

1996

DEFCON

Первые киберучения, которые проводились в формате соревнований, с жюри, присуждающим игровые очки. Позднее подсчет очков был автоматизирован.



2001

Cyber Defense Exercise

Первые соревнования по компьютерной безопасности для учащихся военных академий США.



UCSB iCTF

Местные учения по кибербезопасности на базе Калифорнийского университета в Санта-Барбаре.



2004

UCSB iCTF

В 2004 году iCTF стали международными, участие приняли команды из США, Австрии, Германии, Италии и Норвегии.



Эволюция соревнований и учений

в области компьютерной безопасности

Примеры наиболее выдающихся соревнований

2006

UralCTF

Первые CTF-соревнования в России. Участие приняли две команды.



2008

RuCTF

Первые открытые межвузовские соревнования в России, в которых приняли участие девять команд.



Codegate

Первый CTF в Азии. Проводится по сей день, в 2020 году в отборочных соревнованиях участвовали 324 команды.



2010

RuCTFE

Первые международные CTF-соревнования, организованные в России и проводившиеся онлайн. Участвовали 56 команд.

Locked Shields

Первые международные соревнования, в которых столкнулись команды защитников (blue teams) и атакующих (red teams). Киберполигон, на котором ежегодно проводятся Locked Shields, оборудован Центром кибербезопасности НАТО в Таллине. На его базе развивается обширная тренировочная сеть, в составе которой около 5 тыс. виртуальных

машин, разнообразных клиентов, серверов и сетевых компонентов. В частности, для Locked Shields 2019 была реализована система управления условной водонапорной станцией, а также реальная сеть мобильной телефонии со своим провайдером. Во время учений эти виртуальные и реальные системы стали целями атакующей команды.

2011

PHDays CTF

Первые соревнования, прошедшие в рамках конференции Positive Hack Days. Ключевое отличие от аналогичных соревнований — условия, максимально близкие к реальным. Все уязвимости не выдуманы, а действительно встречаются в современных информационных системах. Формат соревнований необычайно широк благодаря насыщению игровой среды уникальными элементами (захват и удержание систем по принципу «царь горы», возможность решать игровые задачи вслепую, например атаковать системы, не обладая доступом к ним).

С годами на полигоне PHDays CTF появились элементы инфраструктуры умного города — электроподстанция, ракетные установки, железная дорога, оператор сотовой связи, новостное агентство, банковская система.

2012

Hack.lu

PlaidCTF

HITB CTF

Nuit du Hack

C3 CTF

InCTF

Разные страны стремятся проводить свои CTF-соревнования. Большинство из них проходят в формате jeopardy (или task-based), где участники решают отдельные задачи. Но есть и соревнования формата attack — defense (например, Nuit du Hack), в которых каждой команде выделяется сервер или небольшая сеть для поддержания их защиты. Во время игры команды получают очки за корректную работу сервисов своего сервера и за информацию, украденную с серверов соперников («флаги»).

2016

The Standoff

PHDays CTF сменил формат: командам нападающих противостоят защитники. Соревнования впервые проходят на макете города с реальной инфраструктурой, выполняющей реальные бизнес-задачи. За игрой следит SOC.

Сегодня

Более 180 CTF-соревнований проводятся по всему миру. Большинство из них проходят онлайн и посвящены выполнению отдельных заданий. Примерно 6% соревнований проходят в рамках конференций по компьютерной безопасности и требуют личного присутствия участников.

The Standoff

Единственная в мире среда, позволяющая моделировать сценарии развития инфраструктуры современного мегаполиса в условиях взаимодействия различных технологий и влияния хакеров на этот процесс. В последних соревнованиях приняли участие 29 команд атакующих, шесть команд защитников и три мониторинговых центра.

