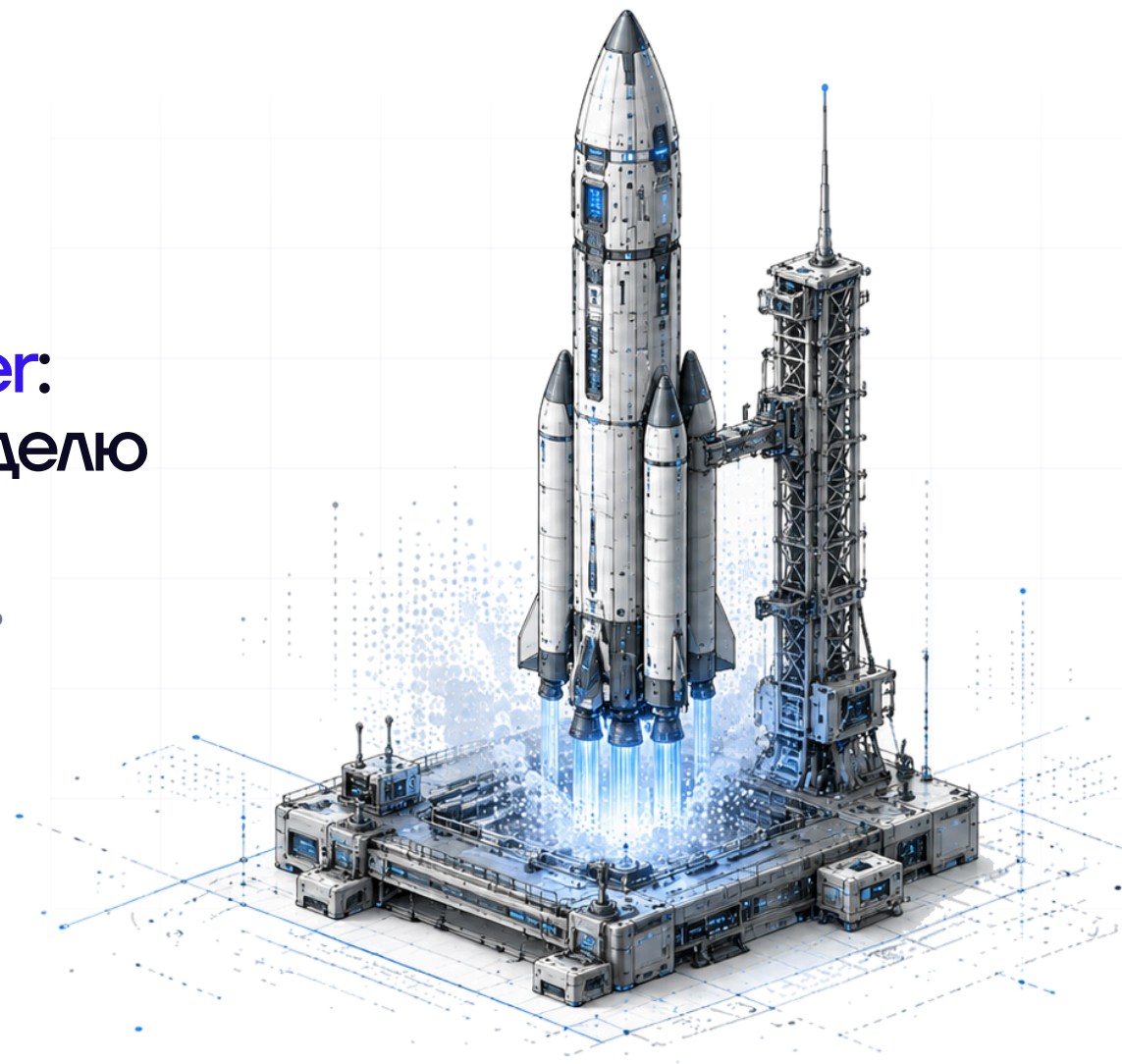


// открытый воркшоп

AI в работе **Security Engineer**: ЭКОНОМИМ **часы** КАЖДУЮ НЕДЕЛЮ

Как новичку в разы быстрее стать
продуктивным: учиться, писать код и решать
задачи по ИБ.

Евгений Строев // Security Expert



// 90 минут • открытый воркшоп



// спикер

Евгений Строев

Security Expert

Показываю, как сам каждый день использую ChatGPT, Claude, Cursor и Claude Code в реальных задачах ИБ.

> **Pentest**

От небольших сервисов до корпоративных инфраструктур

> **Business Information Security**

Изменение процессов, анализ рисков, практическая ИБ

> **Professional Consultation**

virtual-CISO, анализ защищённости, карьерные консультации

4

место на HTB Business CTF 2025–2026
среди 800+ команд мира

Давайте **познакомимся**

А) Отметьте, кто вы и откуда пришли

01 Новичок без ИТ / ИБ бэкграунда

02 Новичок с ИТ-бэкграундом

03 Работаю в ИТ

04 Работаю в ИБ

Б) Какие у вас цели на встречу?

Напишите в чат одним словом — научиться промптить · писать код · автоматизировать рутину · войти в ИБ · разобраться в инструментах · что-то своё

// план встречи

Что разберём

01 Ежедневный ускоритель где AI экономит часы

02 Offensive / CTF AI на HTB CTF

03 Defensive IOC, CVE, детекты

04 Где AI подводит ограничения модели

05 Демо вживую черновик за 5 минут

06 Твоя неделя с AI правила и старт



// только в августе · Нейроавгуст

Нейроавгуст: 2 программы по цене 1

Онлайн-интенсив

Сразу внедрение

Безопасность ИИ-систем и агентов

Внедрять ИИ-агентов в корпоративные процессы: моделировать угрозы, ограничивать полномочия, контролировать работу с данными, API и кодом.



Денис Макрушин

Директор по продуктам безопасной разработки · Яндекс



Глеб Михеев

Разработчик ИИ-помощника · СберБанк

Онлайн-интенсив

Практика

AI-усиленный пентест

Собрать систему ИИ-агентов на полный цикл пентеста — от разведки до отчёта — и протестировать на реальных сценариях багбаунти Standoff 365.



Сергей Зыбнев

R&D AI, Похек



Оставьте заявку у менеджера

2 программы по цене 1 · только до 1 сентября

~~90 000 ₽~~

45 000 ₽

Не замена. Не «будущее». Ускоритель — уже сегодня.

- ✗ замена инженеру
- ✗ «AI — это будущее через пять лет»
- ✗ кнопка, которая делает вас экспертом
- ✗ инструмент только для Senior

- ✓ персональный наставник и ускоритель
- ✓ учит в разы быстрее осваивать новое
- ✓ полезен уже сейчас, на реальных задачах
- ✓ черновик на скорости под вашу проверку



CyberED

AI — черновик. Ты — проверка.

AI даёт скорость. Контекст и проверку
даёте вы — на каждом шаге доклада.

сквозной приём



// с чего начнём · реальная история

AI разобрал незнакомую технологию за 10 минут.
И уверенно выдал **неверное решение**.

Контекст

HTB Business CTF, незнакомый стек под таймером. Читать всю документацию — некогда.

Что помогло

AI дал быстрый mental model и черновик — сэкономил десятки минут исследования.

Где подставил

Один ответ был уверенным и неправильным: несуществующая опция, «галлюцинация» синтаксиса.

Мораль

AI даёт скорость. Проверка — на тебе.

// индустрия согласна

Hack The Box: AI допустим как co-pilot

Официальная позиция — Global Cyber Skills Benchmark 2026.

разрешено как co-pilot

- ✓ Суммаризация логов и кода
- ✓ Генерация команд, скриптов, запросов
- ✓ Брейншторм гипотез
- ✓ Перевод и пояснение документации

вне бенчмарка

- ✗ Автономное решение задач за инженера
- ✗ Работа без проверки человеком

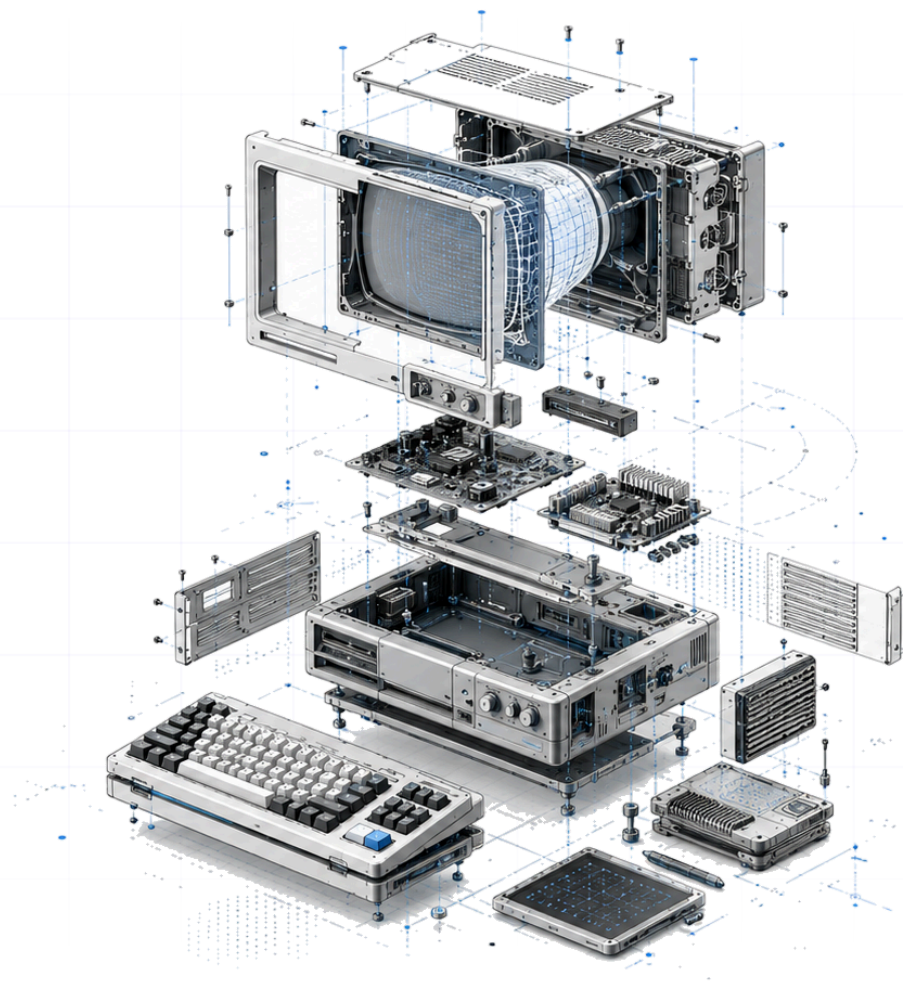
// человек всегда за рулём

// тема 1 • ежедневная работа

Где AI реально ЭКОНОМИТ ЧАСЫ

Сильнее всего — там, где много текста и рутины.

- > Документация и политики безопасности
- > Требования и отчёты
- > Диаграммы и схемы
- > Скрипты и автоматизация рутины
- > Презентации из документов
- > Черновики писем и пересказы встреч



Термины, которые встретятся **дальше**

CTF

Соревнование по практической ИБ: захватываешь «флаги», решая задачи

IOC

Индикатор компрометации: след атаки в логах или системе

YARA / Sigma

Правила для детекта вредоносных и подозрительных событий

threat modeling

Разбор, как и откуда систему могут атаковать

PoC

Proof of Concept: демонстрация, что уязвимость реально работает

CVE

Запись о конкретной публично известной уязвимости

SIEM

Сбор и анализ событий безопасности (например, Splunk)

HTB Business CTF: AI как **напарник**, а не решала

AI не решал за меня — помогал двигаться быстрее.

- > Понять условие задачи
- > Объяснить незнакомый протокол
- > Набросать черновик PoC
- > Составить вызовы к API
- > Разобраться с новой технологией
- > Разобрать ошибку
- > Проанализировать логи
- > Быстро прочесть документацию

На стороне **защиты**

- > Анализ IOC
- > Объяснение чужого PoC
- > Запросы в Splunk
- > Threat modeling
- > Разбор CVE
- > Правила Sigma / YARA
- > Анализ логов
- > Security Review и 3rd-party assessment

Где AI **ПОДВОДИТ**

- › Врёт и уверенно галлюцинирует
- › Придумывает несуществующий API, CVE, флаги
- › Делает не то, что просили
- › Не знает ваш корпоративный контекст
- › Слаб без хорошего промпта

инженер проверяет всегда



// демо • вживую

Черновик презентации за 5 минут

Берём транскрипты 5 встреч по проверке безопасности запуска продукта — и собираем черновик презентации в корпоративном стиле.

что даём AI

- > Транскрипты встреч
- > Требования к структуре и стилю
- > Целевую аудиторию и длительность
- > Свои мысли, идеи, скриншоты

что проверяем сами

- > Факты по первоисточникам
- > Корпоративный контекст
- > Что не вставили ничего чувствительного
- > Выдуманные пункты и «галлюцинации»

Пять шагов демо

шаг 01

Постановка

Даём AI транскрипты и требования к структуре и стилю

шаг 02

Черновик

AI собирает презентацию в корпоративном стиле

шаг 03

Проверка

Сверяем факты, ищем выдуманное, корп-контекст и чувствительное

шаг 04

Доработка

Правим руками до готового вида

шаг 05

Итог

Повторяем приём для отчётов, скриптов и других задач

5 минут вместо
5 дней

5 мин

черновик презентации

20+ ч

экономии на одной
задаче

5 дней

заняло бы ручную



// демо • запасной кейс

Автоматизация: JSON → GDrive за один промпт

Если основное демо не пойдёт — показываем автоматизацию рутины.

шаг 01

Описываем

Задачу словами: разобрать JSON и сохранить результат

шаг 02

Скрипт

AI пишет Python: парсинг JSON по нашим полям

шаг 03

GDrive

Скрипт сохраняет результат в Google Drive

шаг 04

Готово

Файл с данными на диске — потом читаем и тестируем

// скрипт читаем построчно, проверяем на небезопасные паттерны, тестируем

Правила, которые не нарушаем

- 01 Не вставляй секреты, ключи, токены, PII, внутренние конфиги и клиентский код
- 02 Любой AI-код — недоверенный ввод: прочитай, пойми, протестируй
- 03 Проверяй факты (CVE, команды, конфиги) по первоисточникам
- 04 Помни про корпоративный контекст — AI его не знает
- 05 Предполагай prompt injection, когда ввод контролирует кто-то извне
- 06 Человек одобряет всё, что действует (агенты)
- 07 Учись на выводе — не вставляй бездумно, разбирайся

// перед тем как вставить AI-вывод

Чек-лист из 10 пунктов

- [] Сформулировал задачу в 1–2 фразы
- [] Дал модели контекст и ограничения
- [] Не вставил ничего чувствительного
- [] Попросил перечислить допущения и краевые случаи
- [] Протестировал результат
- [] Прочитал и понял каждую строку вывода
- [] Проверил факты по первоисточнику (CVE, флаги, команды)
- [] Учёл корпоративный контекст
- [] Проверил на небезопасные паттерны (TLS, shell, secrets, eval)
- [] Понял решение достаточно, чтобы объяснить коллеге

// стартовые промpts • с чего начать

Пять промpts, с которых стоит **начать**

- > Разбор документации / технологии
- > Черновик кода / скрипта
- > Презентация из документа
- > Проверка идеи / инструмента
- > Ревью безопасности

// каркас любого промпта

Задача: ...

Что даю (контекст): ...

Что НЕ даю (чувствительное): ...

// проси перечислить допущения и краевые случаи

Что сделать уже в ПОНЕДЕЛЬНИК

1 Выбери 1–2 рутинные задачи недели: документация, отчёт, скрипт или презентация

2 Прогони приём: AI — черновик, ты — контекст и проверка

3 Засеки сэкономленное время — это и есть «часы каждую неделю»

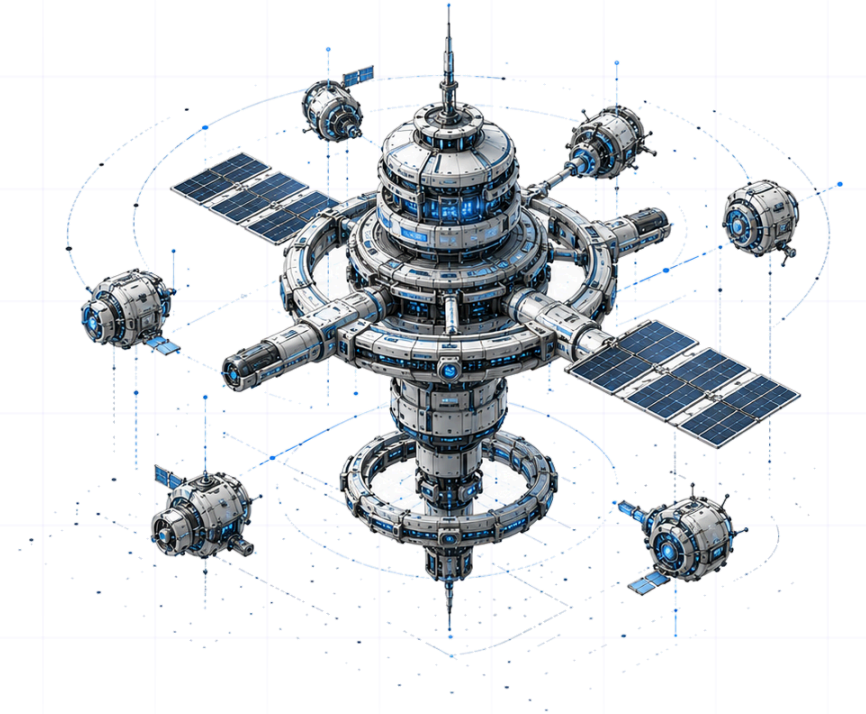
4 Держи рядом чек-лист и применяй его с первого дня

// тема 6 • обучение CyberED

Сегодня — база. Дальше — на обучении CyberED

Сегодня всё под контролем человека: чат, Cursor, Claude Code. Продвинутое — на обучении.

- > AI-агенты и YOLO-режимы: агент действует сам, человек проверяет диффы
- > Мультиагентные системы и оркестрация: рои агентов
- > Скилы и плагины, расширяющие инструменты
- > 3 интерфейса работы с агентами: IDE · Plugin · CLI
- > 8 стадий эволюции программиста 2024–2026 (по Steve Yegge)



// только в августе · Нейроавгуст

Нейроавгуст: 2 программы по цене 1

Онлайн-интенсив

Сразу внедрение

Безопасность ИИ-систем и агентов

Внедрять ИИ-агентов в корпоративные процессы: моделировать угрозы, ограничивать полномочия, контролировать работу с данными, API и кодом.



Денис Макрушин

Директор по продуктам безопасной разработки · Яндекс



Глеб Михеев

Разработчик ИИ-помощника · СберБанк

Онлайн-интенсив

Практика

AI-усиленный пентест

Собрать систему ИИ-агентов на полный цикл пентеста — от разведки до отчёта — и протестировать на реальных сценариях багбаунти Standoff 365.



Сергей Зыбнев

R&D AI, Похек



Оставьте заявку у менеджера

2 программы по цене 1 · только до 1 сентября

~~90 000 ₽~~

45 000 ₽

// твоя неделя с AI

Скорость — от AI. Проверка — от вас.

Сильнее будут не те, кто игнорирует AI, а кто умеет работать вместе с ним.
Начните с одной задачи на этой неделе.

LinkedIn

evgeny-stroev

Telegram

@estroev

// до связи