



POSITIVE  
TECHNOLOGIES

# Как хакеры взламывают промышленные системы

Михаил Левин

Заместитель директора  
Positive Technologies Expert Security Center

[ptsecurity.com](https://ptsecurity.com)

# Не про Stuxnet/Triton/etc

PT

Вы не увидите здесь:

- Хитрых векторов
- Узконаправленного инструментария
- Катастроф планетарного масштаба

Посмотрим на **массового хакера**  
и узнаем с чем его едят



# Посмотрим на примере ежегодных киберучений **The Standoff**



# Standoff@PHDays

Игровой состязательный формат



# Standoff@PHDays

Реальная инфраструктура  
на реальном оборудовании



PHDays  
Positive Hack Days

BREAKING THE CONSTANT

# Standoff@PHDays

PH

Повышенная плотность

атак (1 год за 2 дня)

**PH**  
Positive  
Hack  
Days  
**BREAKING**  
THE  
CONSTANT

## Что происходило?

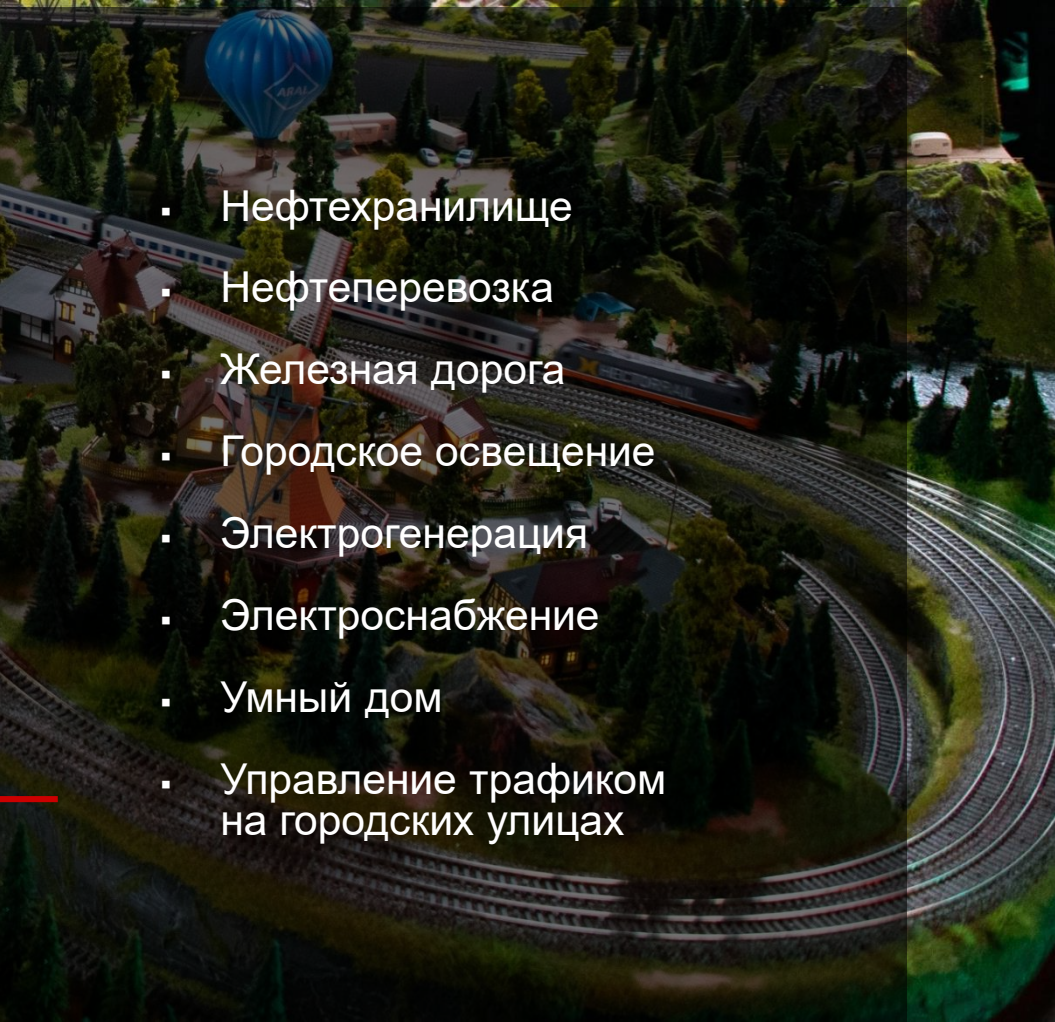
**18** Команд  
хакеров

со всего света -  
огромное разнообразие  
опыта, техник,  
инструментов

**28**  
Часов

непрерывно ломали  
различные  
технологические  
процессы:

---

- 
- Нефтехранилище
  - Нефтеперевозка
  - Железная дорога
  - Городское освещение
  - Электрогенерация
  - Электроснабжение
  - Умный дом
  - Управление трафиком на городских улицах

# Кейс с погрузкой нефти

PT

01.

Хакер нашёл  
интересный  
хост

02.

Проэксплуатировал  
MS17-010

03.

mimikatz

04.

Открыл консоль SCADA

05.

Нарушил тех.  
процесс



# Античеклист

PT

## Как помешать хакеру заполнить его чек лист

- Проверь свой сетевой периметр прежде, чем это сделает хакер. Это просто!
- —Патчинг Харденинг
- Начните жить в парадигме «меня уже взломали»
- Получите опыт Противостояния



# Приходите и убедитесь

PT

## Standoff@PHDays

Май 2020 | PHDays

Проверь своё оборудование  
у нас

(с вас только желание, всё остальное  
мы сделаем сами)





**Спасибо**

**за внимание!**

[ptsecurity.com](http://ptsecurity.com)