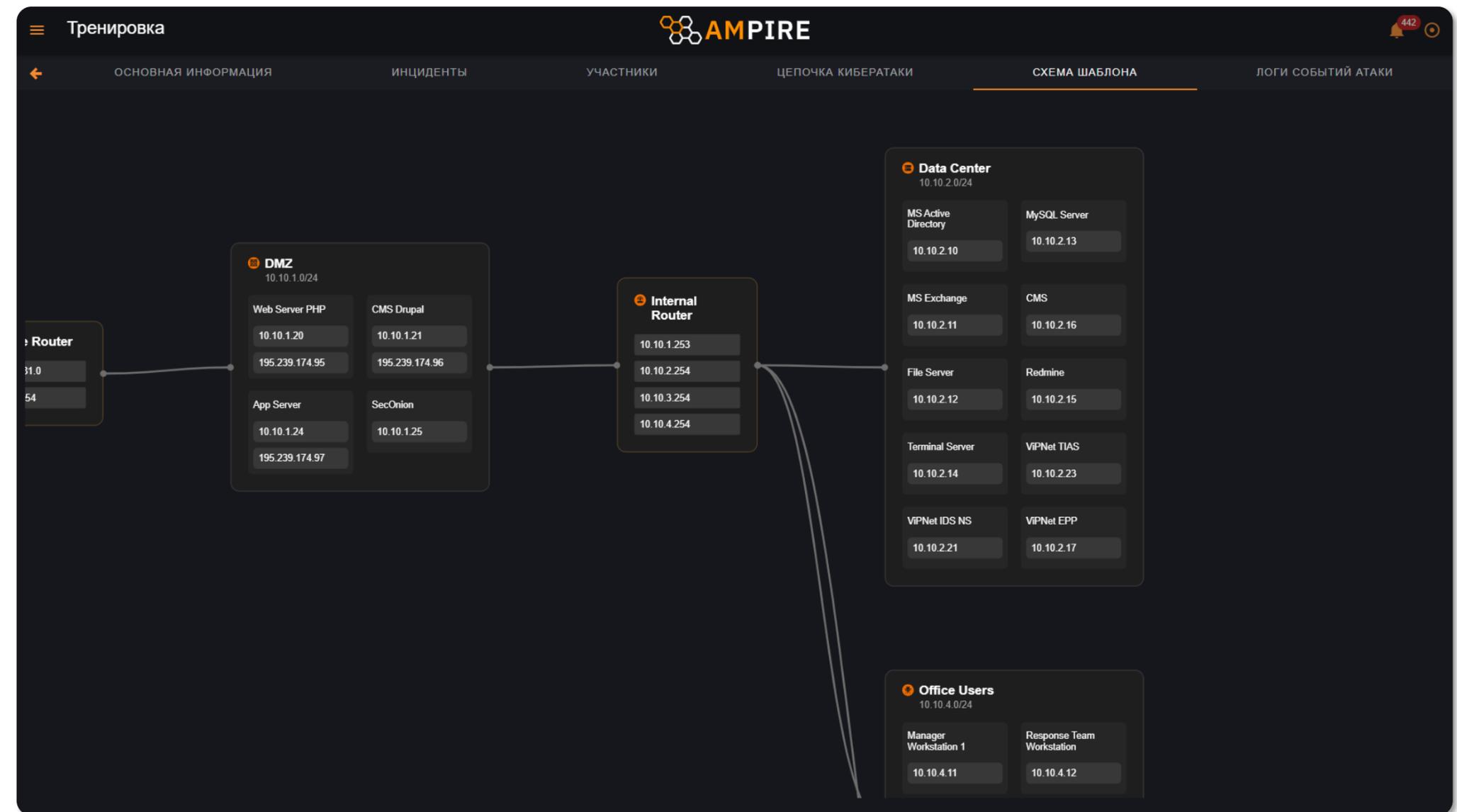
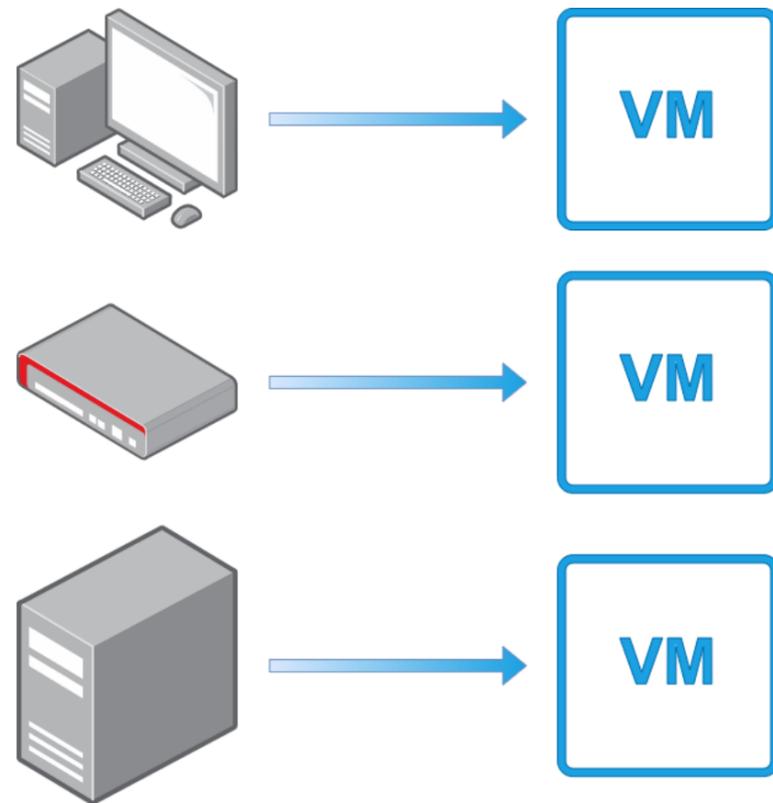
Концепция работы



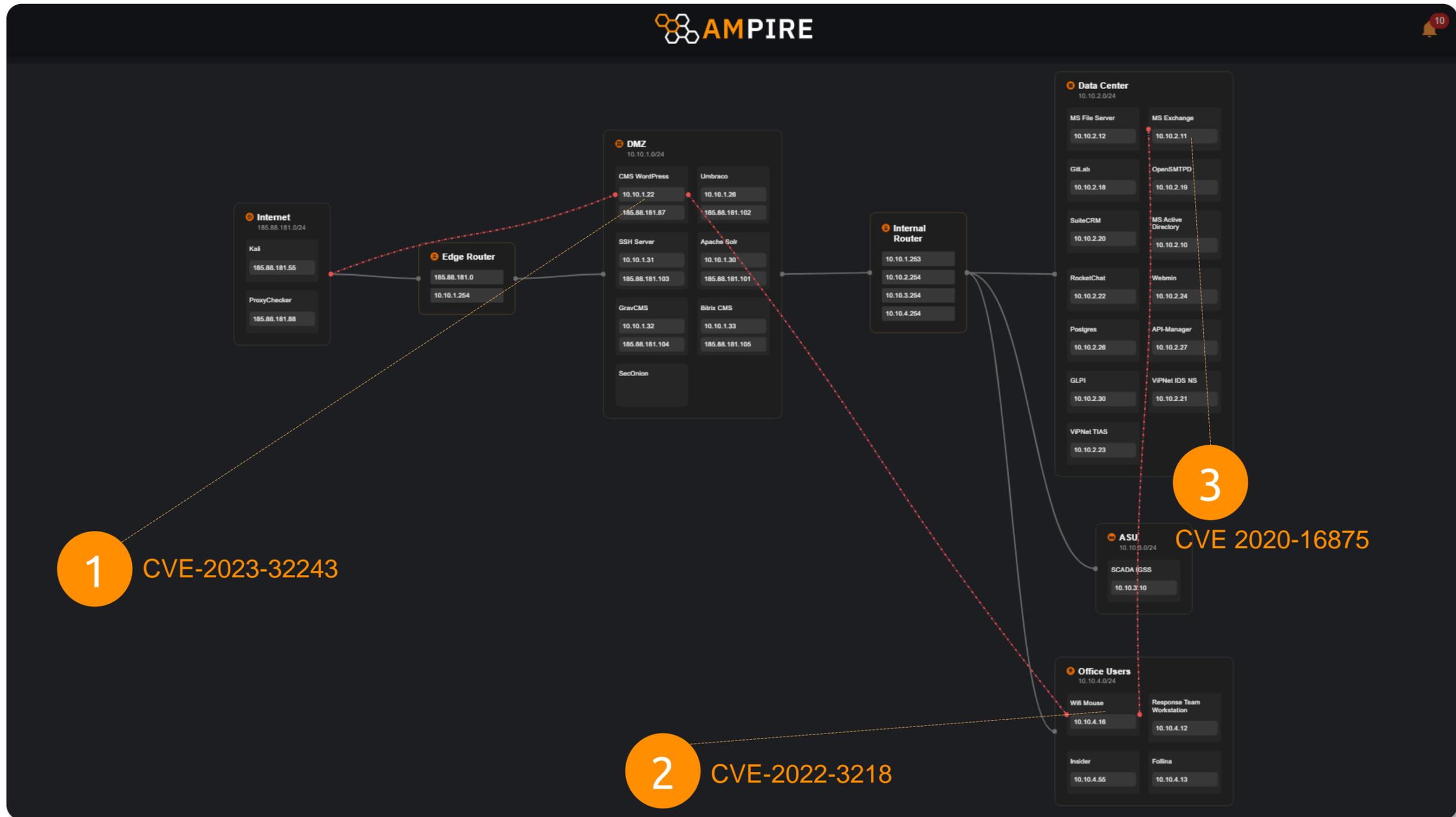
Шаблон



Виртуальная модель сети предприятия



Сценарий



Форматы тренировок



- Blue Team
- Red Team
- OSINT
- CSIRT

The screenshot displays the AMPIRE training interface. At the top, there is a navigation bar with the title 'Тренировка' and the AMPIRE logo. Below the navigation bar, there are tabs for 'ОСНОВНАЯ ИНФОРМАЦИЯ', 'ИНЦИДЕНТЫ', 'УЧАСТНИКИ', 'ЦЕПОЧКА КИБЕРАТАКИ', 'СХЕМА ШАБЛОНА', and 'ЛОГИ СОБЫТИЙ АТАКИ'. The 'УЧАСТНИКИ' tab is currently selected.

The main content area is divided into two columns: 'Команда мониторинга' and 'Команда реагирования'. Each column contains four participant cards, each with a 'Не в сети' status indicator and a list of statistics.

Команда мониторинга	Команда реагирования
Иванова Евгения Не в сети Создано инцидентов: 4 Закрыто инцидентов: 1 Средний балл: 3.25	Сергеев Михаил Не в сети Назначено ответственных: 3 Закрыто инцидентов: 1 Закрыто уязвимостей: 0
Петров Алексей Не в сети Создано инцидентов: 1 Закрыто инцидентов: 0 Средний балл: 4	Сидоров Сергей Не в сети Закрыто инцидентов: 1 Закрыто уязвимостей: 1
Аксенова Елена Не в сети Создано инцидентов: 2 Закрыто инцидентов: 0 Средний балл: 5	Кузнецов Петр Не в сети Закрыто инцидентов: 1 Закрыто уязвимостей: 1
Быстров Федор Не в сети Создано инцидентов: 3 Закрыто инцидентов: 3 Средний балл: 3.33	

Учебно-тренировочная платформа



6

шаблонов

31

сценарий

73

уязвимых
узлов

162

уязвимости и
последствия

- Методические пособия для преподавателя и для обучаемого
- Документация по уязвимым узлам для конфигуратора
- Примеры работы с СЗИ, карточками инцидентов и другими сущностями

Пример применения – технический ВУЗ



- Занятия по Ampire на всех курсах
- 5-6 лабораторных работ в семестр на старших курсах
- До 4-5 занятий в день
- Использование Ampire в курсовых и дипломных проектах
- Использование Ampire в публичных мероприятиях и на олимпиадах
- Отдельная аудитория с сервером и рабочими местами под Ampire



Пример применения – регион

- Амприге размещен на мощностях ЦОД региона
- Доступ для организаций бюджетной сферы
- Регулярные киберучения
- Соответствие законодательству по киберучениям для предприятий КИИ
- Профильное обучение старшеклассников и молодых специалистов



Ampire Junior



- Лабораторные работы с заданиями на теорию и практику
- Виртуальная среда для выполнения практических заданий
- Методические материалы с теорией для преподавателей и обучаемых
- 8 реализованных сценариев:
 - Эффективный поиск в сети
 - Google Hacking
 - Доксинг
 - Кибербуллинг
 - Фейковые новости
 - Основы цифровой гигиены
 - Фишинг
 - Антифишинг

Концепция информационной безопасности детей, утвержденной Председателем Правительства Михаилом Мишустиным в Распоряжении от 28 апреля 2023 года №1105-р

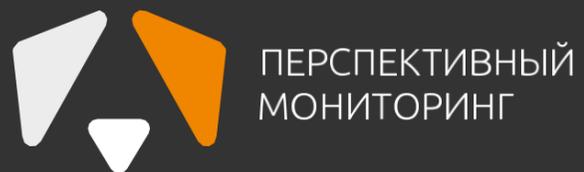
Указ Президента РФ от 17 мая 2023 г. № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года»

Статья 5 ФЗ № 436 «О защите детей от информации, причиняющей вред»

Федеральный закон N 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006

Федеральный закон N 273-ФЗ «Об образовании в Российской Федерации»

Федеральный закон №152-ФЗ «О персональных данных»



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



Спасибо за внимание!



t.me/pm_public



[@AMonitoring](https://www.youtube.com/@AMonitoring)



[ampire.team](https://www.ampire.team)

Сергей Нейгер

Директор по развитию бизнеса

+7 (495) 737-61-97

info@amonitoring.ru