

Amprige 2.0: новый формат, карточки НКЦКИ и требования регулятора



Георгий Мелихов

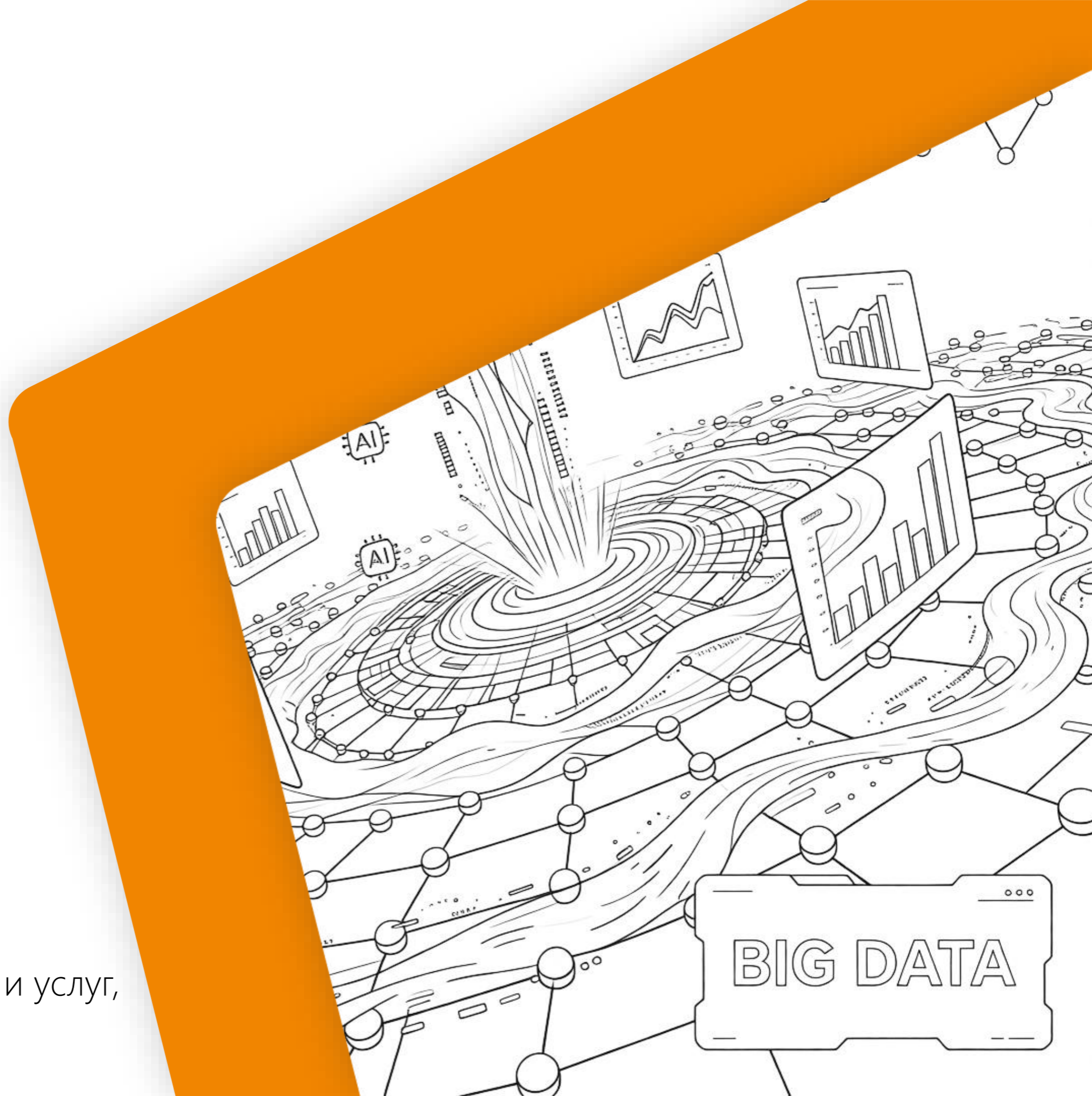
Руководитель направления развития продуктов
и услуг компании «Перспективный мониторинг»

Ampire 2.0:

новый формат,
карточки НКЦКИ
и требования регулятора

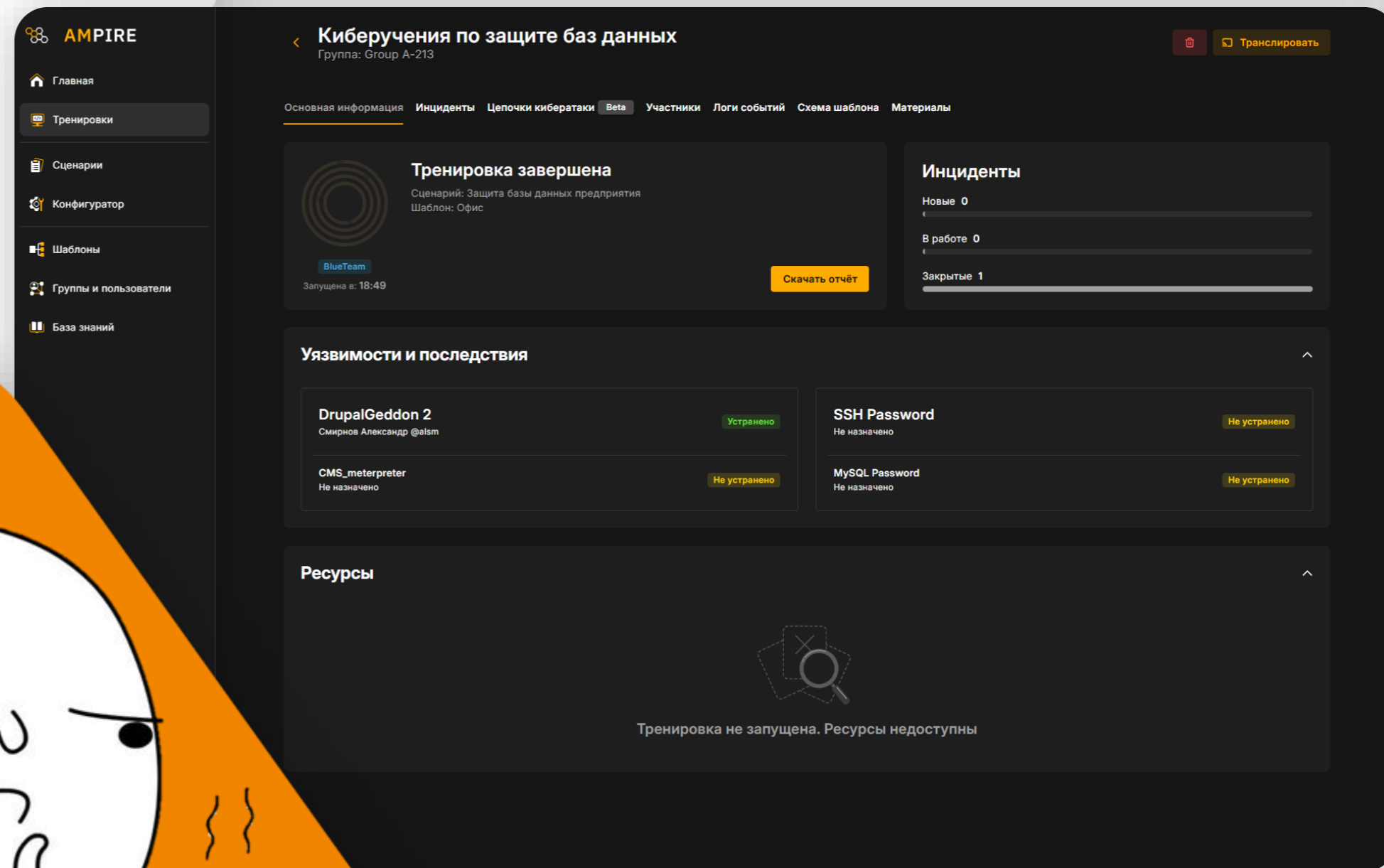
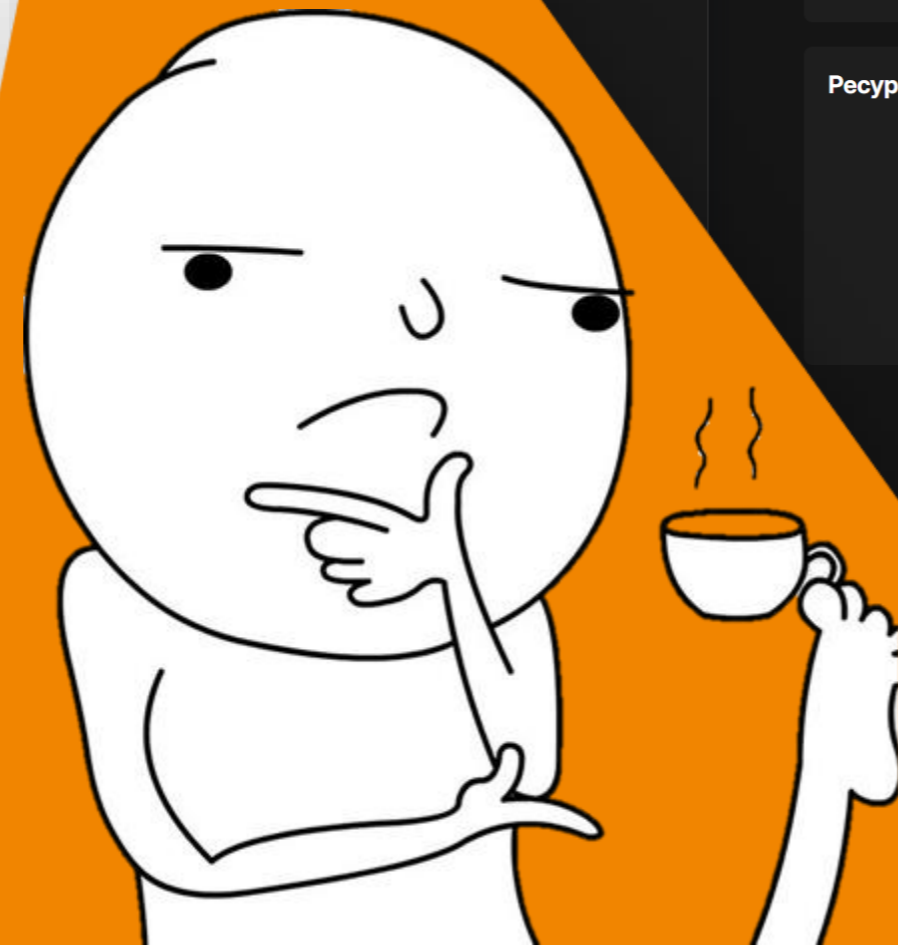
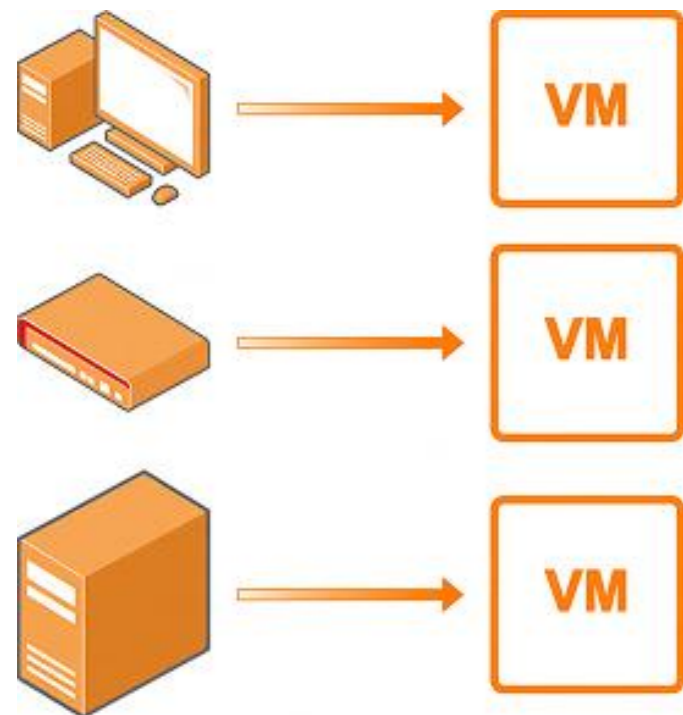
Георгий Мелихов,

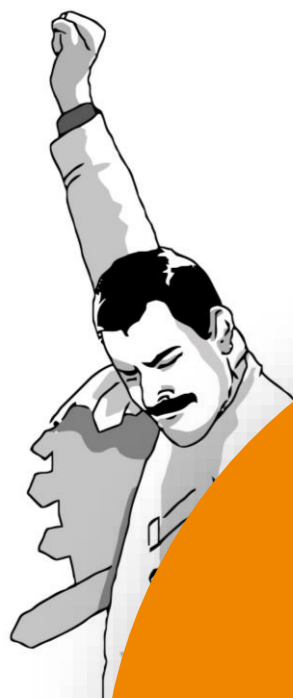
Руководитель направления развития продуктов и услуг,
«Перспективный мониторинг»



Что такое **Ampire**

Учебно-тренировочная платформа для отработки навыков противодействия киберугрозам





40

действующих
киберполигонов

610
проведено
киберучений

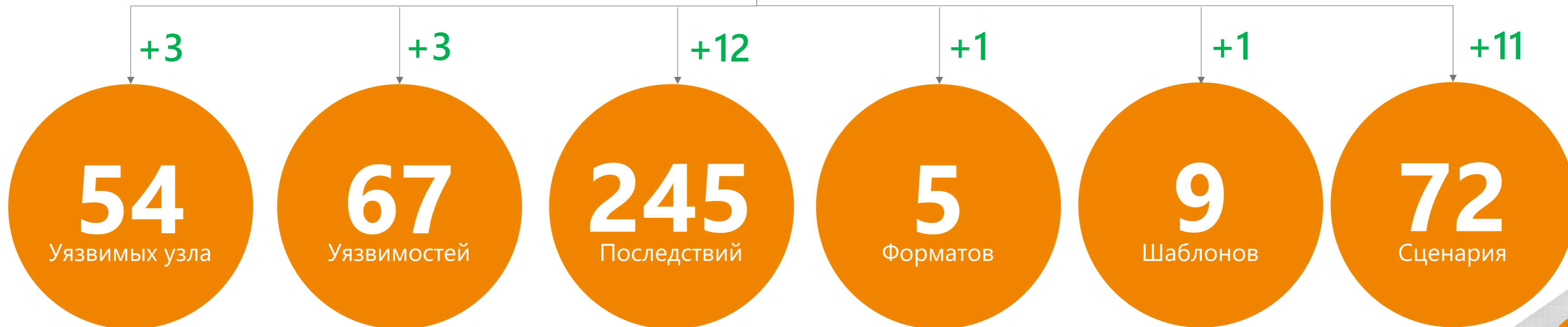
11
брендированных
лабораторий

405
сертифицировано
преподавателей

Ampireметр: доступно из коробки



Вклад Ampire 2.0 в «Ампирметр»



Что новенького в **Ampire 2.0**



Red Team Labs



Карточки инцидентов в формате НКЦКИ



Сценарий фишинга в Red Team, новые уязвимые узлы, улучшение стабильности

Новый формат Red Team Labs



- ▶ Командный формат «Red Team» сложный
- ▶ Не хватает практических навыков
- ▶ Потребность в снижении порога входа
- ▶ Желание тренироваться в индивидуальном темпе



- ▶ Индивидуальный формат «Red Team Labs»
- ▶ Пентест и исследование защищенности
- ▶ Пошаговое прохождение сценария
- ▶ Поиск флага, ответы на теоретические вопросы
- ▶ Полностью автоматическая проверка заданий

Как работает Red Team Labs

2

Участник подключается к индивидуальному экземпляру инфраструктуры для прохождения сценария

4

Участник отправляет задания на проверку – система автоматически их проверяет и ставит балл

8

1

Преподаватель выбирает сценарий и запускает тренировку

3

Участник пошагово проходит задания на поиск флага и на теорию

The screenshot displays the Red Team Labs interface. At the top, it shows the title 'Практика по базовым инструментам' (Basic Tools Practice) for a group 'Группа: Группа А-213'. The session is 'Запущена' (Running) with a timer at '00:56:38'. Below this, there is a 'Задания' (Tasks) section with a list of tasks and their scores. At the bottom, there is a 'Ресурсы' (Resources) section with a table of participants.

Максимальная оценка	Название
3	Выполните комплексное сканирование портов целевого хоста 195.239.174.13 и определите TCP-порт с неизвестной (unknown) службо...
3	Выполните сканирование веб-сервера 195.239.174.13 для обнаружения всех файлов с расширением .ph...
4	Откройте веб-страницу Burpsuite flag. Настройте Burp Suite как прокси, после этого активируйте процесс выполнения задания нажат...
2	Откройте веб-страницу JTR flag. Скачайте и взломайте зашифрованный zip-архив с помощью утилиты John The Ripper. Флаг записан в...
3	Откройте веб-страницу FFuF flag. Используя утилиту FFuF взломайте веб-форму....
5	Получите reverse shell (обратный шелл) с веб-сервером на порту 5757....

Название	Участник	IP Адрес	Логин	Пароль
Удалённое рабочее место	Кузнецов Георгий @geku	10.10.210.50	reduser3	*****
Удалённое рабочее место	Петров Петр @pere	10.10.210.90	reduser3	*****
Удалённое рабочее место	Иванов Иван @iviv	10.10.210.216	reduser3	*****

Что доступно в Red Team Labs



В Red Team Labs для версии Empire 2.0:

- ▶ 2 модуля – «Web» и «AD»
- ▶ 10 сценариев разного уровня сложности
- ▶ Методическое пособие для обучаемого по каждому сценарию
- ▶ Решебник для преподавателя по каждому сценарию
- ▶ Автоматическое создание групповых и индивидуальных отчётов о тренировке

Сценарии применения Red Team Labs



Практическое сопровождение лекций по различным ИБ-дисциплинам, например, «Анализ безопасности Web-приложений», «Тестирование ИС на проникновение» и др.

Проведение зачётов, экзаменов, вступительных испытаний, собеседований и аналогичных мероприятий для разной целевой аудитории

Создание индивидуального графика отработки навыков, обеспечение индивидуального контроля успеваемости

Разработка собственных сценариев с учётом желаемой специфики в рамках курсовых и дипломных работ, грантов и иных дополнительных активностях

Инциденты в форме НКЦКИ



Тренировки Blue Team и CSIRT

Карточки инцидентов в упрощенной форме

Знакомство с процессом оформления инцидентов

Практика базовых навыков передачи данных о компьютерной атаке

Карточки инцидентов в формате НКЦКИ

Отработка навыков передачи данных об инцидентах и компьютерных атаках по требованиям регулятора

Воссоздание ситуаций, требующих взаимодействия с НКЦКИ

Тренировка с карточками НКЦКИ

Как можно практиковаться:

1

Участники детектируют атаку, проводят расследования и по итогам подробно оформляют карточку инцидентов НКЦКИ

Преподаватель рассматривает заведенный инцидент и оценивает корректность заполнения

2

Преподаватель или организатор самостоятельно составляет легенду сценария и определяет сам сценарий

Участники знакомятся с форматом отправки данных об инциденте и заполняют карточку по требованиям преподавателя

Киберучения

Зачет, экзамен

Соревнования

Олимпиады

Мастер-классы

#1 Web Vote rce

Категория Общие сведения Контролируемый ресурс Технические сведения Чат

Общие сведения

Тип события ИБ
Успешная эксплуатация уязвимости

Компания
magic monitoring team

Владелец информационного ресурса
ГБУ МФЦ Города Москвы

Статус реагирования
Меры приняты

Требуется содействие НКЦКИ
Нет

Выявлен
07.04.2026 09:35

Закрыт
08.04.2026 09:35

Средство выявления
VIPNet IDS

TLP
● TLP-Red

Описание
В ходе эксплуатации уязвимой версии модуля голосований на веб-ресурсе МФЦ города Москвы злоумышленник смог проэксплуатировать найденную уязвимость CVE-2022-27228, которая заключается в достаточной валидации пользовательского ввода, что привело к полному контролю над веб-ресурсом и изменению внешнего вида главной страницы.

Влияние на целостность Высокое | **Влияние на доступность** Высокое | **Влияние на конфиденциальность** Высокое

Иные последствия
Произведена загрузка вредоносного файла в следствии чего был изменен внешний вид сайта, установлена meterpreter-сессия и изменен пароль администратора.

Что ещё **НОВОГО**



Фишинг в Red Team

Участники должны организовать фишинговую рассылку на виртуальной инфраструктуре, «убедить» виртуального пользователя скачать вредоносное вложение и установить сессию с пользовательской APM

Уязвимые узлы

Новые уязвимые узлы для конфигуратора, связанные с настройками безопасности ОС и особенностями работы SSL-сертификатов.
Новый уязвимый узел для шаблона «Телеком ОКС-7», который моделирует систему биллинга с уязвимостью, приводящей к удаленному выполнению кода в обход аутентификации

Стабильность

Дополнительный контроль над процессом развертывания тренировки и автоматический учёт готовности всех необходимых для сценария элементов инфраструктуры

Влияние Ampire



Специалисты

Разработчики СЗИ

Школьники

Непрофильные специалисты

Специалисты ИТ

Начинающие специалисты

Разработчики и DevOps

Отраслевые специалисты



▶ Резюме с Ampire за месяц: 120

▶ Резюме с Ampire за год: 288

Ampire де-факто становится стандартом практической подготовки в области ИБ

Спасибо за внимание!

 [@AMonitoring](#) [ampire.team](#) [amonitoring.ru](#)

Георгий Мелихов,

Руководитель направления развития
продуктов и услуг,

«Перспективный мониторинг»

+7 (495) 737-61-97

info@amonitoring.ru

САНКТ
ПЕТЕРБУРГ

инфотекс
ТЕХНОДЕСТ

Подписывайтесь
на наши соцсети



инфотекс
Академия



AMPIRE

TELEOFIS®

КОМФОРТЕЛ
оператор связи бизнес-класса

РУТОКЕН
КОМПАНИЯ ПРАКТИВ

TS Solution

AXOFT®