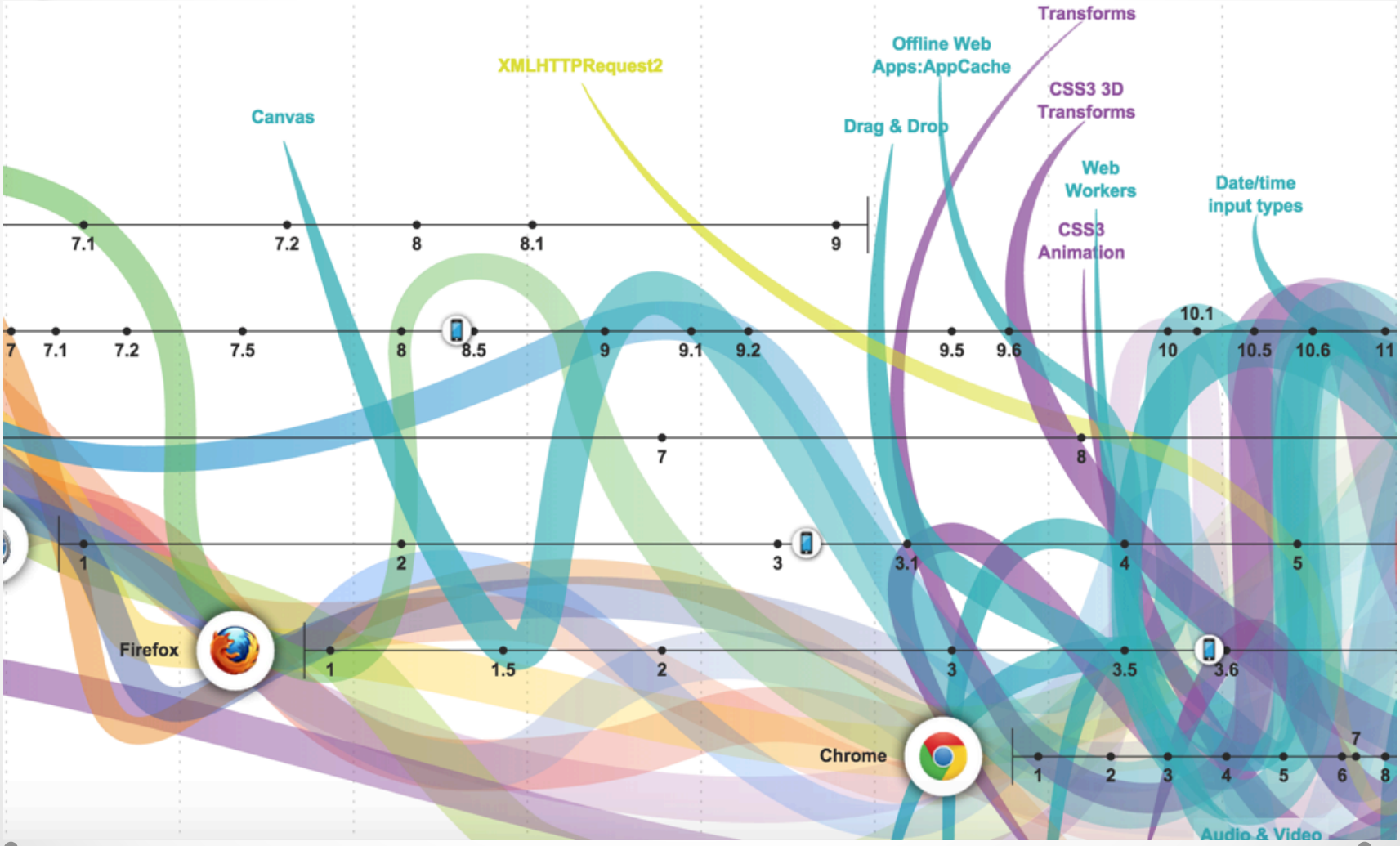
CTF-движение как новый формат обучения информационным технологиям

Денис Гамаюнов
зав. лабораторией интеллектуальных систем кибербезопасности,
ВМК МГУ имени М. В. Ломоносова

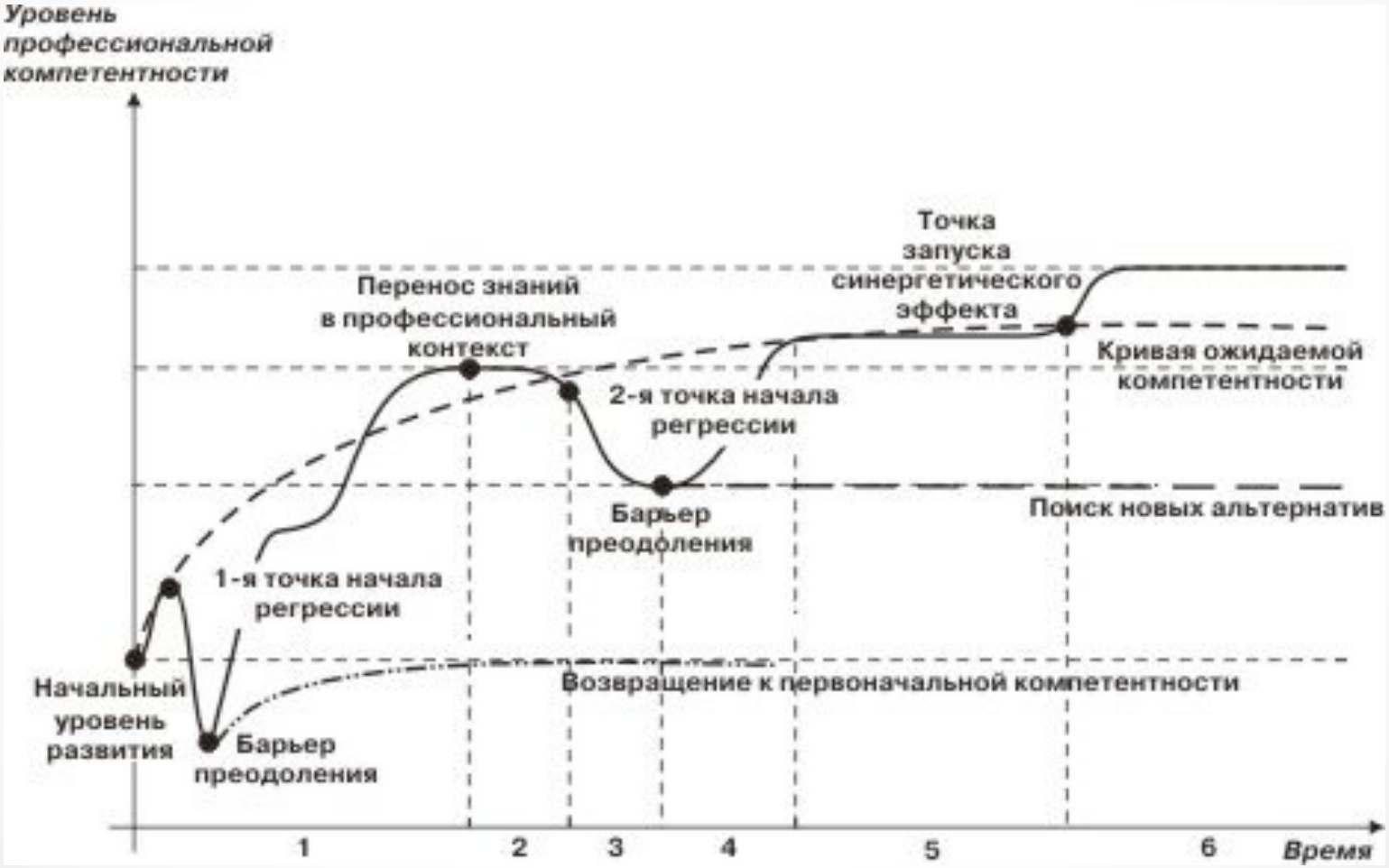
Взрывной рост и усложнение технологий



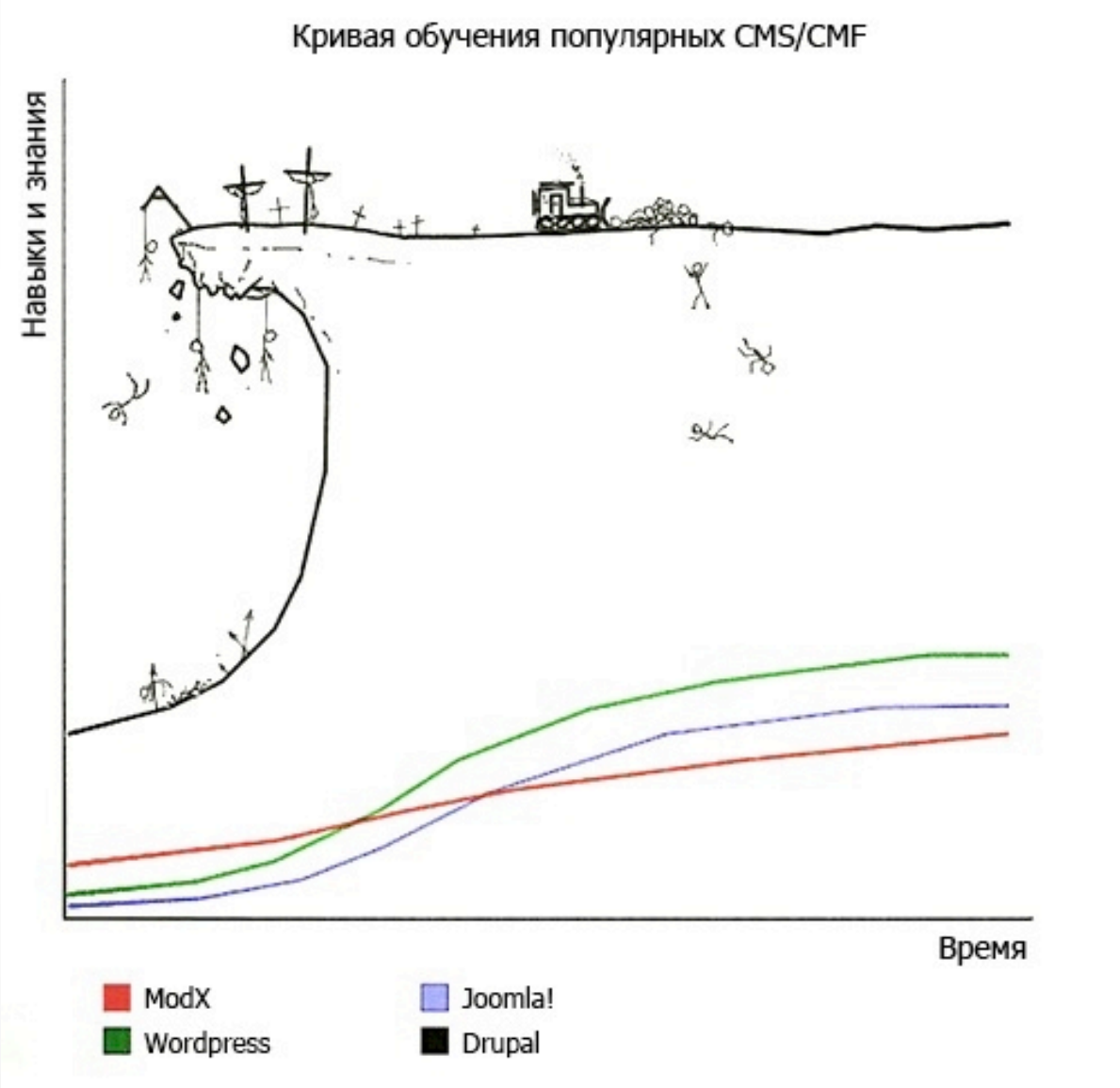
Повсеместное проникновение

Проблема обучения: теория

Еще немного теории

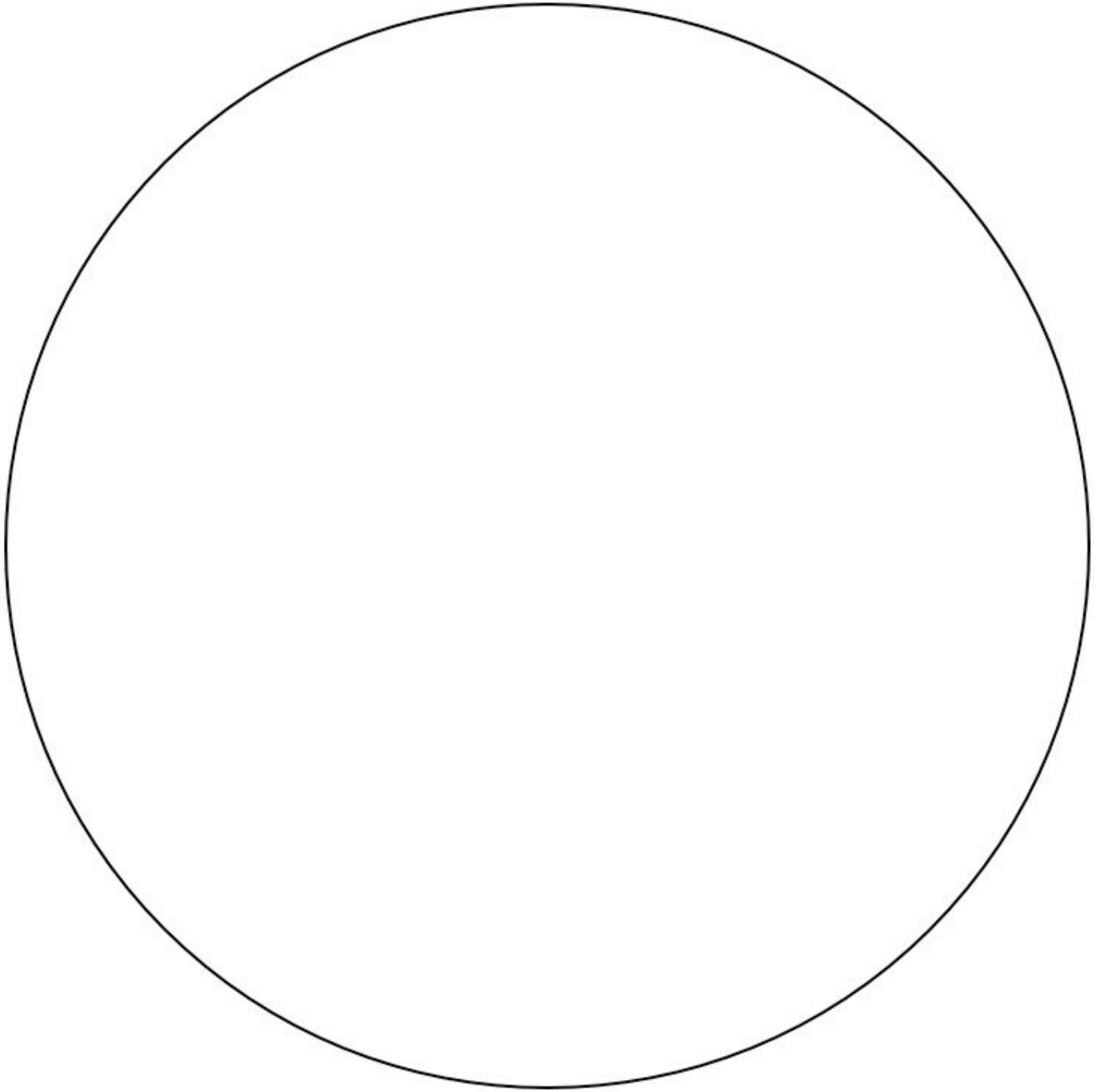


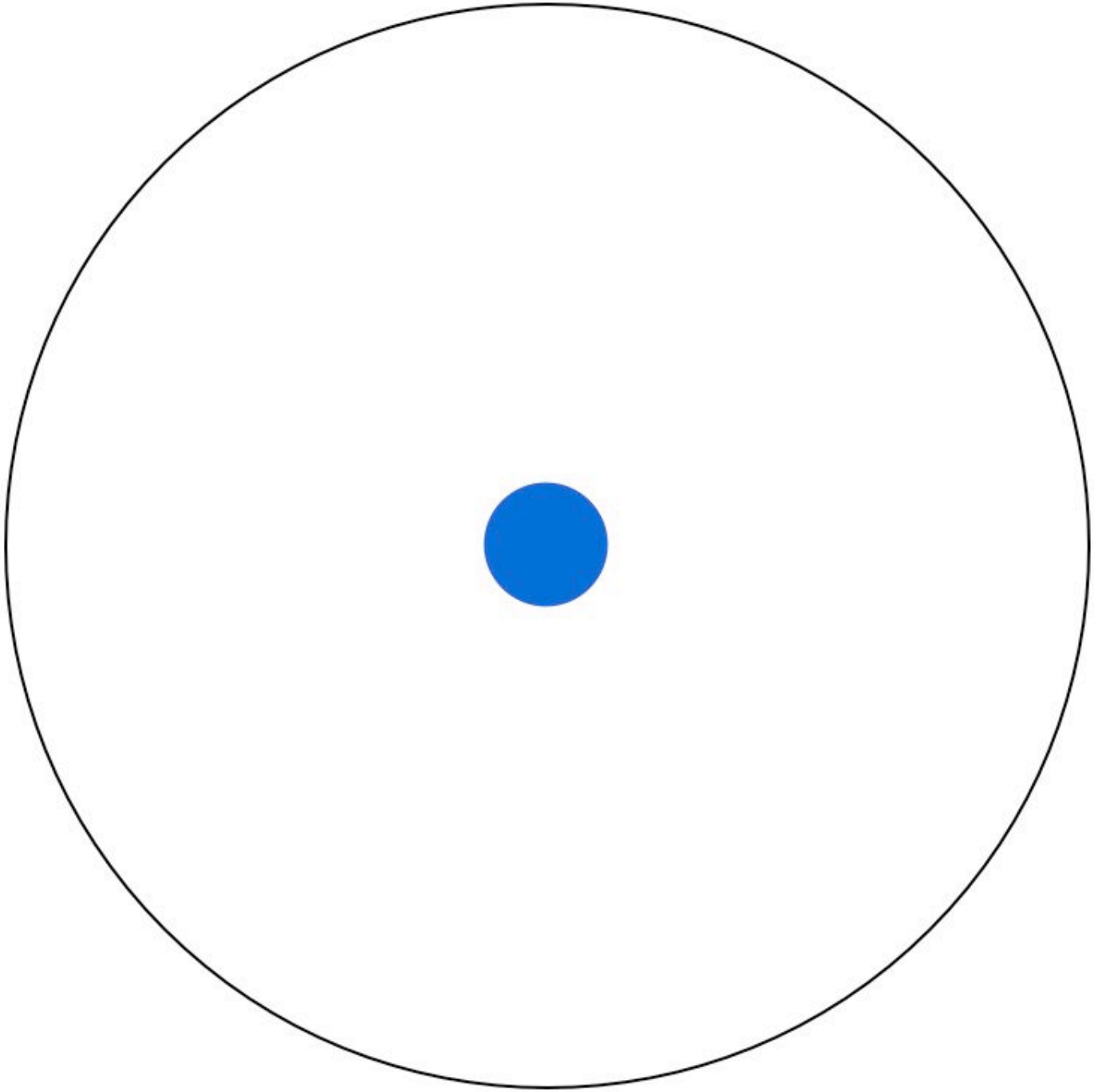
Еще вариант

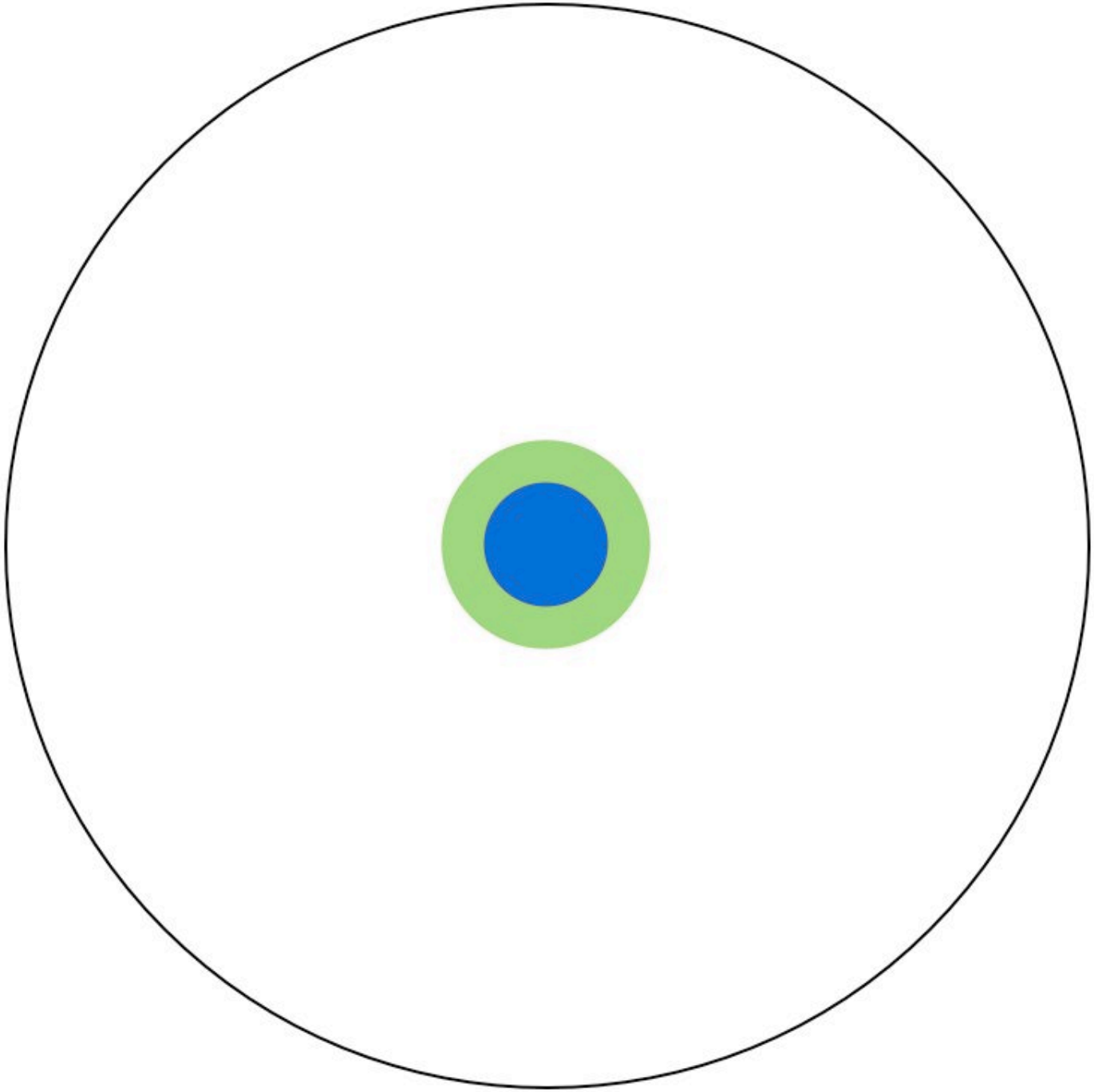

Кривая обучения популярных CMS/CMF
Навыки и знания
Время
ModX
Joomla!
Wordpress
Drupal

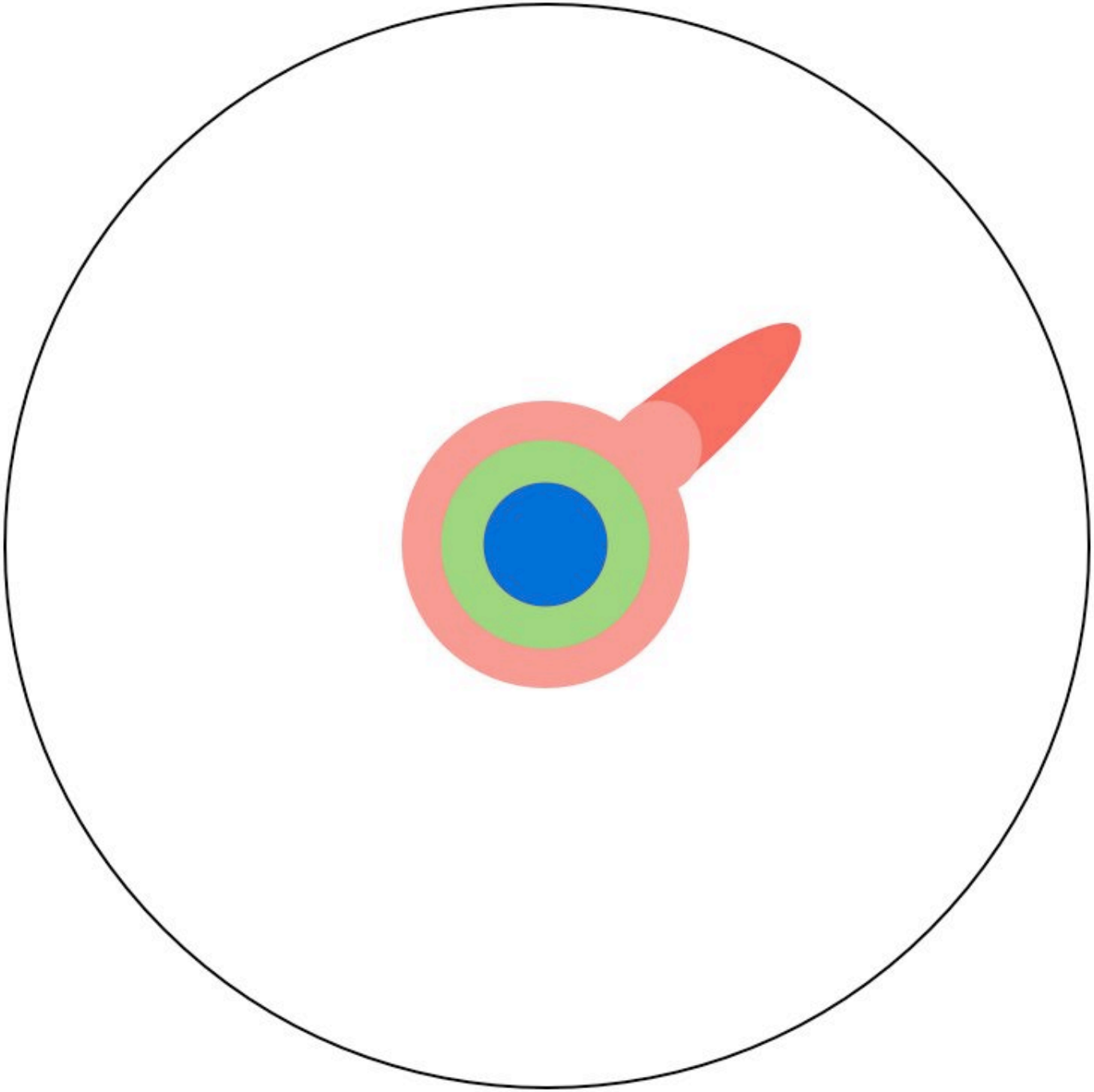
Традиционный путь

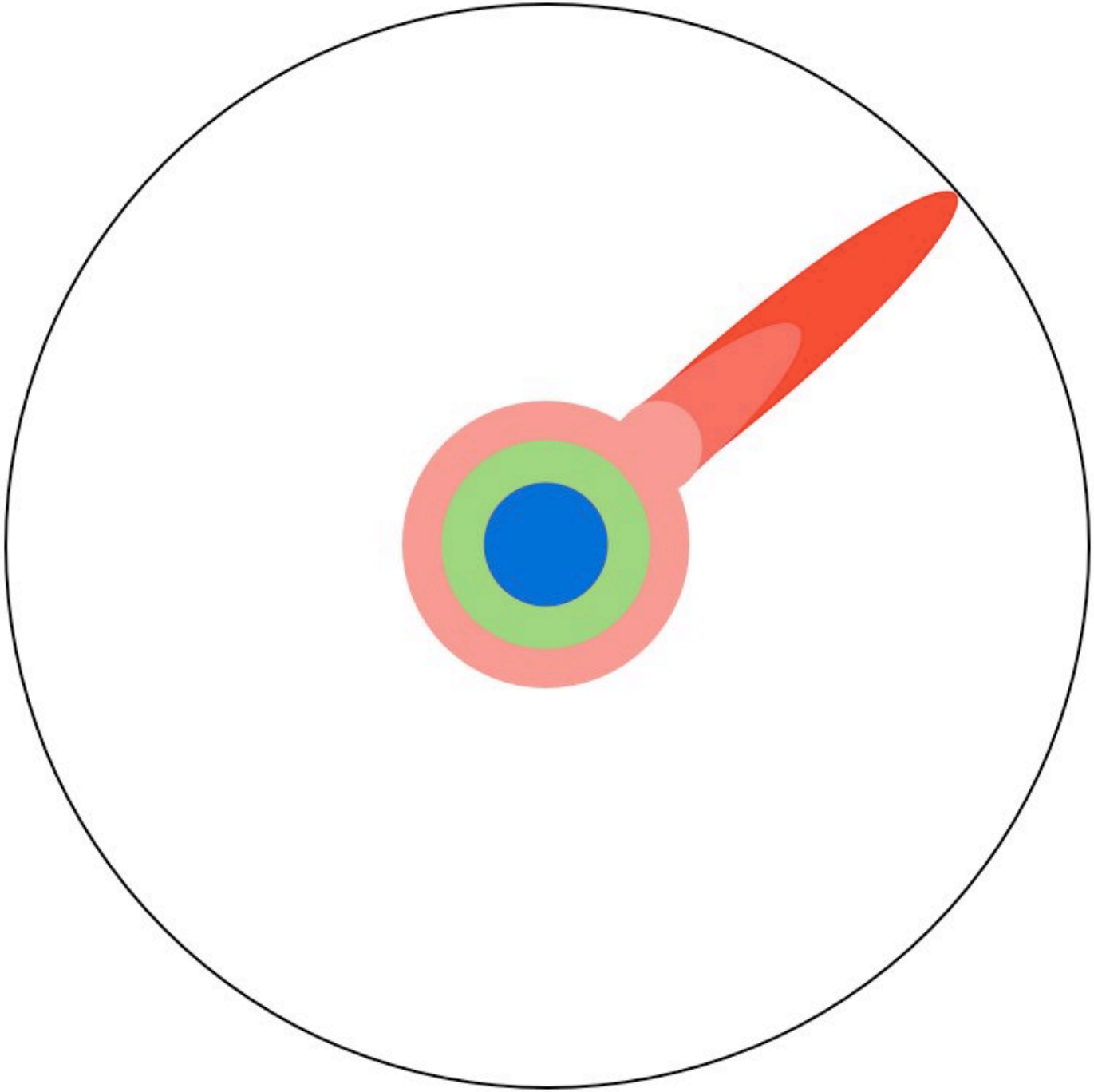
The illustrated guide to a Ph.D. by Matt Might

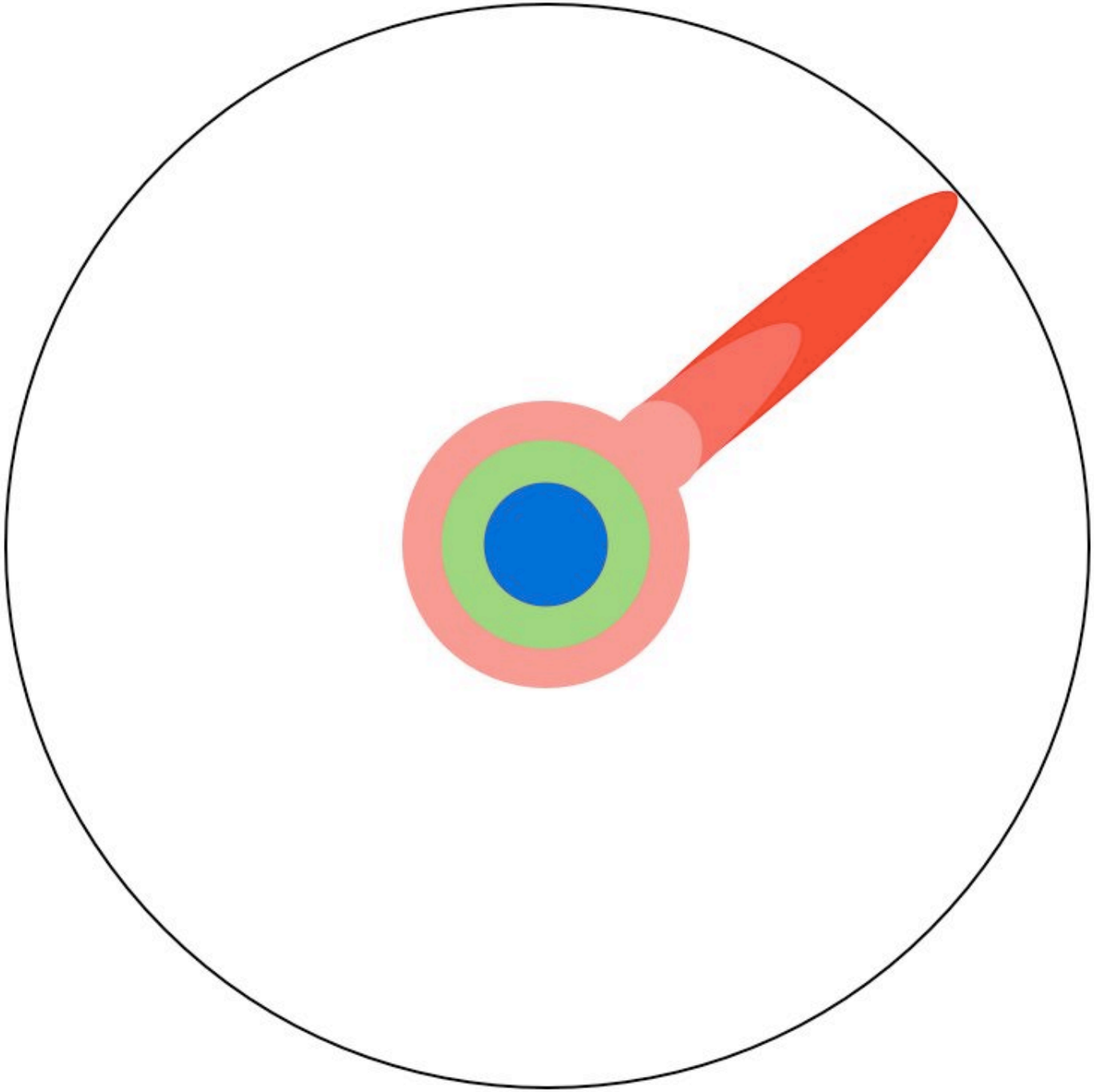


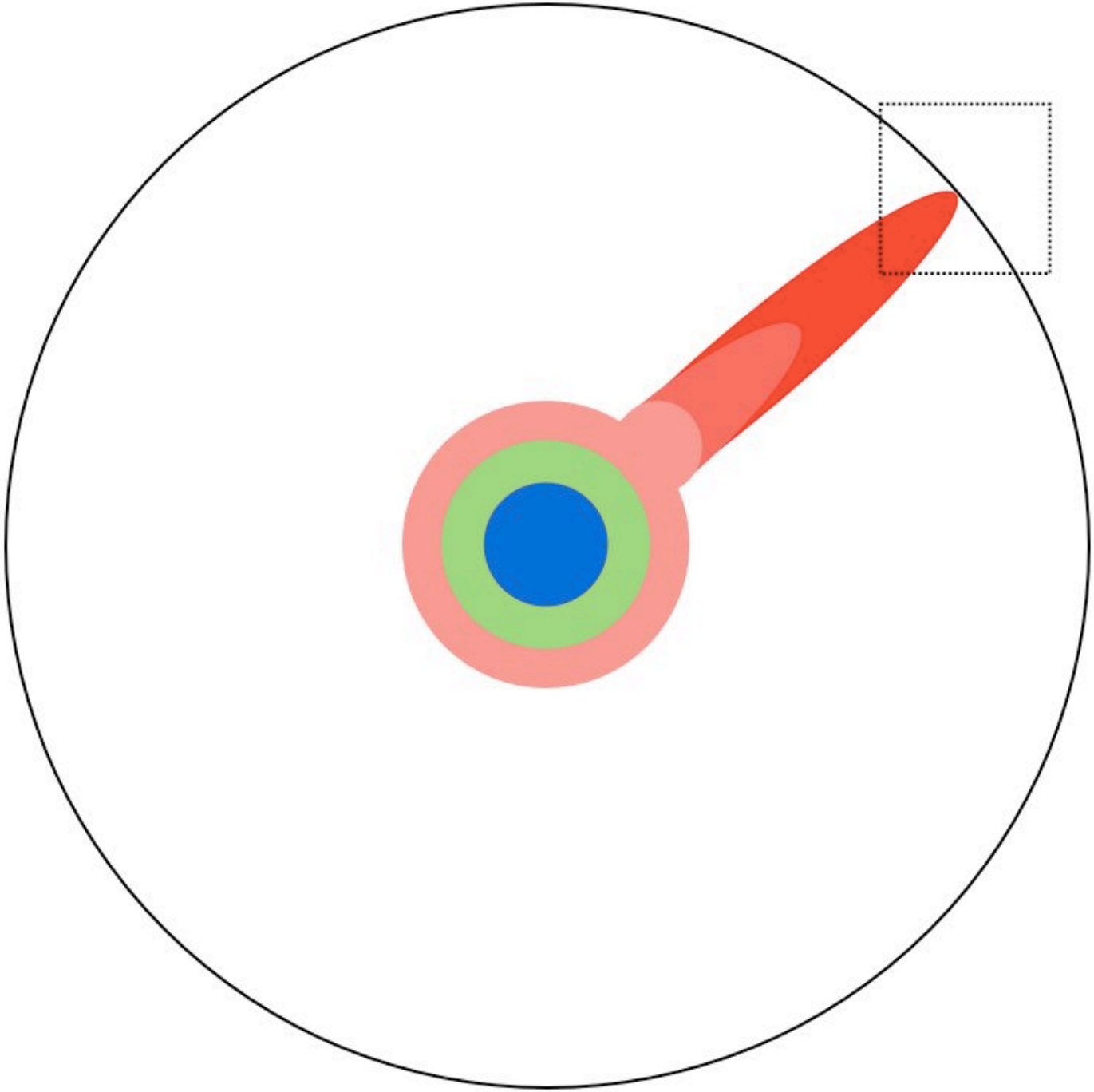


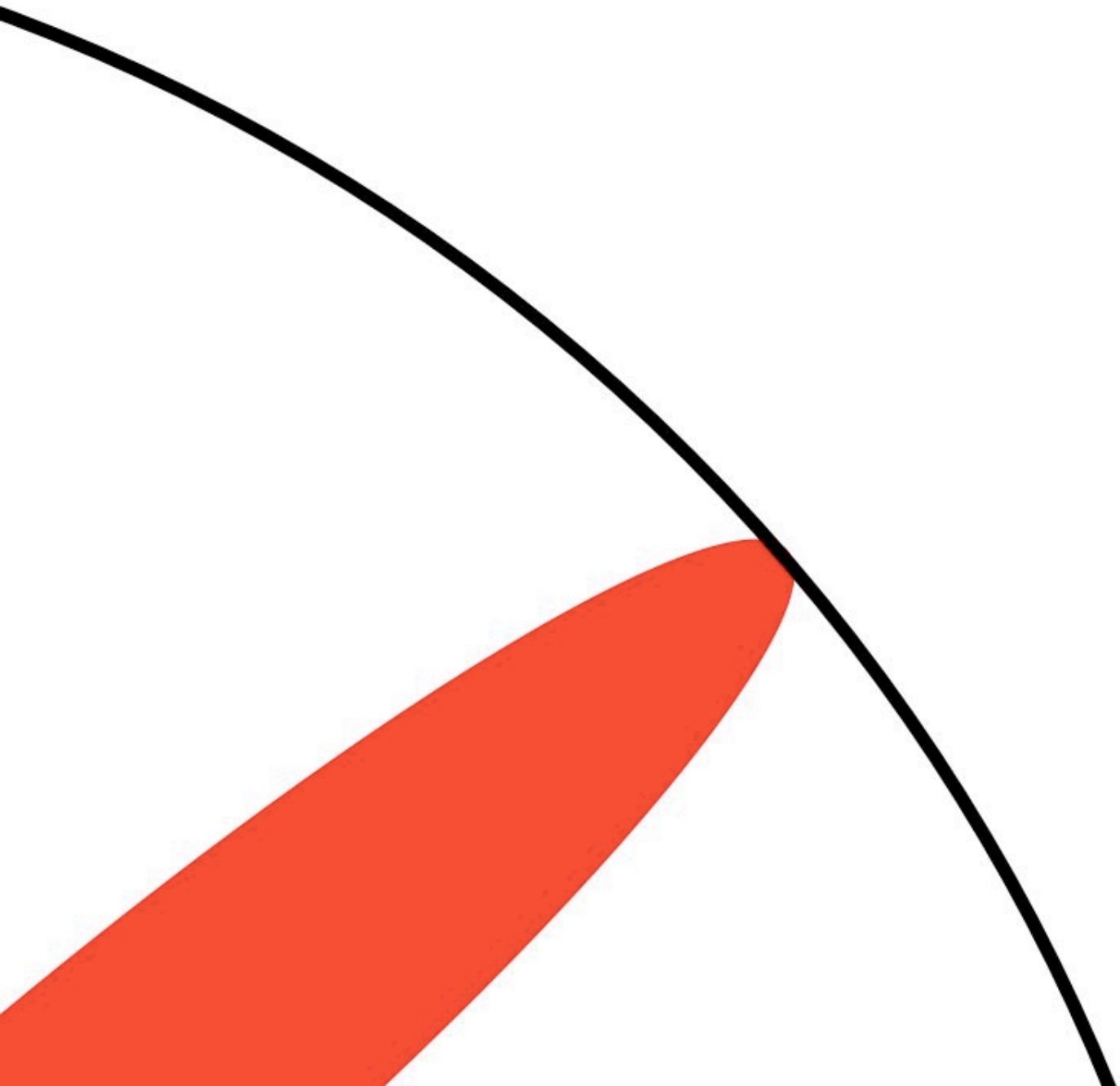


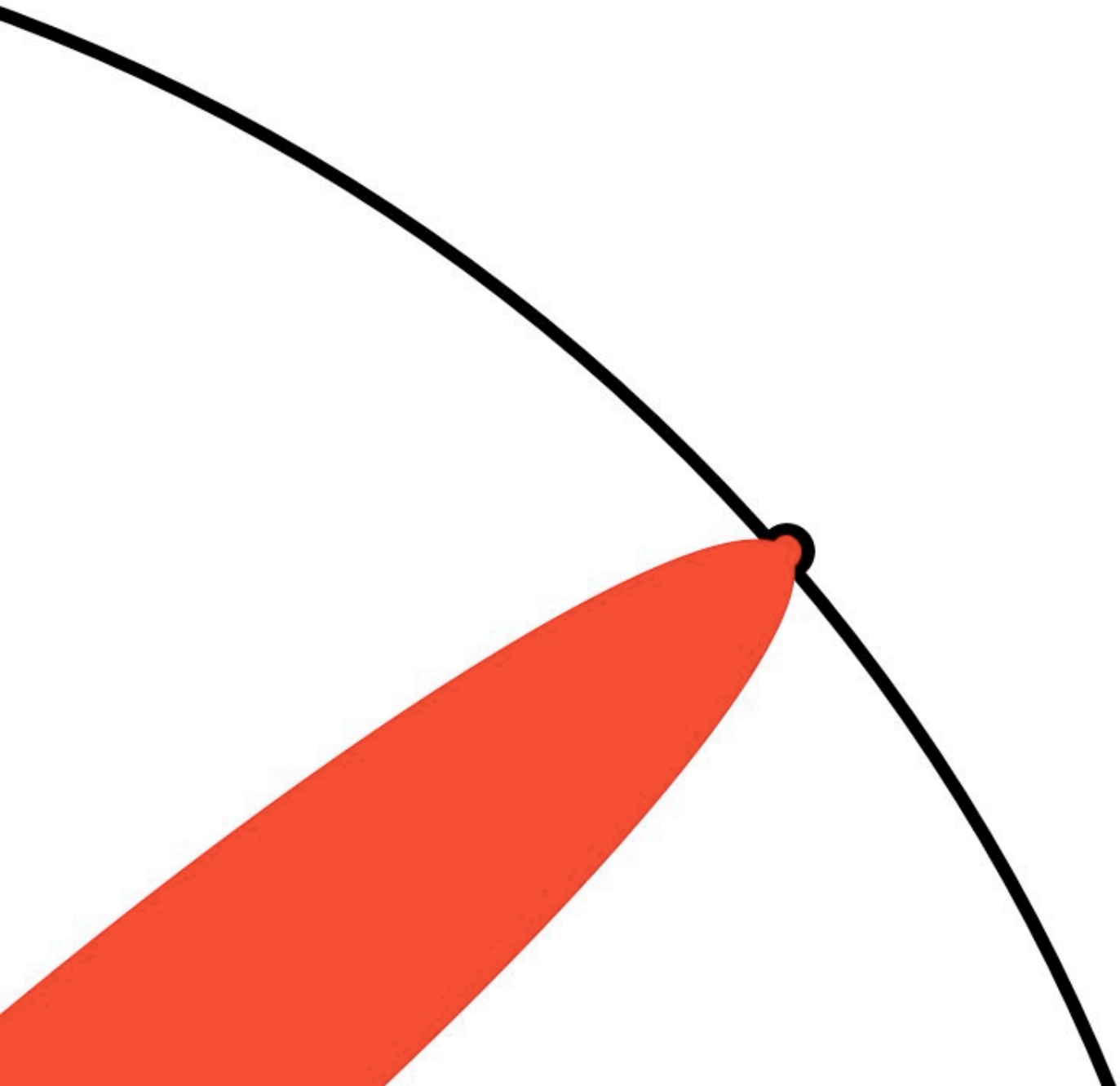


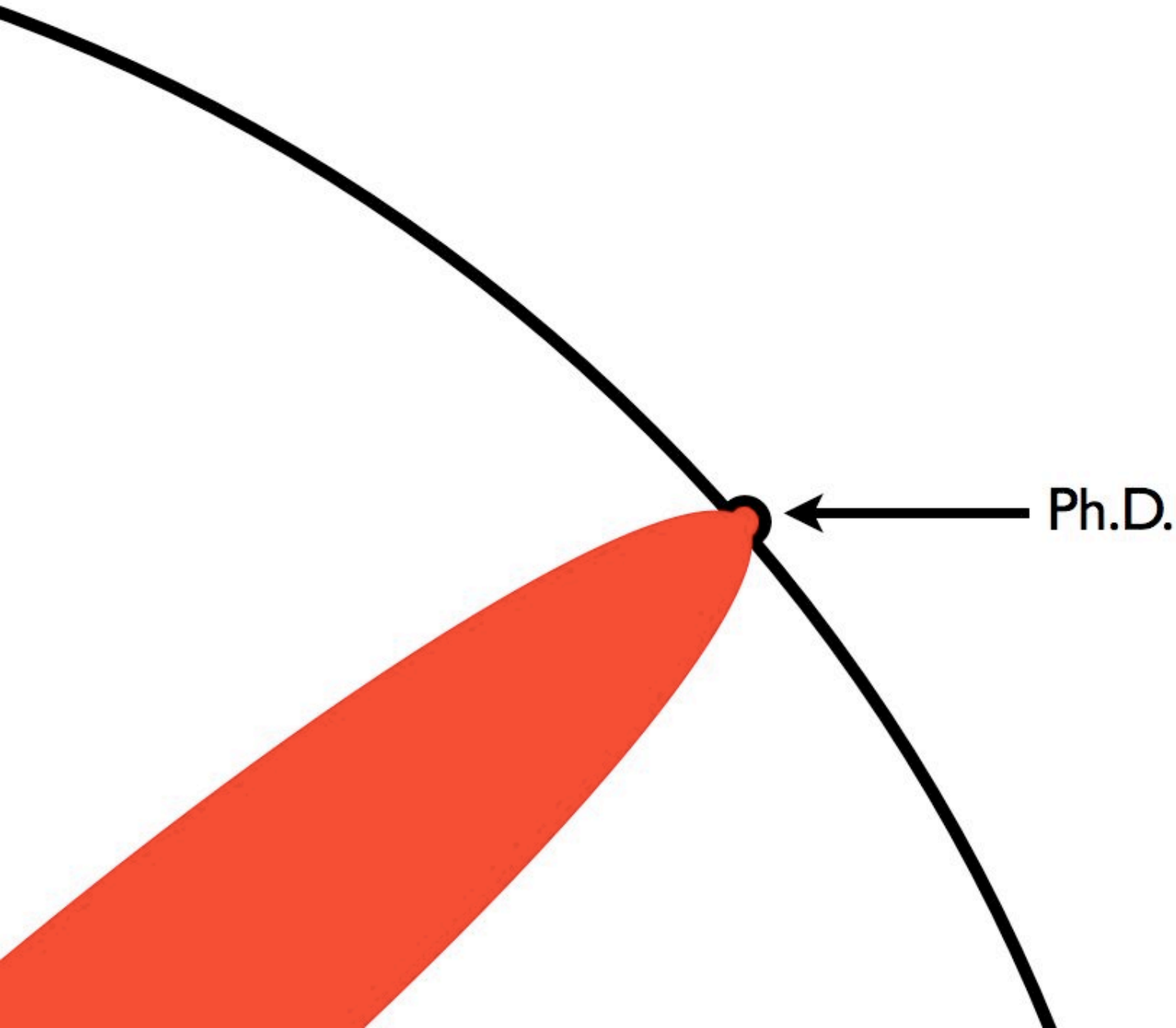


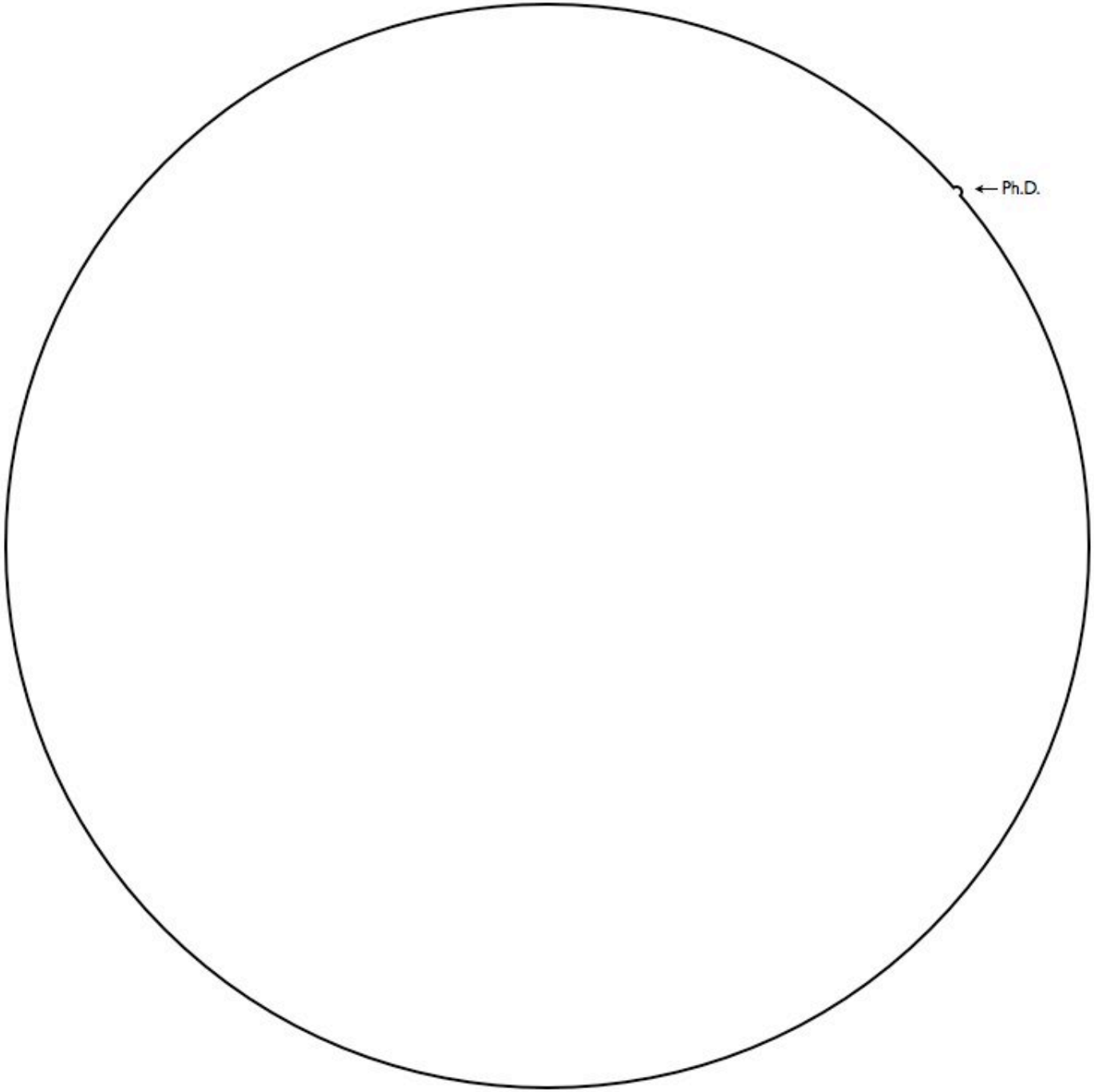






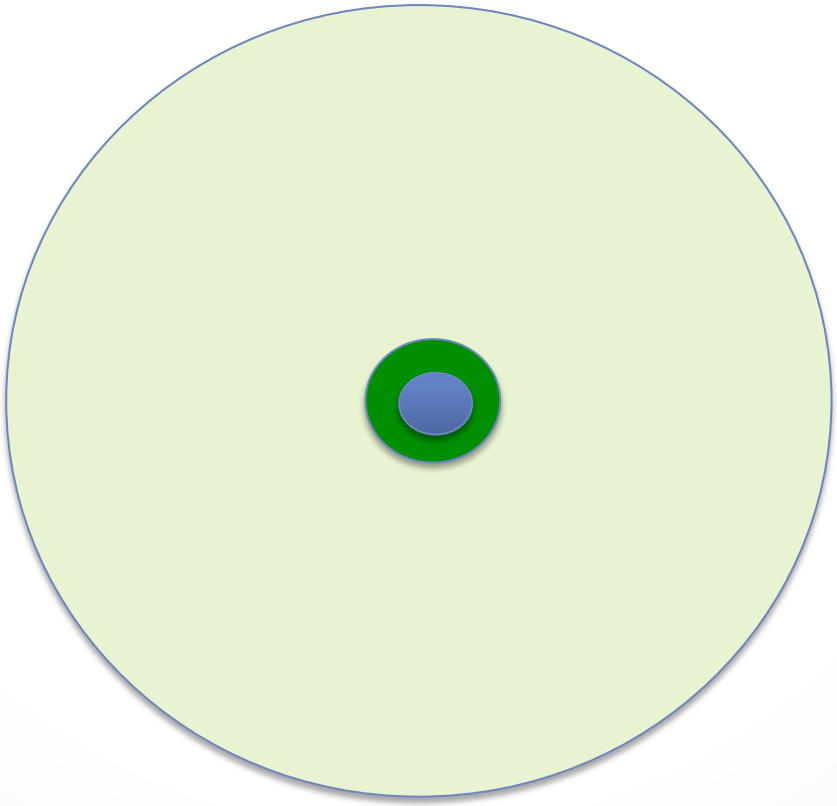



Ph.D.


Ph.D.

IT и информационная безопасность: проблема

Нужно знать всё



XSS CSRF

OWASP Top 10

PCI DSS

SQL Injection

PHP Injection

SNORT

Buffer Overflow

WAF

Suricata

Reverse Engineering

Криптография

HoneyPot

DNS poisoning

DDOS

ГОСТ

BotNet

Атаки наWi-Fi

Capture The Flag (CTF)

Командные или индивидуальные («хакерские») соревнования

Что такое CTF?

Игра за «захват флага» в оригинале – детская командная игра, где команды защищают свои флаги в лагере, и пытаются захватить флаги чужих команд.

Первые CTF игры в ИБ

DEF CON 4 (19 лет назад)

- Первая формализованная игра, где участникам предлагалось несколько серверов для взлома
- Специальные судьи оценивали результат и начисляли баллы участникам

Разнообразие CTF

Виды CTF:

- Attack/defense (нападение/защита, классические)
- Jeopardy (наборы задач)

Типы игровых сетей CTF:

- Online (Internet)
- Offline (сеть организаторов)

Виды участия:

- Командные
- Индивидуальные

Attack/defense CTF

Множество команд соревнуются друг с другом, объединенные общей сетью – атакуют сервисы друг друга и защищают свои

Типичные правила Attack/defense CTF

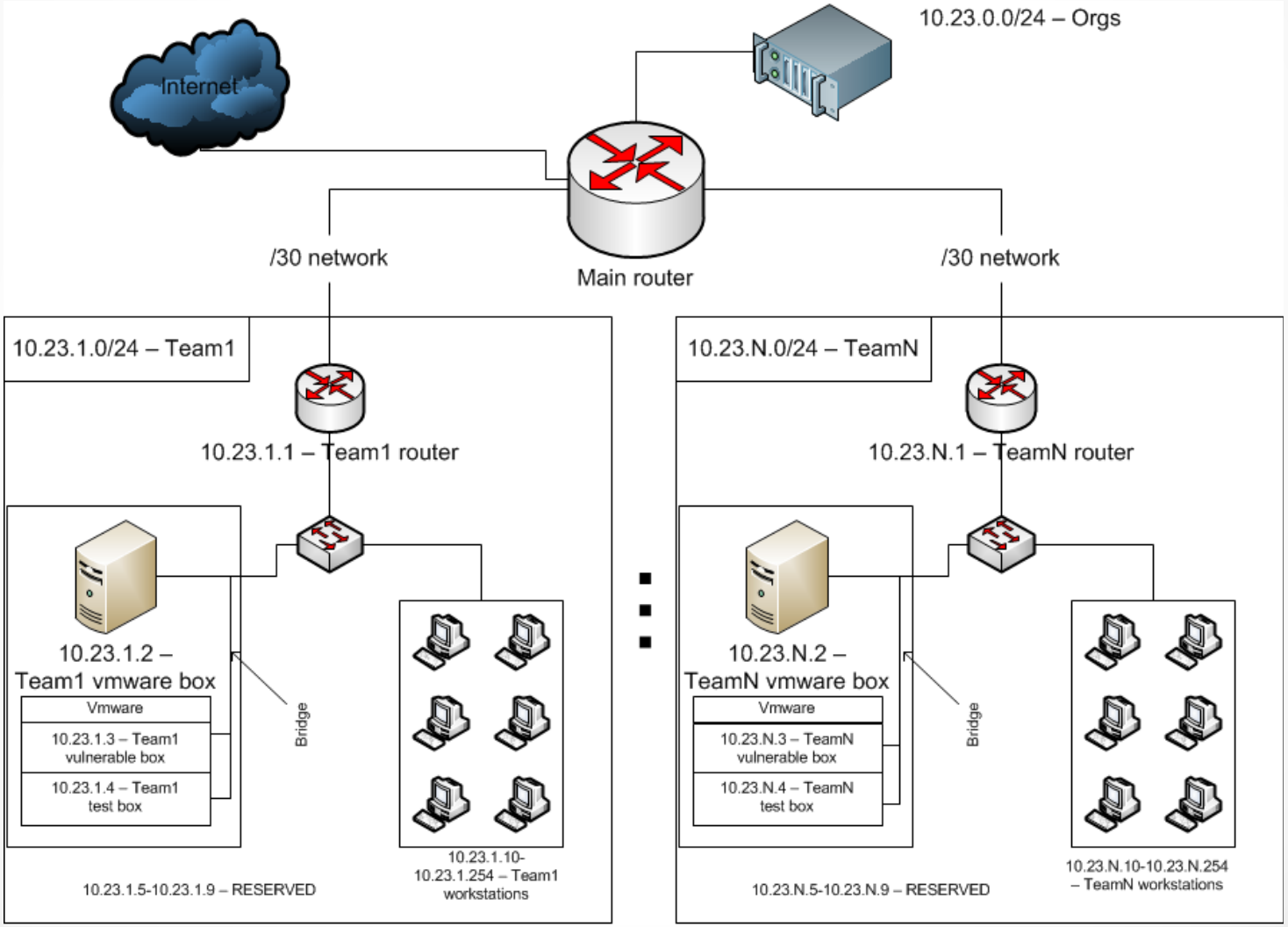
Команды могут:

- Делать что угодно со своим персональным сегментом сети. Как правило, команды заняты поиском и закрытием уязвимостей в сервисах и организацией мониторинга и/или автоматической фильтрации трафика для блокирования атак других команд
- Атаковать другие команды

Командам запрещено:

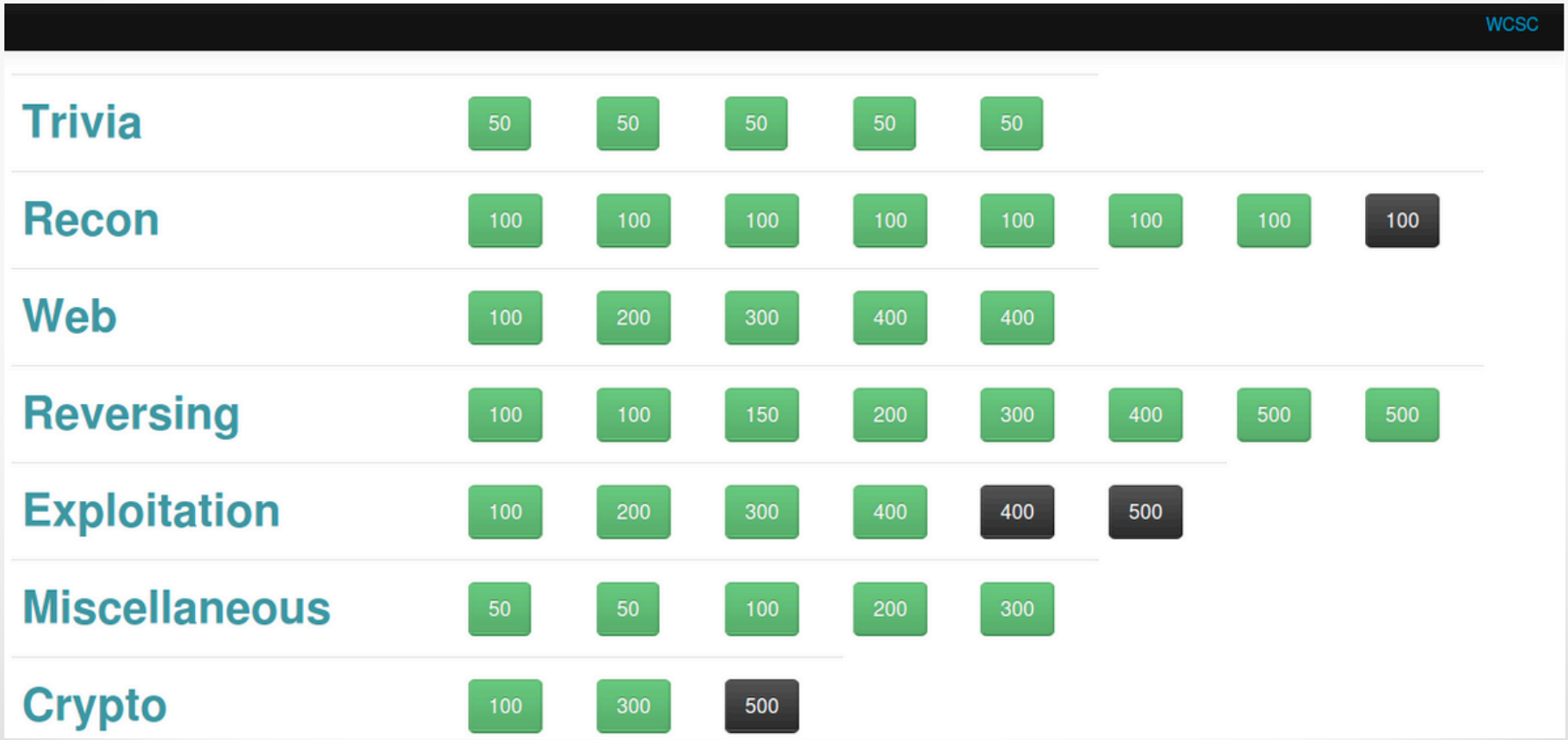
- Блокировать трафик других команд по признакам команд
- Создавать большие объемы трафика, которые нарушают работоспособность игровой сети
- Атаковать команды за пределами игровой сети
- Атаковать игровую инфраструктуру

Attack/defense CTF



Jeopardy CTF

Множество заданий разного уровня сложности, разделенные по видам: программирование, расследование инцидентов, взлом уязвимостей, обратная инженерия, криптография и многие другие.



Jeopardy CTF – категории: PWN

- Удаленная система или сервис
- Различные архитектуры: X86-32, x86-64, ARM, MIPS, что угодно
- Исходные тексты недоступны
- Найти уязвимость и создать эксплойт (программу для эксплуатации уязвимости)
- Сложная категория для начинающих, требует опыта и специфических знаний

Пример: найти переполнение буфера в программе под Linux, являющейся частью системы дистанционного обучения, взломать СДО, получить флаг

Jeopardy CTF – категории: веб безопасность

- Удаленное веб-приложение
- CGI, PHP, Python, Ruby, Perl, etc.
- Иногда исходные тексты доступны
- Найти уязвимость и взломать сайт
- Сложные и экзотические уязвимости

Пример: найти инъекцию SQL-кода в СДО и вытащить флаг из СУБД бэкенда

Jeopardy CTF – категории: криптография

- Шифротекст
- Симметричные, асимметричные, старинные, экзотические шифры
- Иногда алгоритм известен
- Расшифровать шифротекст, найти уязвимость в криптосистеме

Пример: проанализировать криптосистему и расшифровать сообщение

Jeopardy CTF – категории: обратная инженерия

- Бинарный исполнимый файл
- X86-32, x86-64, ARM, etc.
- Windows, Linux, Android, iPhone, etc.
- Проанализировать файл и вытащить флаг
- Сложная категория для начинающих, требует опыта и специфических знаний

Пример: вытащить регистрационный код из бинарного файла под Windows

Jeopardy CTF – категории: расследование инцидентов

- Даны дампы трафика, снапшоты файловых систем или жестких дисков, etc.
- Разбор файловых систем, сетевых протоколов, форматов файлов, изучение программ для расследования
- Сбор информации, восстановление данных
- Несложно для начинающих

Пример: проанализировать образ жесткого диска и вытащить флаг из удаленного файла

Jeopardy CTF – категории: стеганография

- Дан мультимедиа файл (изображение, звуковой файл, видео), дамп трафика или данные в другом виде
- Типовые или экзотические методы стеганографии
- Проанализировать контейнер и вытащить скрытое сообщение
- Несложно для начинающих

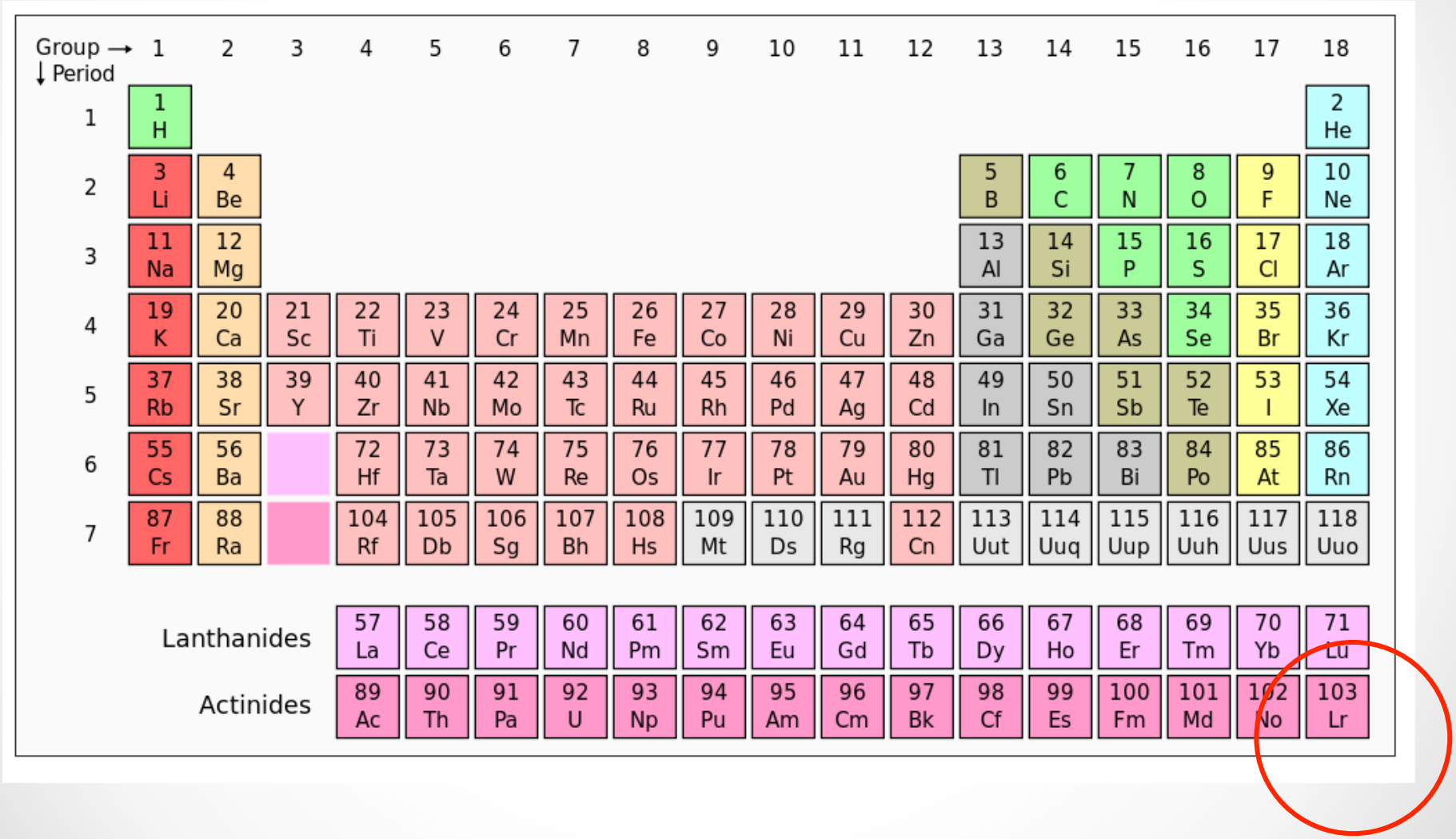
Стеганография: пример

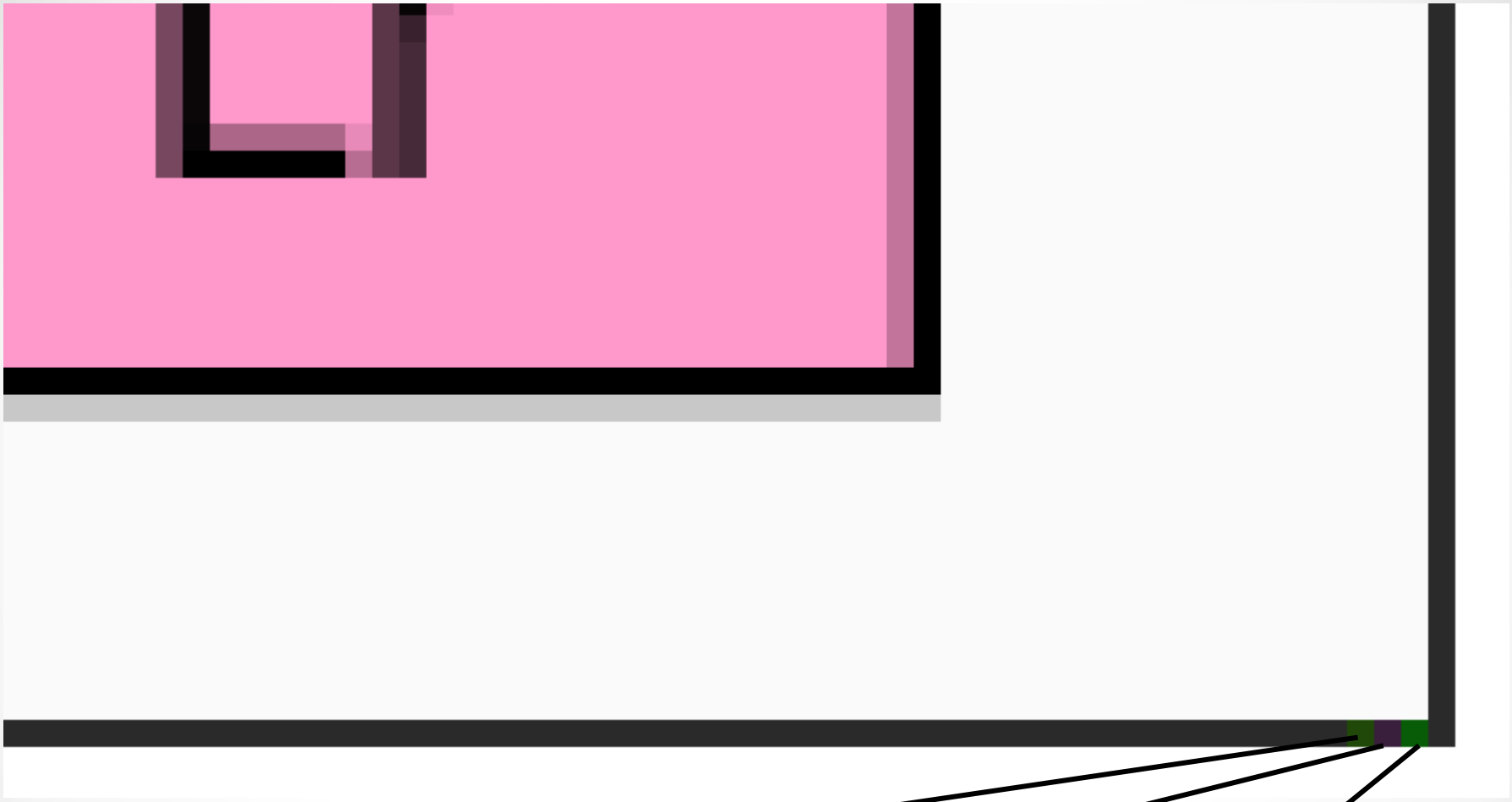
Химия, химия...
Вы перехватили файл с таблицей.
Известно, что этот файл содержит какое-то послание. Какое?

Файл с таблицей

Group → / Period ↓	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1 H																	2 He
2	3 Li	4 Be											5 B	6 C	7 N	8 O	9 F	10 Ne
3	11 Na	12 Mg											13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
4	19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
5	37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
6	55 Cs	56 Ba		72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
7	87 Fr	88 Ra		104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Rg	112 Cn	113 Uut	114 Uuq	115 Uup	116 Uuh	117 Uus	118 Uuo
Lanthanides				57 La	58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb	71 Lu
Actinides				89 Ac	90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No	103 Lr

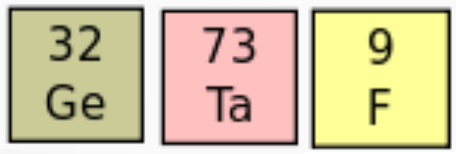
Разбор задания

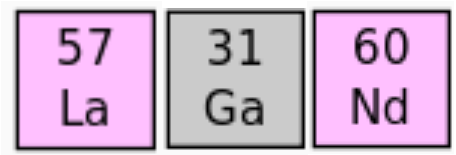


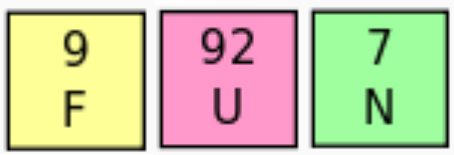


RGB: 32,73,09 RGB: 57,31,60 RGB: 09,92,07

RGB: 32,73,09 RGB: 57,31,60 RGB: 09,92,07







Ответ: GeTaFLaGaNdFUN

Еще пример

Наиболее известные соревнования CTF

- **DEFCON** (on-site, Las Vegas, USA)
- **iCTF** (удаленные через интернет, Santa Barbara, USA)
- **CODEGATE** (on-site, Seul, South Korea)
- **RuCTFE** (удаленные через интернет, Екатеринбург, Россия)
- **rwthCTF** (удаленные через интернет, Aachen, Germany)
- **PHDays** (on-site, Moscow, Russia)
- **Hack.Lu CTF** (удаленные через интернет, Luxembourg)
- **RuCTF** (on-site, Екатеринбург, Россия)

BUSHWHACKERS

Наш опыт

История команды

- Осень 2009 года – научная конференция в Милане
- Январь 2010 – создание команды, участие в первых РусКрипто CTF
- Первоначально 5 человек, в 2014-2015 гг. до 30+ человек
- Призовые места:
  - 1 место UCSB iCTF 2013
  - 1 место RuCTFe 2014
  - Квалификация для участия в DEF CON 2015 (top 15 команд)

CTFTIME.ORG

CTF TIME | CTFs | Upcoming | Archive | Calendar | Teams | FAQ | Contact us | About | Sign in

Bushwhackers

Website: bushwhackers.ru

0

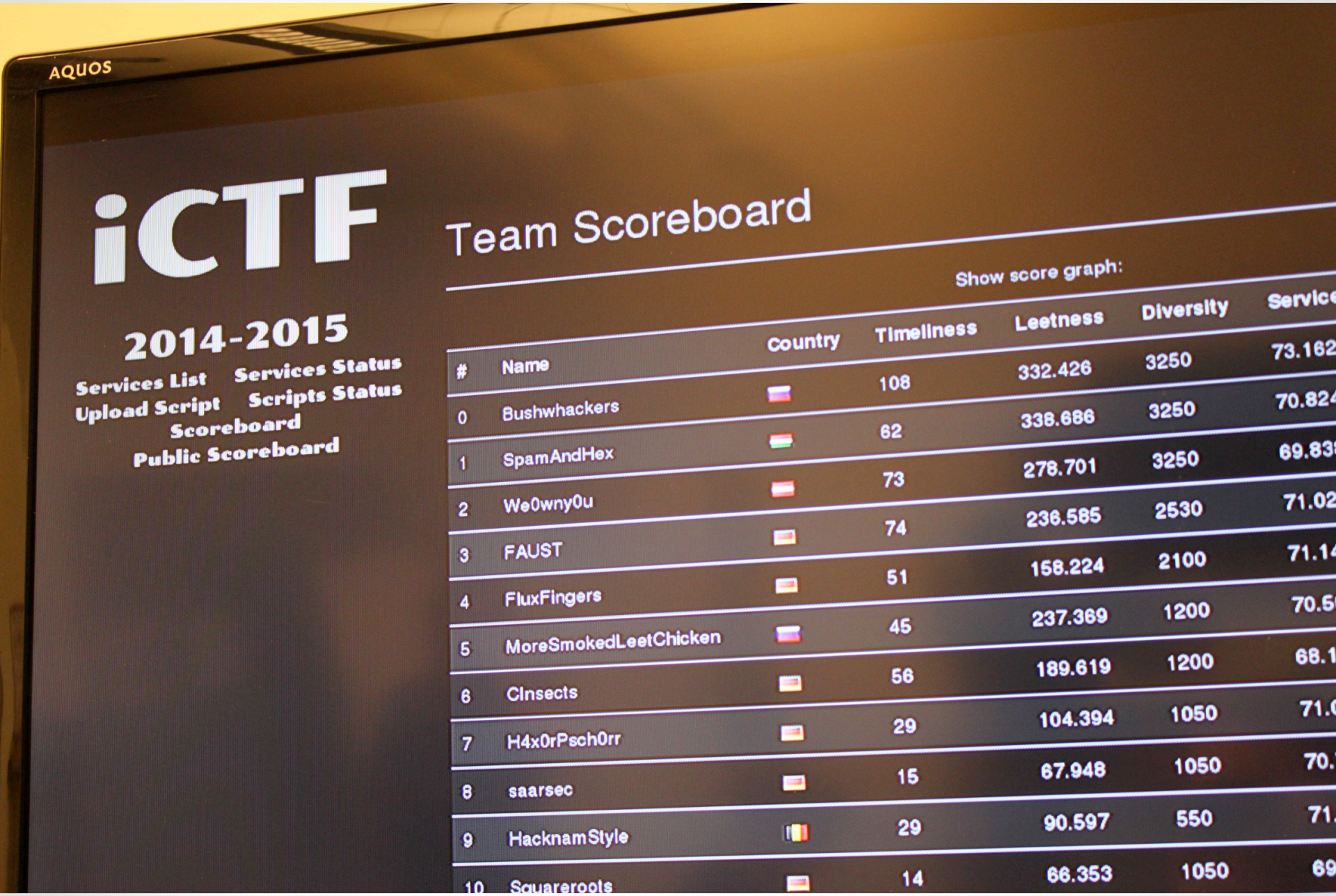
Sign in to join the team.

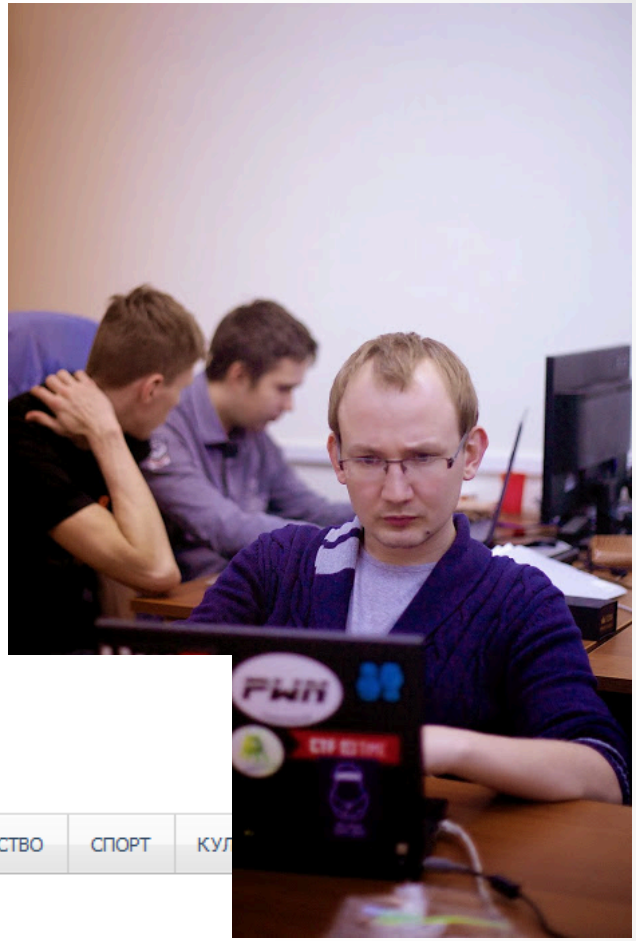
Participated in CTF events

2015 | 2014 | 2013 | 2012 | 2011 | 2010

Overall rating place: **33** with **186.536** pts in 2015

Place	Team	CTF points	Rating points
15	DEF CON CTF 2015	7447.0000	15.105
53	PoliCTF 2015	1200.0000	7.846
8	PHD CTF Finals 2015	630445.0000	4.402
70	DEF CON CTF Qualifier 2015	10.0000	17.075
21	ASIS CTF Quals 2015	2551.0000	14.736
7	VolgaCTF 2015 Quals	4550.0000	20.700
52	PlaidCTF 2015	1021.0000	18.191


AQUOS
iCTF
2014-2015
Services List
Services Status
Upload Script
Scripts Status
Scoreboard
Public Scoreboard
Team Scoreboard
Show score graph:
Name Country Timeliness Leetness Diversity Servic
0 Bushwhackers 108 332.426 3250 73.162
1 SpamAndHex 62 338.686 3250 70.824
2 We0wny0u 73 278.701 3250 69.83
3 FAUST 74 236.585 2530 71.02
4 FluxFingers 51 158.224 2100 71.14
5 MoreSmokedLeetChicken 45 237.369 1200 70.5
6 CInsects 56 189.619 1200 68.1
7 H4x0rPsch0rr 29 104.394 1050 71.
8 saarsec 15 67.948 1050 70.
9 HacknamStyle 29 90.597 550 71.
10 Squareroots 14 66.353 1050 69



RG.RU Российская Газета | http://ИНТЕРНЕТ

ВЛАСТЬ | ЭКОНОМИКА | В РЕГИОНАХ | В МИРЕ | ПРОИСШЕСТВИЯ | ОБЩЕСТВО | СПОРТ | КУЛ

Российские хакеры обошли своих конкурентов с помощью ядерной ракеты

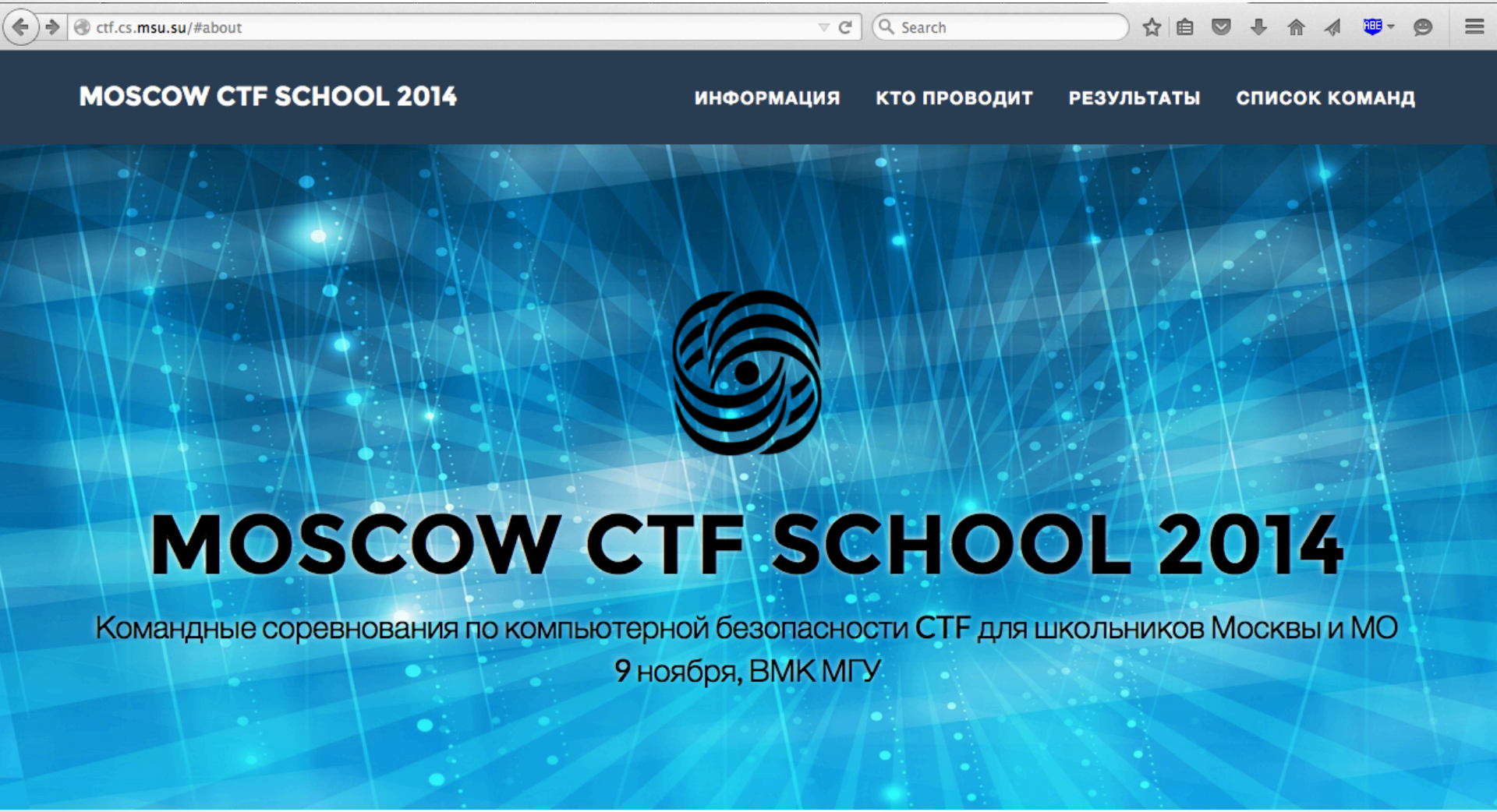
Текст: Юлия Воронина

10.12.2013, 16:54 Версия для печати

DEF CON 23

RuCTF 2015

А теперь – для школьников!



MOSCOW CTF SCHOOL 2014
2nd place
MOSCOW CTF SCHOOL 2014
1st place
MOSCOW CTF SCHOOL 2014
3rd place

РЕЗУЛЬТАТЫ MOSCOW CTF SCHOOL 2014

#	TeamName	Score
1	Shadow servants	5700
2	Пылающие Помидоры	5500
3	1336 h4x0rz	3200
4	Салат "Цезарь"	3000
5	VectorTeam	2800
6	101	2700
7	The_invulnerable	2200
8	DS	2200
9	Undefined	2000
10	SegFault	1900

Видео о соревнованиях

CTF – непрерывное обучение

Что дальше?

- Участвовать в Bug Bounty! Вот хороший хаб - https://hackerone.com/
- Актуальный список Bug Bounty: https://bugcrowd.com/list-of-bug-bounty-programs

Контакты

Денис Гамаюнов

- к.ф.-м.н., зав. лабораторией интеллектуальных систем кибербезопасности ВМК МГУ
- gamajun@seclab.cs.msu.su
- +7 (495) 939 00 91