

CyberED × STANDOFF 365

Врывайся в AI-гонку

AI-агенты в наступательной безопасности — что
меняется в профессии и в турнирах.

Четверг, 24 сентября • 19:00 МСК



Сегодня с вами



Иван Булавин

- + Директор по продуктам платформы Standoff 365, Positive Technologies
- + Капитан команды True0xA3 на Standoff 13
- + Сам формирует площадку, на которой будет тренироваться твой поток



Егор Богомолов

- + CEO CyberED, архитектор программы «Пентестер» — запускает её в десятый раз
- + Вице-капитан True0xA3, призёр Standoff
- + Основатель компании белых хакеров Singleton Security
- + Лично ведёт часть занятий и разбирает атаки вживую

О чём говорим сегодня

Кибербитва Standoff 2027

Полигон — копия целой компании

Разработка AI-агентов

AI против AI на Standoff

AI-турниры и челленджи

Приватный Bug Bounty

Приватные кибериспытания

Командные турниры

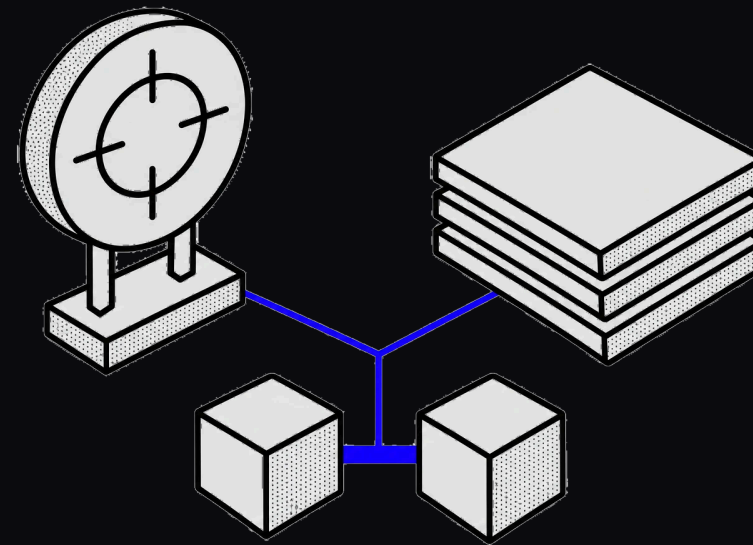
Рейтинг

Персональная траектория

Карта компетенций

Авторские интенсивы без доплат

Мы уже **4 года** в партнёрстве
обучаем специалистов
по кибербезопасности



Что мы уже сделали вместе

// программы

Программы

- > Учишь находить баги и зарабатывать на этом — совместный курс со Standoff Bug Bounty
- > Готовим к турнирам топовые команды Standoff
- > Наши эксперты учат хакингу студентов со всего мира — в хак-лагере Positive Technologies: 300 студентов, 3 года, 40 стран
- > Готовим целые команды компаний к битве на Standoff — под ключ
- > Эксклюзивный запуск со Standoff 365 — практикуешься на площадках по всему миру, вплоть до Зимбабве
- > Запуск 10-го потока — тоже со Standoff 365

// турниры и челленджи

Командные турниры



- > Командные CTF-турниры с призами
- > AI-челленджи по пентесту на Standoff 365

// мероприятия и эфиры

Мероприятия



- > Практики на платформах Standoff с топовыми хантерами
- > Обучающие эфиры, разборы атак и задач турниров, практикумы

AI уже ломает и защищает

Каждую неделю — новый громкий кейс.

Claude Code на автопилоте

Госхакеры угнали AI-инструмент Anthropic для кибершпионажа против 30 целей — AI сам вёл 80–90% тактических операций

Испания: взлом без человека

Регулятор AEPD зафиксировал первый взлом, который от начала до конца провёл автономный AI-агент — сам нашёл уязвимость и подменил данные

Google поймал AI-эксплойт

Нашли 0-day, разработанный с помощью AI, и остановили готовившуюся массовую атаку ещё до старта

Hugging Face: спасла китайская модель

Топовые модели не справились с атакой — отбила её открытая китайская нейросеть

Четыре AI против MaxPatrol O2

На Standoff столкнули HexStrike AI, GLM 5.1, PentAGI и NyxStrike с защитой Positive Technologies — критические события заняли от 40 минут до нескольких часов

AI уже сражается с AI — на Standoff

Такие агенты уже соревнуются на Standoff — крупнейшей кибер-площадке страны, и ты можешь оказаться на любой стороне: атакующей или защищающей.

// продукт · 4 кв. 2026

Standoff Defend

Тренируешься против AI, который сам выбирает путь атаки — как в настоящей атаке.

// эксперимент · ПМЭФ, июль 2026

AI против AI

Лучший атакующий AI выполнил все критические события за 40 минут — против него держит оборону MaxPatrol O2 от Positive Technologies.

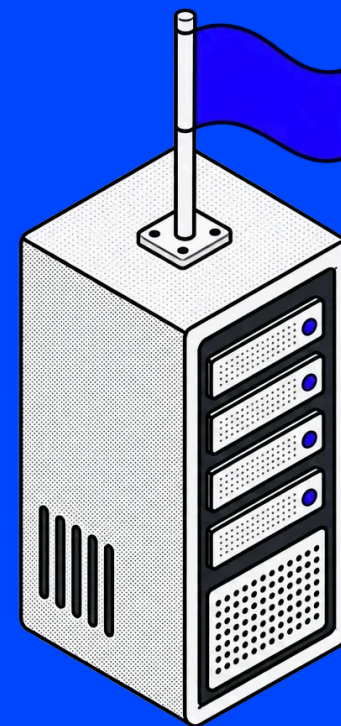
// открытые учения · 6 октября 2026

«Защитники vs. ИИ»

Проверяешь себя против атак AI наравне с людьми — можешь выиграть номинацию, угадав, кто атаковал.

Ландшафт трансформируется: хакеры — и белые тоже — теперь создают агентов, которые работают на них

Разберём, как тренироваться в сезоне 2026–2027 — и как это уже работает на Standoff.



Юбилейный, 10-й поток «Пентестер»

Разработка своих агентов

Интенсив «AI-пентест» от Сергея «Похека» Зыбнева. Разбор дальше в потоке.

Приватные bug bounty и кибериспытания

Разведка, отчёты и вознаграждение в закрытых программах потока.

Полигон с инфраструктурой реальных компаний

Внешний периметр, DMZ, внутренняя сеть. Копия компании целиком.

Подготовка к сертификации

Идёшь к OSCP и LPT по плану. Впервые в потоке.

Стрим с Богомоловым: рынок и наём

Рынок труда, запуск микросервисов и платформ в ИБ. С приглашёнными гостями.

// участвует в потоке

Разрабатывает программу и ведёт её лично — Егор Богомолов

Собрал программу «Пентестер» и постоянно её развивает: обновляет модули под свежие техники и угрозы. Ведёт часть занятий и живые семинары лично.

белый хакер

вице-капитан True0xA3

призёр Standoff

основатель Singleton Security

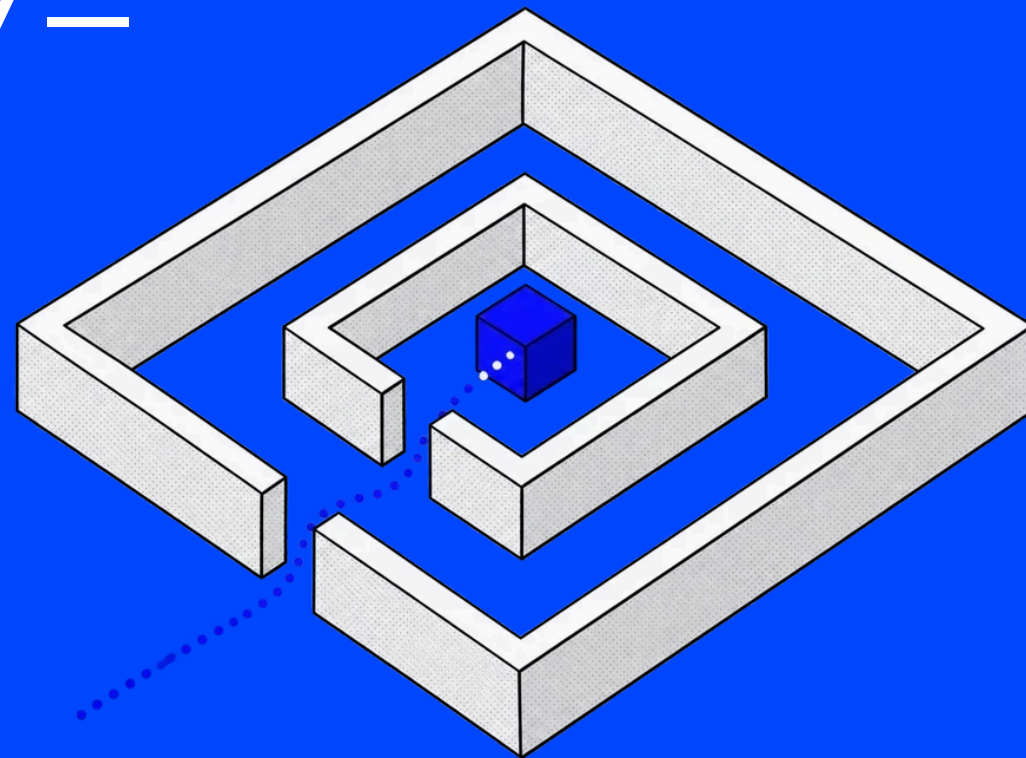
партнёр фонда «Сайберус»



Кибербитва Standoff 2027 — **КОМАНДОЙ** и без отбора

Крупнейшая кибербитва страны: атакующие команды реализуют недопустимые события на макете целого государства — банки, транспорт, энергетика, промышленность. За битвой следит весь рынок — и туда идёт команда топ-10 рейтинга потока.

- > обычно в состав берут с именем и результатами — тебе путь короче
- > строчка «участник Standoff» в резюме говорит нанимающему больше любого сертификата
- > опыт под давлением, в команде и против живых защитников
- > команда потока едет на Standoff 2027 гостевым слотом — играете рядом с топ-командами рынка и боретесь за приз



// фундамент • базовая подготовка

Сначала фундамент: базовая подготовка

Карта компетенций

Растёт вместе с тобой — 3 уровня сложности на технику, видно, что уже освоено.

Портал CyberEd	Fundamentals	Red	Blue	Освоена полностью (158)	Освоена частично (25)	Начата (0)	Не начата (6)	Поиск	Сортировка: По дате получения
Дашборд	Р301 Пентестер								
Обучение	1. Использование целей тестирования (5/7)								
Активности	2. Получение первичного доступа через атаки на аутентификацию (4/5)								
Матрица компетенций	3. Получение первичного доступа через атаки на веб-приложения (6/11)								
Профиль	4. Получение первичного доступа через атаки социальной инженерии (2/2)								
	5. Эксплуатация известных уязвимостей (6/77)								
	6. Подготовка инструментов атак (1/2)								
	7. Повышение привилегий в Linux (11/24)								
	8. Повышение привилегий в контейнерных средах (3/6)								
	9. Повышение привилегий в Windows (7/12)								
	10. Пробои сетевого трафика (11/5)								
	11. Атаки на локальные сети (6/6)								
	12. Атаки на Active Directory (5/12)								
Ещё									
Справка									
	Техника	Базовый	Средний	Продвинутый	Модули				
	1-8114 Техника повышения привилегий через уязвимости в Windows Print Spooler (PrintNightmare)	У/1	18.04.2025	30.04.2025	8391-45				
	1-8111 Техника эксплуатации File Upload	У/1	17.04.2025	01.05.2025	8391-45				
	1-8178 Техника повышения привилегий в Docker-контейнере через mounts	У/1	11.06.2025	30.06.2025	8391-45				
	1-8275 Техника атаки на Apache Log4j (CVE-2021-44228)	У/1	10.04.2025	28.04.2025	8391-45				
	1-8171 Техника атак на Confluence	У/1	07.06.2025	28.06.2025	8391-45				
	1-8174 Техника атак на GitLab	У/1	07.06.2025	28.06.2025	8391-45				
	1-8189 Техника пробои сетевого трафика (Pivoting) с помощью встроенных возможностей ОС Windows	У/1	02.09.2025		8391-45				
	1-8191 Техника офлайн-подбора паролей методом грубой силы с помощью правил	У/1	03.04.2025	03.04.2025	8391-45				
	1-8192 Техника офлайн-подбора паролей методом грубой силы с помощью словарей	У/1	03.04.2025	03.04.2025	8391-45				
	1-8121 Техника эксплуатации уязвимостей в Linux через Sudo	У/1	16.04.2025	24.06.2025	8391-45				
	1-8195 Техника исполнения произвольного кода в прикладных программах (Zabbix, Ansible, СУБД и пр.)		07.06.2025	24.06.2025	8391-45				
	1-8125 Техника офлайн-подбора паролей методом грубой силы	У/1	03.04.2025	03.04.2025	8391-45				
	1-8153 Техника поиска ошибок конфигурации автозапускаемых приложений, позволяющих изменять их исполняемые файлы	У/1	12.08.2025		8391-45				
	1-8179 Техника злоупотребления LAPS			09.06.2025	8391-45				

Портал с отработкой техник

3 уровня сложности на каждую технику — от простого до продвинутого.

Briefing

Checkpoint questions

Submit report

Network inventory

Points

Submitted 0

Under review 0

Accepted 0

Meridian

Investigation

The Meridian engineering company learned what had happened not from its own administrators but from a client, who forwarded a signed contract bearing bank details Meridian has never had. The money left on Thursday; the incident was raised on Monday.

The infrastructure has not been touched: no machine reinstalled, no log cleared, no account disabled — everything is as the intruder left it. You have been given administrative access and three days to answer how they went from a public service to the system where contracts are approved.

An attack on the organization's infrastructure has already happened. Your task is to reconstruct it: where the attacker started, how they moved deeper into the network and what they did on each host.

Access to the machines is provided, and you work with the infrastructure as an administrator. It is available in the state the attacker left it in — the traces of every step are still there.

Work from the traces: service and operating system logs, command history, created files and scheduled tasks, accounts and their privileges, network connections. Record your conclusions in the notes of the systems — that way it is clear which hosts have already been covered.

Start by answering the checkpoint questions about the course of the attack: they open the report form. After that the analysis of each stage is submitted as a report.

Unacceptable events of the polygon:

A contract is forged and processed on behalf of the organization.

Access over OpenVPN:

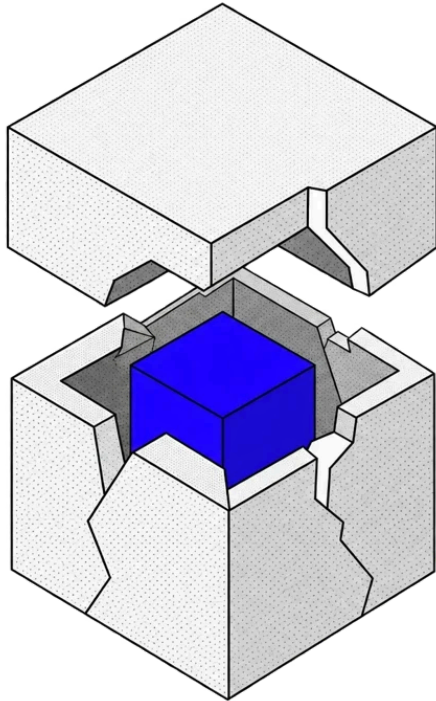
External Perimeter — external.ovpn

Internal Network — internal.ovpn



// полигон CyberED • полигон Standoff 365 • уровень HARD

Учишься ломать компании на **2 полигонах** от CyberED и Standoff 365



- > Полигон воспроизводит компанию целиком: внешний периметр, DMZ и внутренняя сеть — собираешь цепочку атаки, закрепляешься и продвигаешься внутрь
- > Большинство задач решаются несколькими способами
- > В юбилейном потоке открыты все сценарии, включая лаборатории «Банки, SCADA и промышленные системы» — обычно они только для корпоративных клиентов
- > Полигон обновляется и связан с картой компетенций — растёт и у тех, кто уже учится

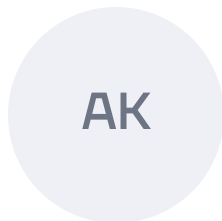
// команда потока

Эксперты программы



Егор Богомолов

Архитектор программы
«Пентестер» · генеральный
директор CyberED



Азамат Кулаков

Специалист по
информационной безопасности
· Госслужба



Кирилл Николаев

Тестирование на
проникновение · Антивирусная
лаборатория



Никита Коломиец

Специалист по тестированию
на проникновение · SberTech



Артём Комарский

Ведущий специалист · Singleton
Security



Руслан Сафин

Chief Security Systems Engineer
· EPAM Systems



Павел Сорокин

Старший инженер по ИБ ·
«Озон Технологии»



Всеволод Тимофеев

Инженер по информационной
безопасности · Тензор



Евгений Строев

Вирусный аналитик · Group-IB

Приглашённые эксперты и авторские программы



Иван Булавин

Директор по продуктам
Standoff 365 · Positive
Technologies



Антон Кузьмин

ex-CTO Innostage



Bagley

Ментор частных
кибериспытаний ·
действующий топ рейтинга
Standoff



Сергей Зыбнев

Автор интенсива «AI-пентест»
· тимлид пентестеров ·
«Бастион»



Денис Макрушин

Автор интенсива «Защита AI-
агентов» · директор по
продуктам · Яндекс



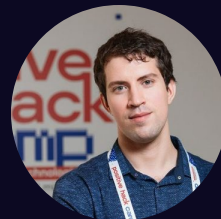
Глеб Михеев

Технический директор
направления генеративного AI ·
Сбер



Егор Зайцев

Автор интенсива «Оценка
устойчивости средств защиты»



Ярослав Шмелев

Старший вирусный аналитик ·
Антивирусная лаборатория



Иван Спиридонов

Senior RedTeam Specialist ·
участник Standoff DreamTeam ·
автор канала FCK HARDER

И сразу — с AI

// главный интенсив потока

«AI-пентест» — интенсив Похека



Сергей «Похек» Зыбнев

тимлид пентестеров в «Бастион»

Собираешь свою команду AI-агентов на полный цикл пентеста: разведка, аудит кода, генерация PoC, автоматизация отчётов. Не «агент взламывает всё сам», а контролируемый AI-пайплайн под свои задачи.

4 семинара

32 ак. часа

удостоверение

Получаешь: рабочий AI-pipeline на весь цикл пентеста, набор промптов и сценариев агентов, PoC-скрипт на основе анализа уязвимости, отчёт по результатам тестирования с AI.

// воркшоп

AI для учёбы

Используешь AI как инструмент прямо в процессе обучения — разбираешь задачи и техники вместе с ним.



// не только поток

AI-воркшопы для всех студентов

Закрытые воркшопы по AI и разным направлениям — доступны всем студентам CyberED.



Первые деньги в профессии — во время учёбы

// модуль · со Standoff Bug Bounty

Bug Bounty Hunter

Компания платит тебе за найденную уязвимость — модуль сделан вместе со Standoff Bug Bounty.

- > Проводишь разведку и готовишь отчёты для триажа — в приватной программе
- > После неё выходишь на открытый рынок Standoff 365

// открывается только участникам потока

Приватный bug bounty

Находишь уязвимость в периметре настоящей компании и сдаёшь за вознаграждение — в закрытой программе потока.

- > Заходишь в программы раньше рынка — конкуренция минимальная
- > Зарабатываешь во время учёбы и проверяешь своих AI-агентов

// открывается только участникам потока

Приватные кибериспытания

Доводишь цепочку атаки до недопустимого события: остановка производства, кража денег, утечка базы — процесс, близкий к red team.

- > Компании-заказчики открывают инфраструктуру и формулируют недопустимое событие для потока
- > Ведут менторы из топа Standoff, среди них Bagley — разбирают ход атаки на созвонах

Все новые интенсивы уже внутри и будут открываться новые

Bug Bounty Hunter

приватная программа триаж

отдельно 25 900 ₽

Разведка, отчёты для триажа, приватная программа.

партнёр · Standoff Bug Bounty

AI-пентест: команда агентов для пентеста

AI-пайплайн разведка → PoC → отчёт

отдельно 60 000 ₽

Команда AI-агентов: разведка, PoC, отчёт.

 **Сергей Зыбнев**
тимлид пентестеров, «Бастион»

Защита AI-агентов

модель угроз MCP

отдельно 60 000 ₽

Модель угроз, полномочия агента, MCP, контроль.

 **Денис Макрушин**
директор по продуктам, Яндекс

 **Глеб Михеев**
Сбер

Оценка устойчивости средств защиты

антивирусы и EDR C2

отдельно 25 500 ₽

Обход антивирусов и EDR, AMSI, работа с C2.

 **Егор Зайцев**
автор интенсива

Обход AppLocker

воркшоп скоро

Воркшоп по обходу ограничений запуска исполняемых файлов.

скоро

Разработка агентных систем

интенсив скоро

Отдельный интенсив по созданию собственных AI-агентов — тему выбрало комьюнити.

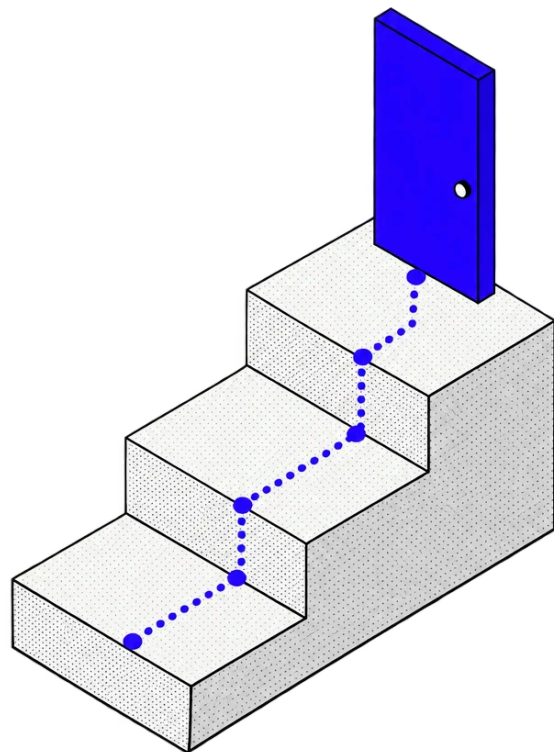
скоро

Карьерная консультация

резюме путь на рынке

Разбираешь свой путь на рынке — что дальше после потока.

включена в поток



// даже если не идёшь в поток

Три шага на рынок — без нас

- 01 Получи навыки
- 02 Собери первого агента
- 03 Найди команду
- 04 Выйди на битву

На Standoff 365 уже есть bug bounty, где зарабатывают, и конкурсы AI-хакеров, где выходят агенты.

Запроси **все материалы** потока

Программу, тарифы и ответы на вопросы пришлют менеджеры в Telegram.

@CyberEd_Russia

telegram · менеджеры CyberED

