



Kaspersky Industrial  
Cybersecurity  
Conference 2023

# Пять правил для построения киберполигона

Андрей Кузнецов  
Технический директор киберполигона  
Группа компаний «Солар»



kaspersky



# Ключевое в обеспечении кибербезопасности

**Насыщение  
технологиями** –  
приобретение SIEM  
и других средств  
защиты  
информации

2000–2010

**Выстраивание  
процессов** –  
построение  
собственных SOC  
или выбор  
надежного  
поставщика услуг

2010–2020

**Практические  
навыки** –  
умение отражать  
атаки и  
ликвидировать  
их последствия

2020–...

Киберполигоны

Платформы для разработки, доставки и использования интерактивных сред моделирования. Среда моделирования – это представление ИКТ, ОТ, мобильных и физических систем, приложений и инфраструктур организации, включая моделирование атак, пользователей и их действий, а также любых интернет-сервисов, общедоступных или сторонних сервисов, от которых может зависеть смоделированная среда. Киберпространство включает в себя комбинацию основных технологий для реализации и использования среды моделирования и дополнительных компонентов, которые, в свою очередь, желательны или необходимы для достижения конкретных вариантов использования киберпространства.

Объяснение сложное...

Виртуальная и физическая инфраструктура  
для практической тренировки специалистов  
и апробации технологических решений для  
промышленных, коммерческих и  
государственных организаций

Объяснение простое...

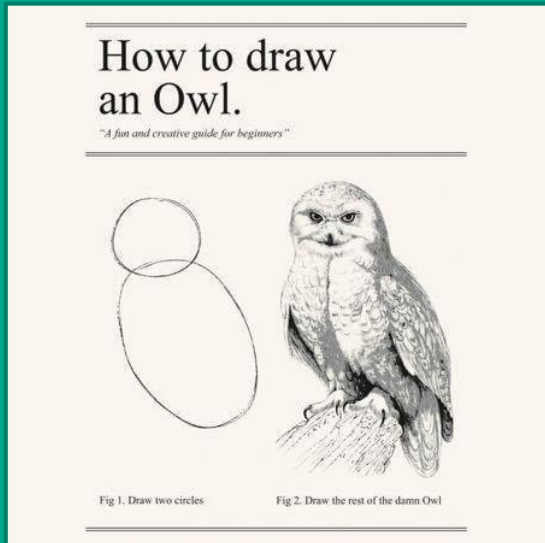
# Киберполигоны в мире



Киберполигоны для  
обучения и тренировки  
специалистов

Исследование физических  
последствий информационных  
воздействий

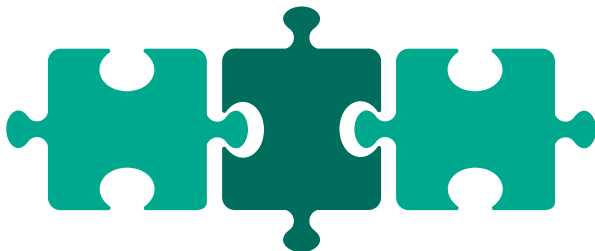
Исследовательские  
лаборатории



1. Проектирование полигона
2. Строительство полигона
3. Profit!

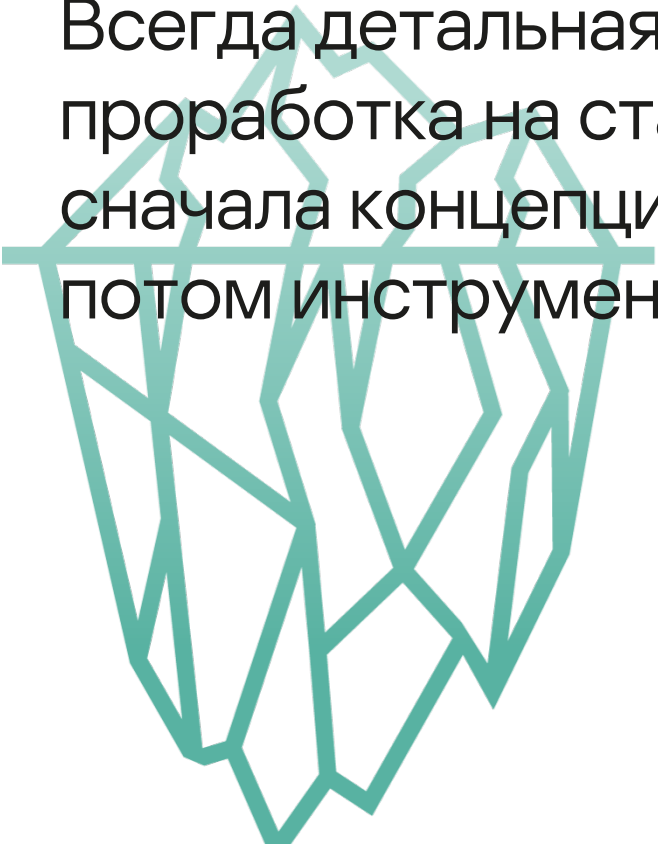
**Пять правил, которые помогут построить киберполигон и не допустить самых распространенных ошибок**

# Заранее определиться со сценариями использования киберполигона



- Площадка для обучения и киберучений: устранение дефицита ИБ-кадров, нехватки актуальных знаний, неумения работать сообща в стрессовой ситуации
- Апробация и развитие технологий: оценка производительности сети и приложений, разработка, проверка и оценка решений для обеспечения безопасности
- Оптимизация расходов: снижение ущерба от киберинцидентов и уменьшение рисков остановки бизнес-процессов
- Повышение эффективности бизнес-процессов: повышение прозрачности управления за счет наглядности цифровых двойников, обкатка регламентов и процессов

И многое другое...



Всегда детальная  
проработка на старте:  
сначала концепция,  
потом инструменты

В процессе разработки концепции необходимо ответить на следующие вопросы:

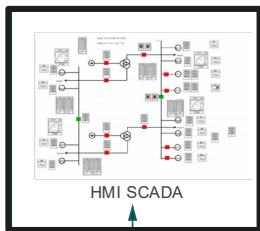
- 1 Для каких целей будет использоваться киберполигон?
- 2 Кто основные пользователи киберполигона?
- 3 Как часто будет использоваться киберполигон?
- 4 Какие технологические и бизнес-сегменты должен включать киберполигон?
- 5 Каким образом будет осуществляться доступ к киберполигону?

# Требования к экспертизе исполнителей: наличие внутренней или внешней экспертизы



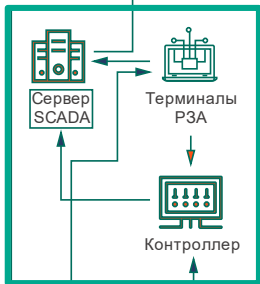
- ✓ Наличие экспертизы построения киберполигона и технологий, применяемых при их создании
- ✓ Наличие профильной экспертизы в промышленных системах автоматизации и бизнес-системах
- ✓ Необходимость понимания, кто будет заниматься обслуживанием и наполнением киберполигона контентом

Модели информационных систем, АСУ, сетей связи



Определитесь, есть ли необходимость в детальном моделировании технологических процессов

Модели интеллектуальных устройств и оборудования промышленной автоматизации



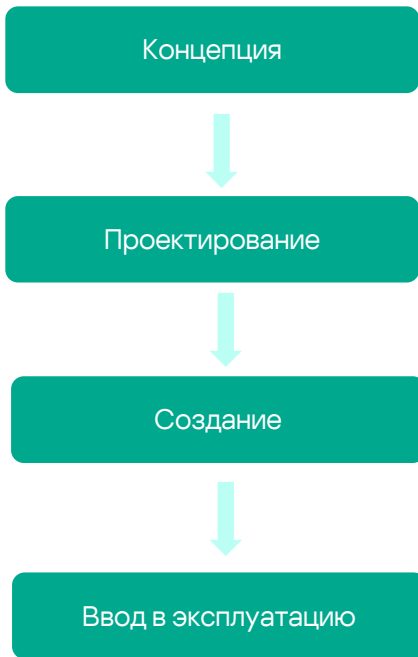
Возможно, что для решения поставленных задач достаточно использование упрощенных моделей

Моделируемый технологический процесс



Создание новых моделей – это всегда дорого. Возможно, в компании уже есть готовые модели

Создание  
собственного  
киберполигона  
требует времени



Создание киберполигона  
занимает от одного года  
до трех лет

Создание киберполигона  
требует больших человеческих  
и материальных ресурсов

Можно использовать готовые  
решения и платформы или  
использовать услуги в формате  
SaaS

# Обсудим?



Андрей Кузнецов

Технический директор  
киберполигона  
Группа компаний «Солар»

[a.kuznetsov@rt-solar.ru](mailto:a.kuznetsov@rt-solar.ru)  
+7 (926) 666-71-78

**kaspersky**