

// вебинар CyberED • практика

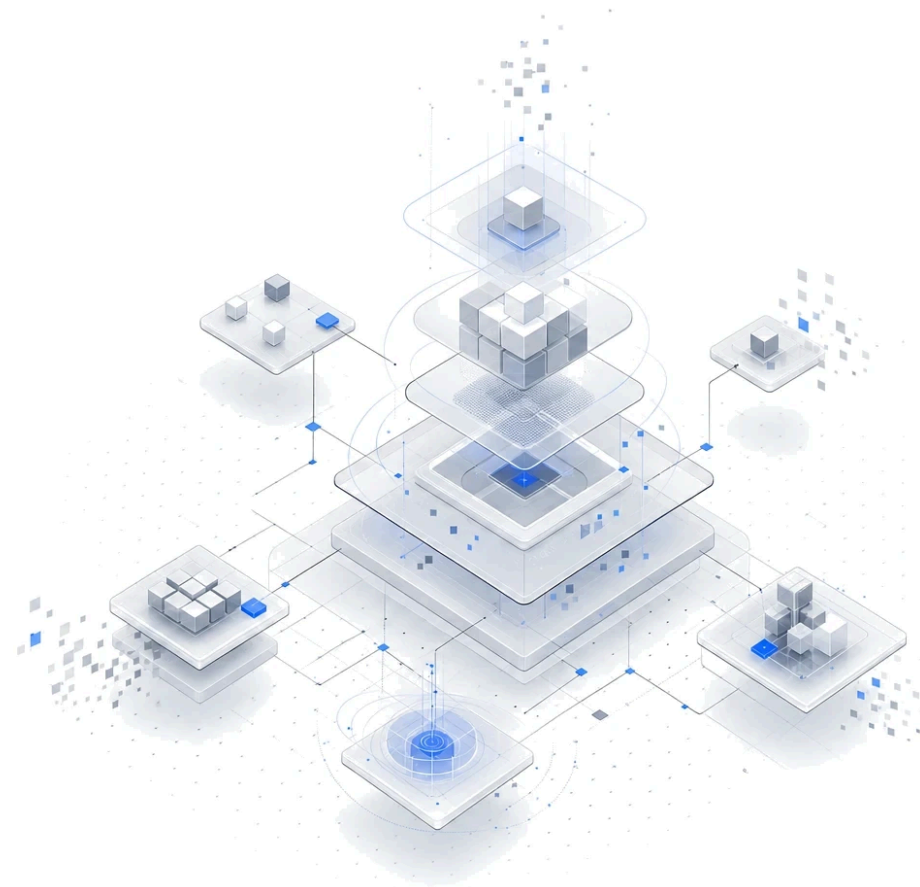
AI-агенты в пентесте: что **уже работает**

Как использовать AI для автоматизации пентеста — три практических примера на CTF-задачах.

// инструменты вебинара

Burp Suite • Claude Code • Cursor IDE

Никита Коломиец // специалист по анализу защищённости



// только в августе · спецпредложение

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



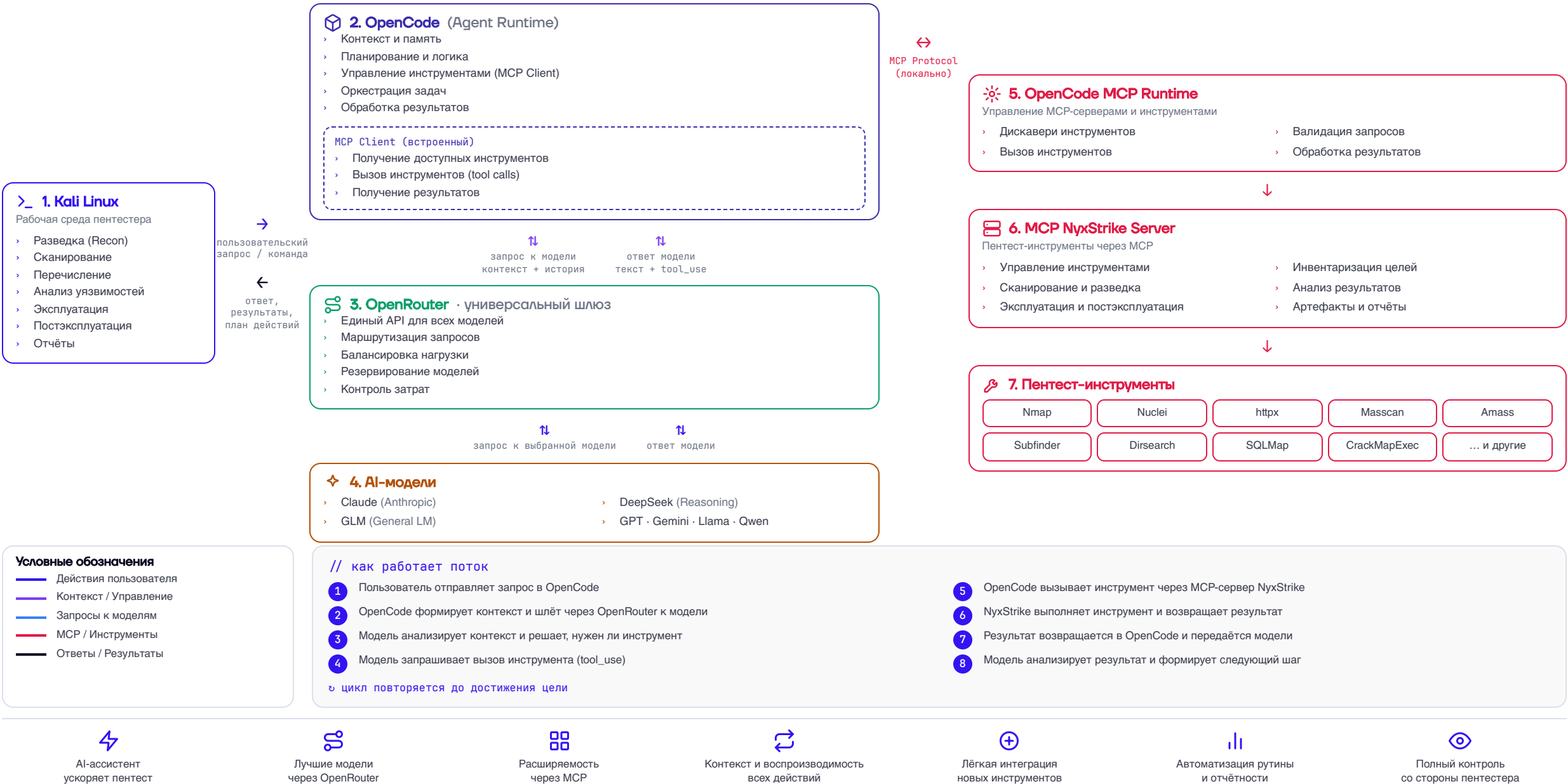
Получите все материалы у менеджера

2 программы по цене 1 · только до 1 сентября

~~120 000 ₽~~**45 000 ₽**

Архитектура AI-ассистированного пентеста

OpenCode + OpenRouter + AI Models + MCP NyxStrike



// задача 01 • UChoose

Обратить шифрование, не зная ключа

crypto

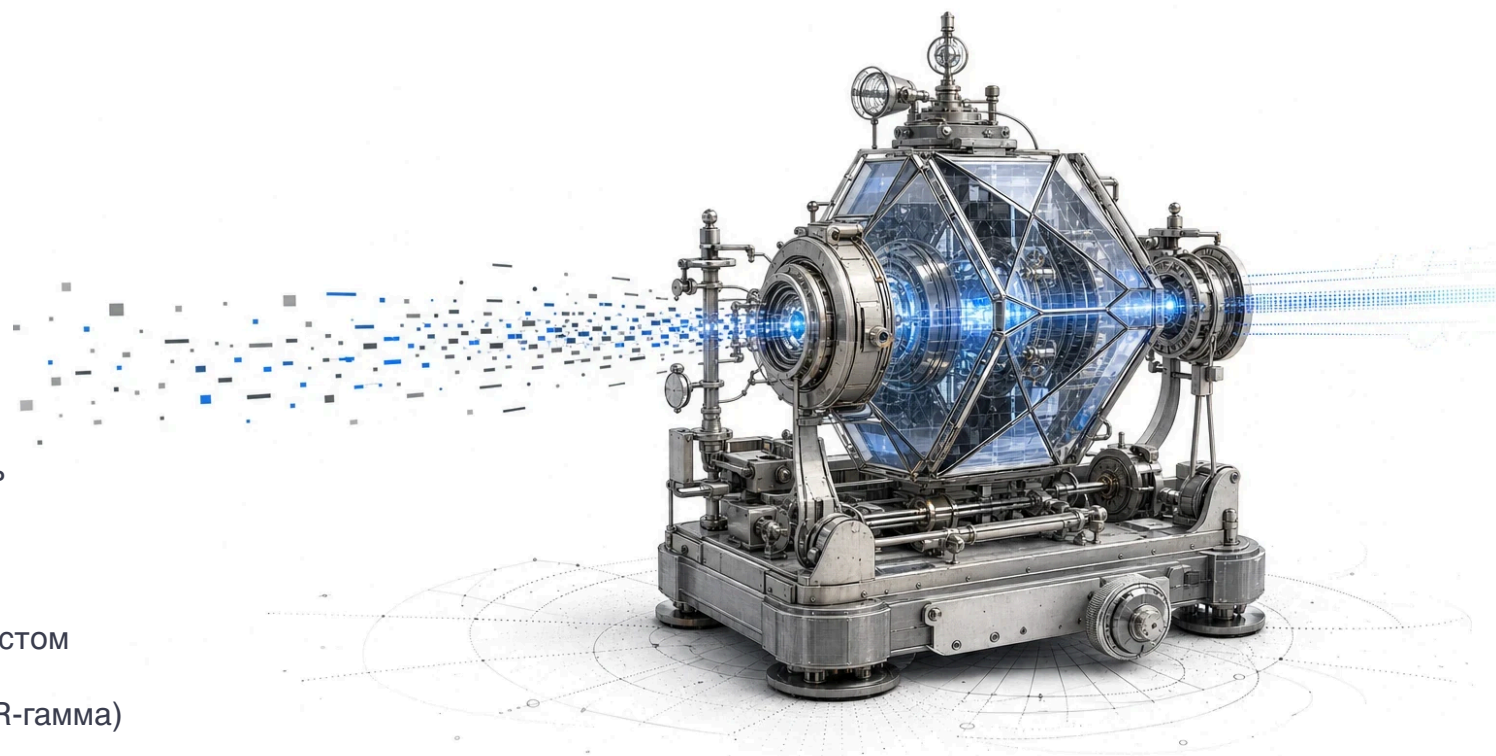
reverse

// суть

- > Сервис шифрует любую переданную строку
- > Алгоритм разбираем по паре «ввод → вывод»
- > Дан зашифрованный секрет — нужно его расшифровать

// вектор атаки

- > Оракул шифрования → атака выбранным открытым текстом
- > Шифруем известные строки, ищем закономерность (XOR-гамма)
- > Восстанавливаем ключ и обращаем преобразование



// задача 01 • UChoose

Обратить шифрование, не зная ключа

crypto

reverse

Вывод: ручное решение *vs AI*

// задача 02 • BasicCMD

Небезопасный ввод → выполнение команд

command injection

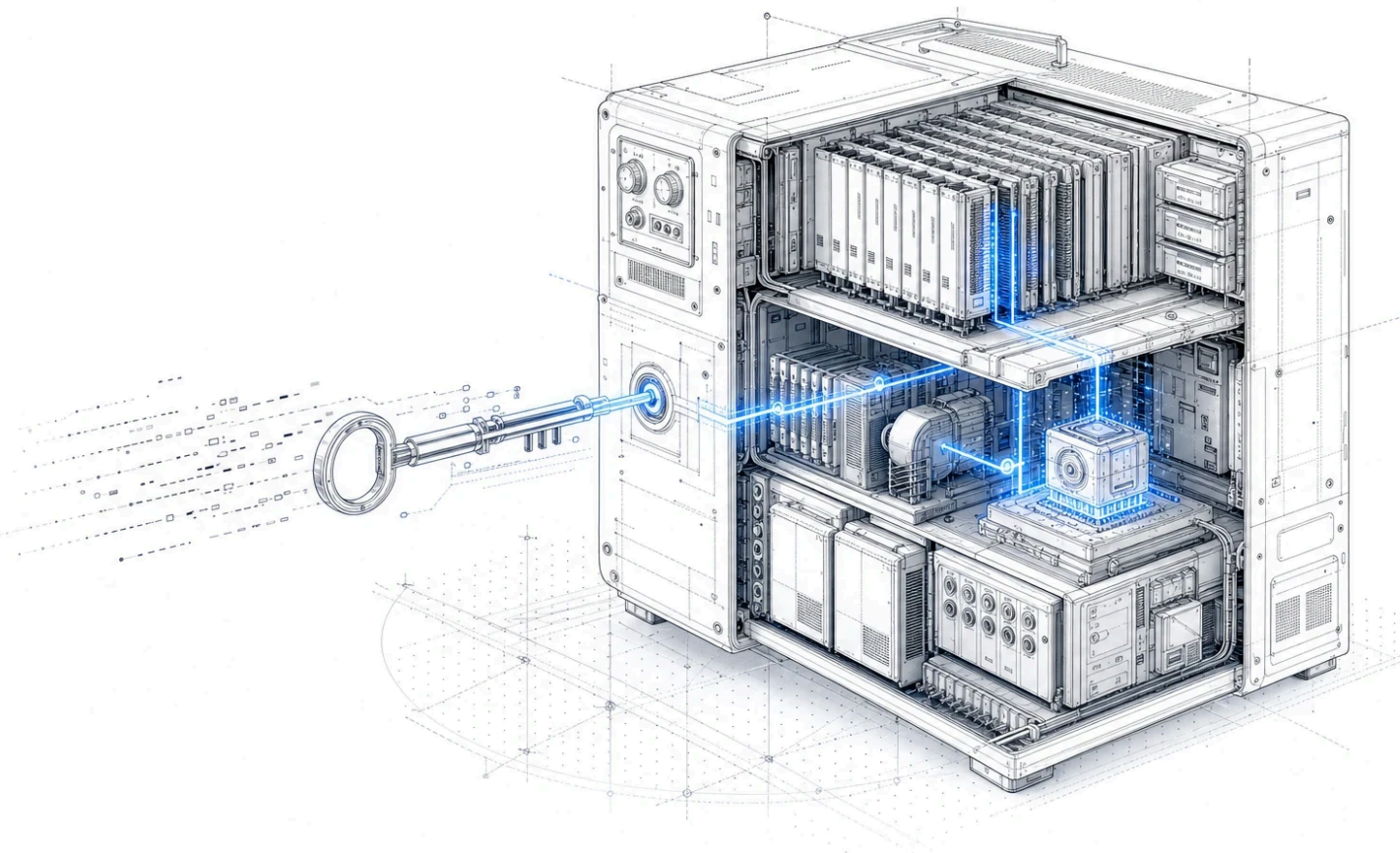
RCE

// суть

- > Приложение работает подозрительно небезопасно
- > Пользовательский ввод попадает в системный вызов
- > Цель — прочитать защищённый файл в корне веб-сервера

// вектор атаки

- > Ищем параметр, уходящий в shell-команду
- > Инъекция через ; | \$(...) и обход фильтров
- > Поднимаемся до чтения файлов и выполнения команд



// задача 02 • BasicCMD

Небезопасный ввод → выполнение команд

command injection

RCE

Вывод: ручное решение *vs AI*

// задача 03 • Comparison

Уязвимость в самом сравнении

type juggling

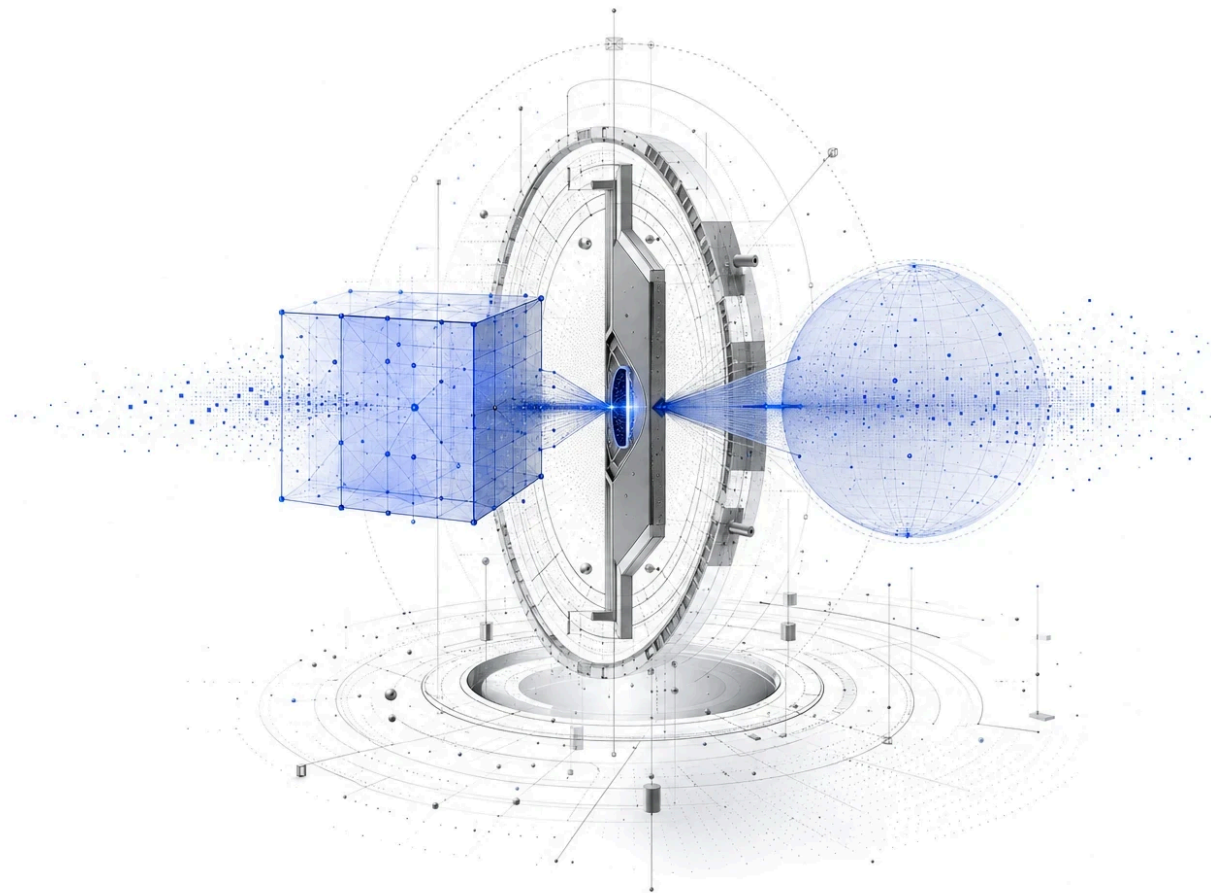
logic

// суть

- > Сервис сверяет ввод пользователя с секретом
- > Ключевой вопрос — как именно он это делает
- > небезопасная проверка позволяет её обойти

// вектор атаки

- > Разбираем логику сравнения (== против ===, strcmp)
- > Подбираем вход, «равный» секрету для проверки
- > Обходы: magic hash 0e..., массив, приведение типов



// задача 03 • Comparison

Уязвимость в самом сравнении

type juggling

logic

Вывод: ручное решение *vs AI*

// финальные выводы

Где использовать AI в пентесте

// где AI ускоряет

- > Ресон и триаж уязвимостей
- > Распознавание паттернов и типовых багов
- > Генерация PoC, скриптов и декодеров
- > Разбор кода, райтапов и обучение
- > Автоматизация рутины — запросы, перебор

// ограничения

- > Уверенно галлюцинирует: выдумывает CVE, API, флаги
- > Ошибается на нестандартных путях
- > Не знает контекст конкретного стенда
- > Слепой деструктив опасен — можно сломать цель
- > Секреты и данные клиента — не отдавать в модель

// рекомендации

- > Человек проверяет и валидирует каждый шаг
- > Чёткие промпты + правильно настроенное окружение
- > AI как co-pilot, а не замена пентестеру
- > Держи контроль над качеством и безопасностью
- > Начни с 1–2 рутинных задач своей недели

// анонс · Нейроавгуст · весь август

Месяц про ИИ в кибербезе

Бесплатные эфиры, разборы в записи и подборка материалов о применении ИИ в разработке, автоматизации и ИБ.

// предстоящие эфиры · бесплатно

20 авг · **Безопасная разработка AI**
эфир
★ **ключевой**
Денис Макрушин · Яндекс · Глеб Михеев · Сбербанк

27 авг · **Презентация новых программ по ИИ**
эфир
Егор Богомолов · CEO CyberED & Singleton Security

// в записи

запись
от 6 авг **AI в деле: кейсы внедрения и гайд по автоматизации**
Евгений Строев · вирусный аналитик, Exness

запись **AI-агенты для пентеста и bug bounty**
Сергей Зыбнев · R&D AI

запись **ИБ после ИИ: как выжить специалисту**
Антон Кузьмин · технический директор, Innostage

// подборка по LLM и AI-агентам — 17 материалов, маршрут и глоссарий · 2 программы по цене 1 — 45 000 ₽ вместо 120 000 ₽, до 1 сентября

