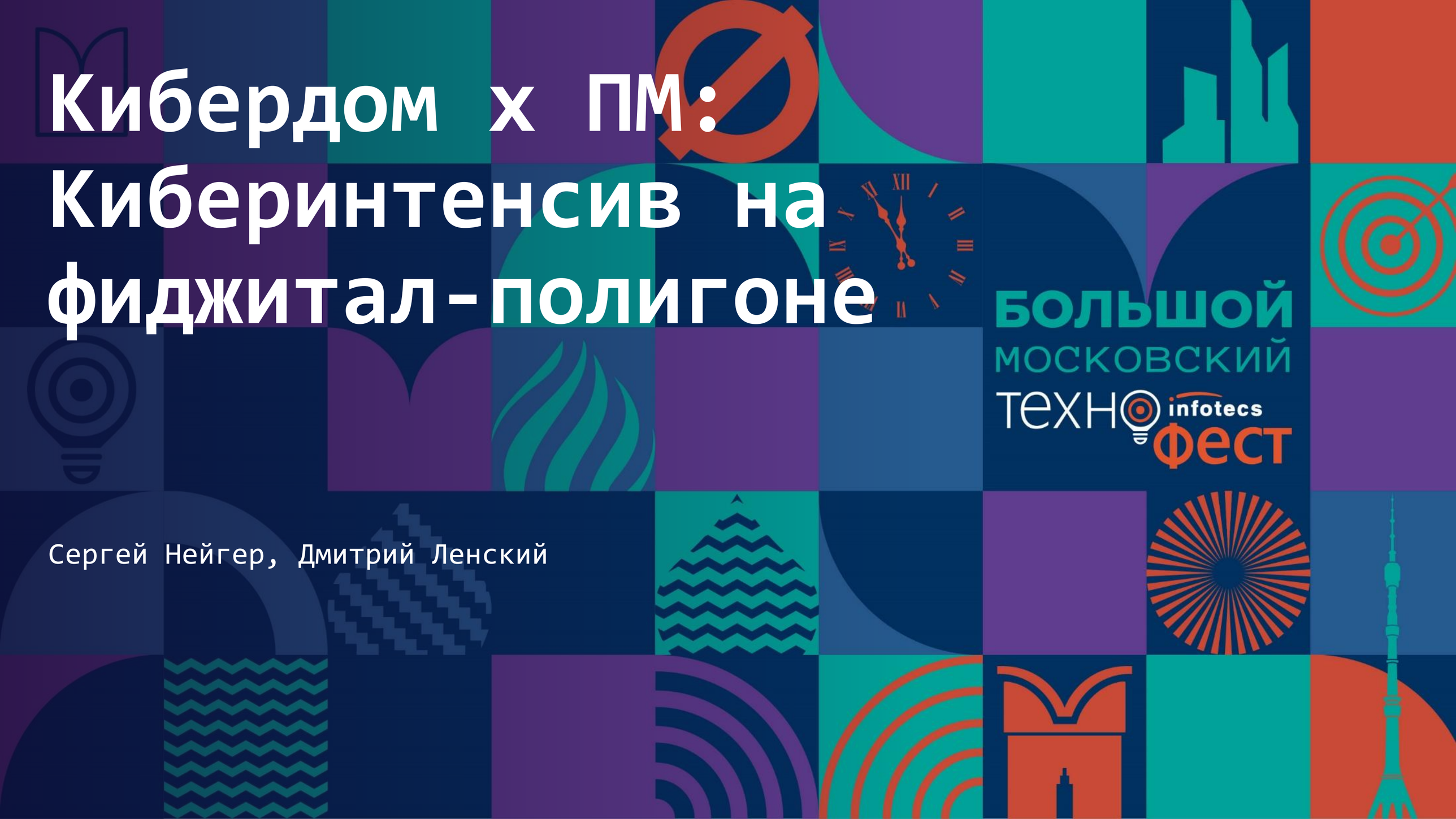
# Кибердом x ПМ: Киберинтенсив на фиджитал-полигоне




Сергей Нейгер, Дмитрий Ленский

кибердом

AMPIRE

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ


Вместе создаем будущее бизнеса

# Киберинтенсив

- 3 дня практических киберучений
- Уникальные сценарии Ampire
- Макет «Городская экосистема»

Расширяем границы киберучений

# Вызовы

Цифровой мир под угрозой хакерских атак: атак становится больше, они чаще целенаправленны, векторы атак становятся всё более изощрёнными

Организации всех отраслей подвергаются регулярным нападениям, причём направлены они не только на прямую выгоду хакера, но и на создание панических настроений у широких слоев населения

В таком цифровом мире ИБ-специалисты должны быть опытнее и подготовленнее своих противников

Так выглядит изнанка цифрового мира

2024 год

- x5 рост числа фишинговых атак
- на 70% увеличилось число DDoS-атак
- на 39% выросло число критичных инцидентов
- За 7 месяцев 2024 года ущерб от ИТ-преступлений составил 99 млрд руб., из них 30% преступлений произошло в сфере кибермошенничества

Источник: Forbes https://www.forbes.ru/tekhnologii/527262-poka-vzlom-ne-granet-kakim-dla-rynka-kiberbeza-byl-2024-god-i-kakim-budet-2025-j

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# Киберинтенсив

3 дня практических тренировок для специалистов

Штабные учения для руководителей

Тренинги для топ-менеджмента

- Киберучения проходят на единственном в России учебно-тренировочном фиджитал-полигоне Кибердома и предоставляют новый уникальный опыт тренировок с глубоким погружением в реальность
- Киберинтенсив разработан экспертами «Перспективного мониторинга» и позволяет повысить готовность ИБ-специалистов к компьютерным атакам
- Сценарии атак смоделированы на платформе Ampire и основаны на актуальных практических кейсах и опыте специалистов SOC и пентестеров «Перспективного мониторинга»

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# Киберинтенсив

### Тренировка на уникальных физических макетах
Макет «Городская экосистема» позволяет отрабатывать атаки на коммунальные, муниципальные, специализированные объекты

### Актуальные сценарии кибератак
Все сценарии разработаны на основе реальных кейсов и постоянно актуализируются в соответствии с новыми тактиками злоумышленников

### Визуализация атаки и устранения последствий
В процессе хакерской атаки участники видят все последствия как внутри киберполигона, так и на физическом макете. При устранении уязвимостей и последствий происходит восстановление штатной работоспособности систем

### Актуальный ИТ-ландшафт
Участники работают на шаблоне типовой современной ИТ-инфраструктуры со встроенными актуальными средствами защиты информации (СЗИ) ведущих производителей

### Ведущие преподаватели
Курс проводят опытные преподаватели «Перспективного мониторинга», которые провели более 500 киберучений и обучили более 5000 специалистов

### А также:
- Треки для руководителей и специалистов
- Методические материалы
- Соответствие рекомендациям регуляторов

# Практические тренировки для специалистов

## Задачи

- Отработаете навыки реагирования на инциденты в критической ситуации
- Отработаете процесс взаимодействия внутри и между командами других департаментов
- Автоматизируете действия реагирования на инцидент по заданному процессу
- Изучите мышление, тактики, техники и инструменты злоумышленников

## Навыки

- Обнаружение атак внутренних и внешних нарушителей
- Устранение уязвимостей информационных систем
- Ликвидация последствий кибератак и восстановление штатной работы систем
- Построение Cyber Kill Chain и устранение возможности атаки по отработанному вектору

## Форматы

Командно-штабные учения в форматах

- Blue Team
- CSIRT

# Штабные учения для руководителей

## Задачи

- Изучите как используемые технологии и процессы влияют на безопасность
- Увидите как сотрудники отрабатывают инциденты и работают в критической ситуации
- Усилите командную работу и отработку взаимодействия между подразделениями, участвующими в процессе реагирования на инциденты

## Навыки

- Обнаружение атак внутренних и внешних нарушителей
- Отработка процесса взаимодействия при ликвидации последствий кибератак внутри и между департаментами, включая коммуникационную стратегию
- Отработка базовых навыков по анализу и расследованию инцидентов
- Отработка моделей киберугроз, техник и методов злоумышленников

## Форматы

Штабные учения

- Киберквест
- CSIRT
- OSINT

# Тренинги для топ-менеджмента

## Задачи

- Погружение топ-менеджмента в задачи информационной безопасности
- Освоение расширенных навыков кибербезопасности для руководителей
- Культура кибербезопасности и обратная связь для каждого участника команды

## Навыки

- Противодействие различным техникам и тактикам злоумышленников, направленных на руководителей организаций
- Анализ рисков кибербезопасности, оценка потерь и последствий для принятия управленческих решений
- Практические навыки кибергигиены, внедрения кибергигиены на всех уровнях организации
- Оценка зрелости ИБ в организации, соблюдение норм ИБ сотрудниками и руководством, изучение инструментов улучшения ИБ

## Форматы

Тренинги и мастер-классы

- Киберквест
- OSINT

# Форматы практических тренировок

## Blue Team

Классический формат киберучений, где участники отрабатывают навыки защиты от виртуального нарушителя. Отработка инцидентов 1 и 2 линий SOC, а также взаимодействия между ИБ и ИТ службами

Участвуют 2 группы: Группа мониторинга и Группа реагирования

Задачи группы мониторинга:

- обнаружить и проанализировать инцидент
- корректно заполнить карточку инцидента
- сформировать рекомендации по устранению для команды реагирования

Задачи группы реагирования:

- ознакомиться с карточкой инцидента
  обнаружить уязвимости
  закрыть уязвимости
  устранить последствия
  построить Cyber Kill Chain

Рекомендуемое число участников:
4-10 человек

## CSIRT

Формат киберучений, в котором группы мониторинга и реагирования объединены в одну. У каждого участника есть доступ к СЗИ и инфраструктуре

Задача участников:

- обнаружить и проанализировать инцидент
- обнаружить уязвимости
  закрыть уязвимости
- устранить последствия
- построить Cyber Kill Chain

Рекомендуемое число участников:
4-12 человек

## Киберквест

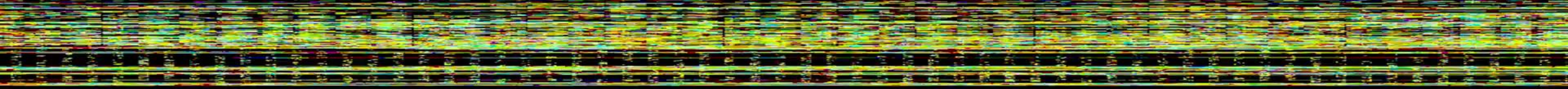
Лекционный формат киберучений, в котором отрабатывается процесс расследования инцидента компьютерной безопасности

Задача участников:

- обнаружить и проанализировать инцидент
- обнаружить уязвимости
- закрыть уязвимости
- устранить последствия
- построить Cyber Kill Chain

Рекомендуемое число участников:
До 20 человек

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ



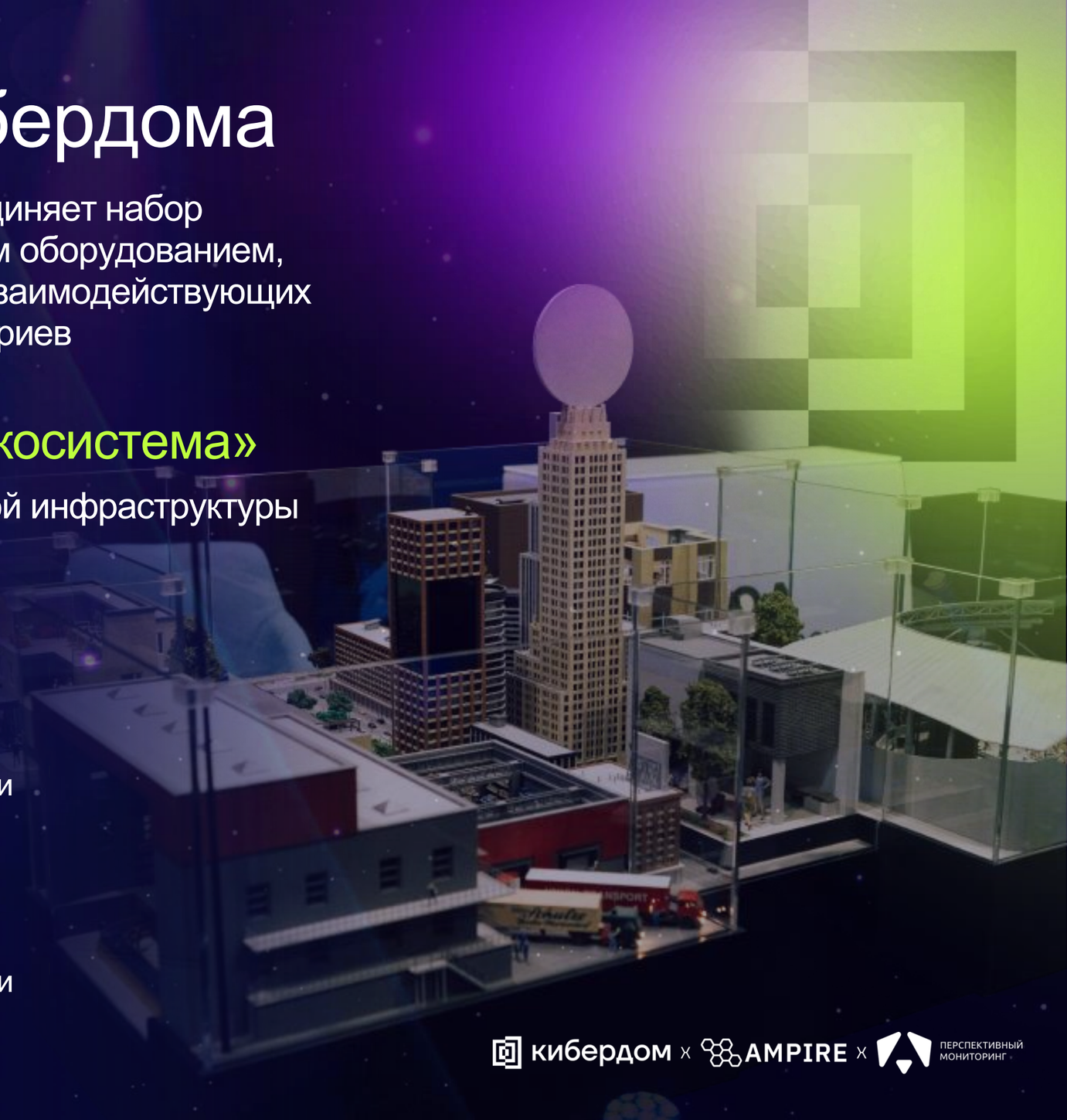
# Фиджитал-полигон Кибердома

Иммерсивное пространство киберполигона объединяет набор областей с мультимедийным, световым, звуковым оборудованием, виброполом и интерактивными инсталляциями, взаимодействующих с посетителем и между собой посредством сценариев

## Иммерсивный макет «Городская экосистема»

Физический макет с подробной моделью городской инфраструктуры

- Деловой центр с небоскребами и офисными зданиями, оборудованными современными LED медиа фасадами
- Здание МФЦ, осуществляющего обслуживание населения
- Стадион для проведения массовых спортивных и развлекательных мероприятий
- Даркстор – крупный логистический центр, обеспечивающий товарами ключевые сферы региона
- Современные жилые дома, оснащенные IoT и управляемые системами класса «Умный дом»



кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# «Городская экоситема» в ваших цветах

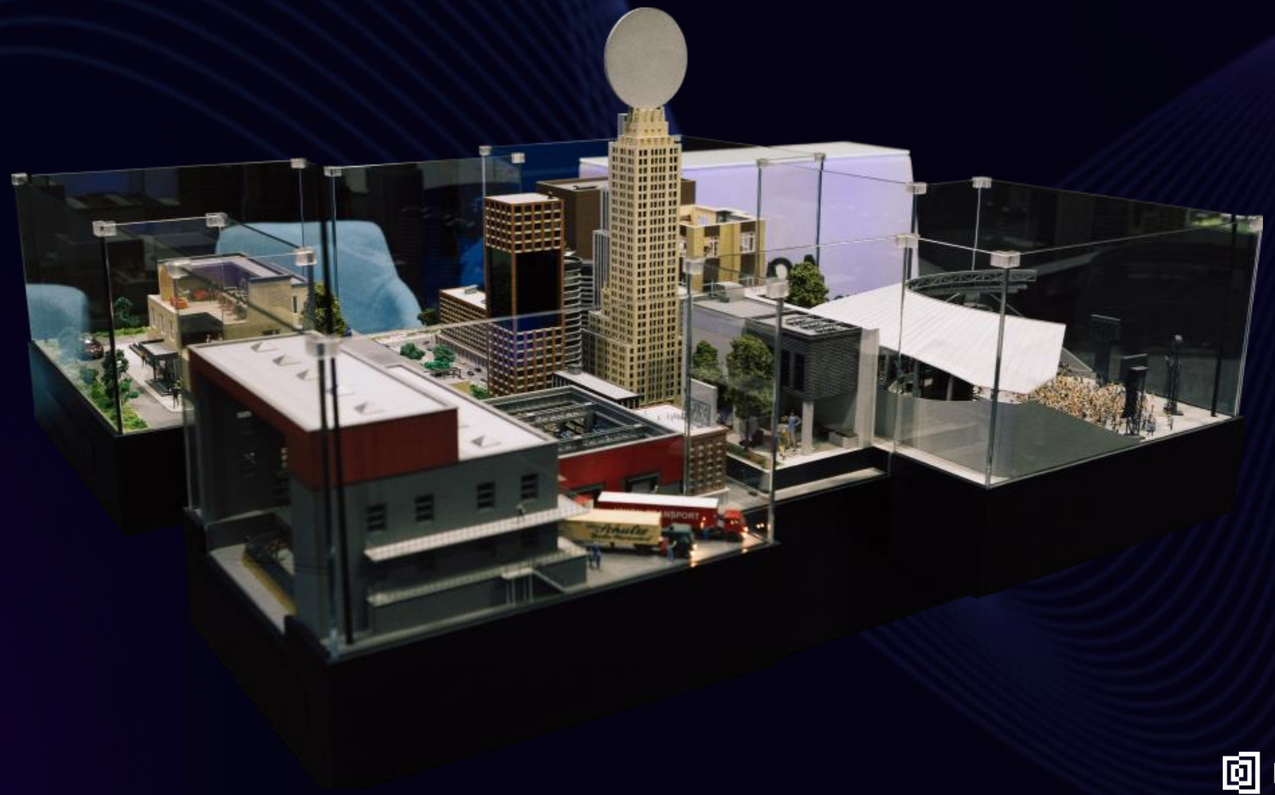
Тренировка на брендированном макете усиливает эмоциональную вовлеченность участников

### Брендирование здания МФЦ

Брендирование вывески,
Брендирование видео-роликов
на экранах внутри здания

### Брендирование зданий Делового центра

Размещение логотипа на шпиле небоскрёба,
Брендирование рекламных видео-экранов на
фасадах зданий



### Размещение логотипа на здании Жилого комплекса

### Брендирование «Даркстор»

Размещение логотипа на крыше
логистического центра,
Брендирование грузовиков,
Брендированный робот-доставщик

### Брендирование стадиона

Размещение объемного логотипа
на крыше стадиона,
Брендирование рекламного ролика
на главном экране стадиона,
Брендирование медиа-стоек

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# Кастомизируйте программу под себя

- Предварительные онлайн-тренировки для лучшего ознакомления с платформой Ampire
- Дополнительные мастер-классы от «Перспективного мониторинга» и Кибердома
- Лабораторные работы OSINT
- Тренинги для топ-менеджеров по кибербезопасности
- Брендирование макета вашими логотипами
- Фото-, видео- сопровождение

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# Как мы взаимодействуем

## до

- Проводим встречу, изучаем ваши потребности
- Выбираем формат, составляем сценарии тренировок, согласуем с вами ТЗ
- Направляем вам необходимые методические материалы, список тактик и инструментов, которые рекомендуем изучить перед Киберинтенсивом

## после

- Составляем отчет по итогам 3-х дней тренировок
- Формируем перечень рекомендаций для сотрудников
- Выдаем именные сертификаты о прохождении киберучений

# Ожидаемый результат Киберинтенсива

**Внимательность к деталям**
Мониторинг угроз информационной безопасности, анализ сетевого трафика, обнаружение угроз, формирование рекомендаций по устранению

**Освоение новых инструментов**
Использование специализированных инструментов и ПО для выявления подозрительной активности

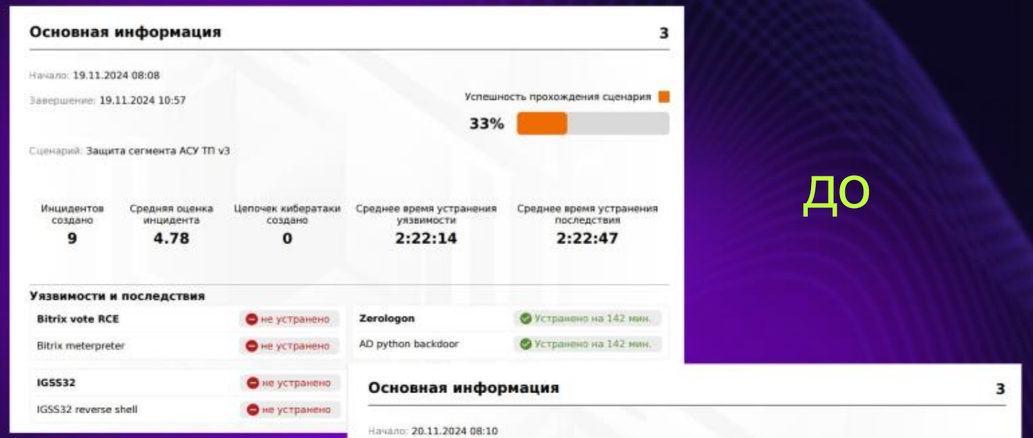
**Ускорение реакции на инциденты**
Реагирование на инциденты и устранение последствий атак: проведение расследований, восстановление данных и минимизация ущерба

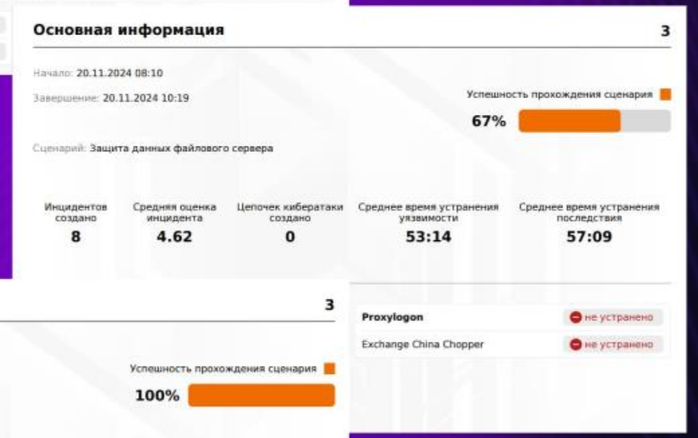
**Креативное мышление**
Навык нестандартно мыслить и искать оригинальные решения для защиты ресурсов и принятия компенсационных мер

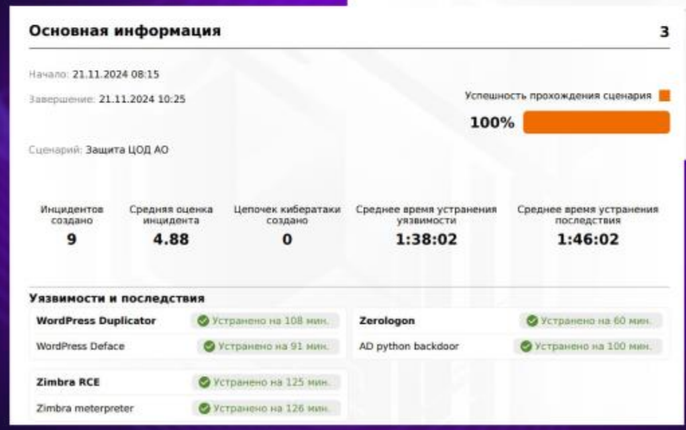
**Коммуникативные навыки**
Отработка алгоритмов коллективного взаимодействия

**Культура кибербезопасности**
Обучение сотрудников безопасному поведению в сети

до




после

кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

cyberdom.pro/cyberintensive


## Сергей Нейгер

директор по развитию бизнеса
«Перспективный мониторинг»

## Дмитрий Ленский

программный директор
Кибердом


кибердом x AMPIRE x ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС