

Цена лишнего факта: как неосознанные утечки бьют по прибыли

Александр Анашин



Кто я?



Александр Анашин (DAFFIER)

Пентестер, автор блога «Пентестер на мотоцикле» в Telegram



Специализируюсь на безопасности внешнего периметра, API, облаков, WEB и мобильных приложений

Ранее выступал с техническим докладом о распространённых уязвимостях в веб-приложениях

Взаимодействие с другими людьми приносит мне радость



Лишний факт = Новая точка атаки

Атака = Прямые деньги

«Лишний факт»

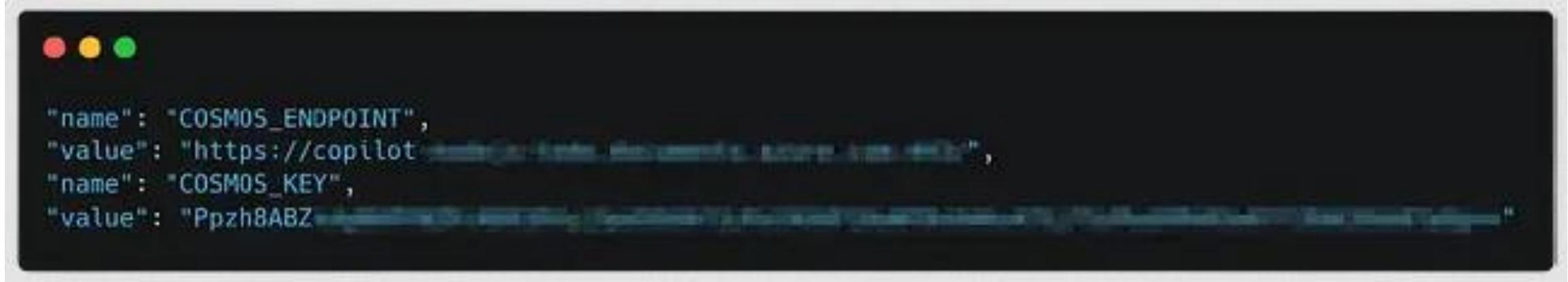
- Персональные данные
- Финансовая и платёжная информация
- Учётные данные и доступ
- Коммерческая тайна
- Техническая и инфраструктурная информация
- И многое другое...



Статистика Алексея Парфентьева, заместителя генерального директора по инновационной деятельности «СёрчИнформ», за 2024 год

Что такое «лишний факт» и где он появляется

Утечка технических данных в конфигурационных файлах

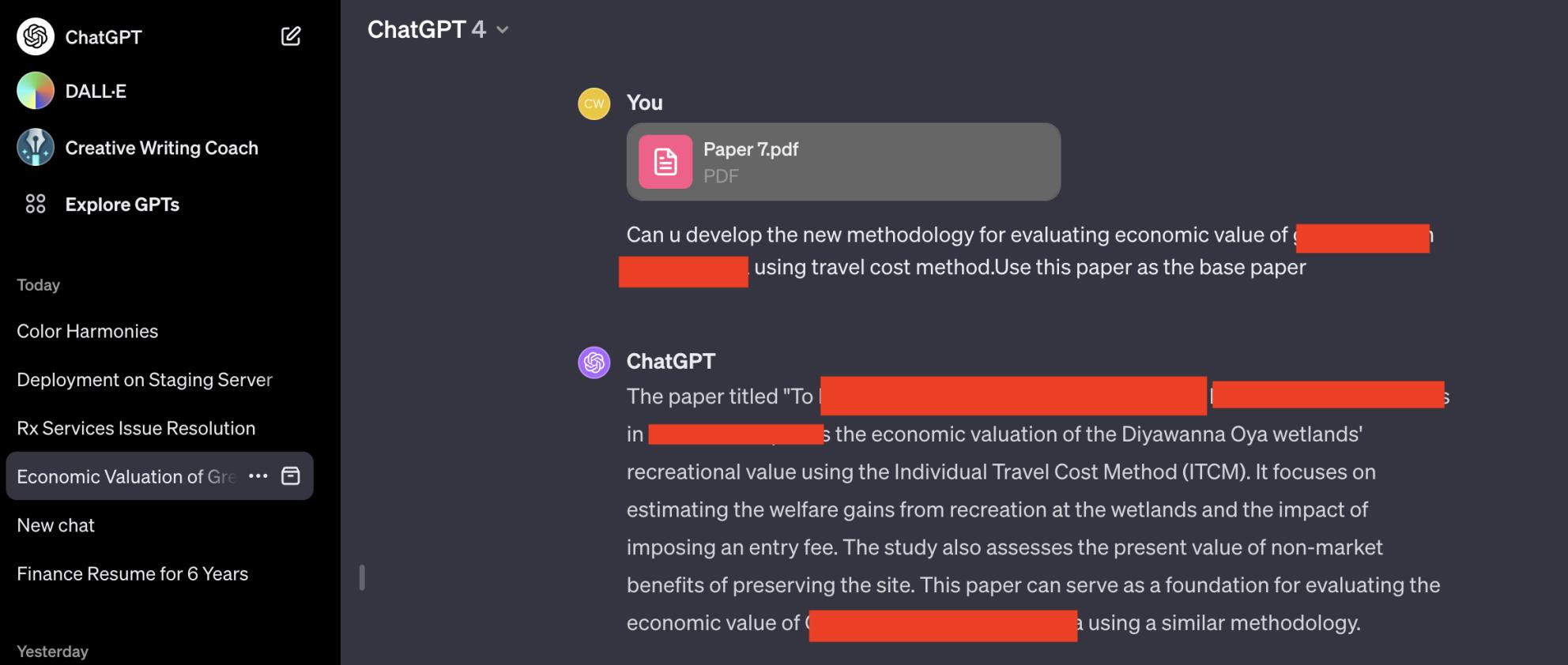


A screenshot of a terminal window with a dark background and light-colored text. The window has the standard OS X title bar with red, yellow, and green buttons. The terminal content shows two configuration entries:

```
"name": "COSMOS_ENDPOINT",  
"value": "https://copilot",  
"name": "COSMOS_KEY",  
"value": "Ppzh8ABZ"
```

The URL in the second entry is partially obscured by a redacted line.

Утечка коммерческой тайны в ИИ-чатах



ChatGPT 4

You

Paper 7.pdf
PDF

Can u develop the new methodology for evaluating economic value of [REDACTED]
[REDACTED] using travel cost method. Use this paper as the base paper

ChatGPT

The paper titled "To [REDACTED] [REDACTED]"
in [REDACTED] the economic valuation of the Diyawanna Oya wetlands'
recreational value using the Individual Travel Cost Method (ITCM). It focuses on
estimating the welfare gains from recreation at the wetlands and the impact of
imposing an entry fee. The study also assesses the present value of non-market
benefits of preserving the site. This paper can serve as a foundation for evaluating the
economic value of [REDACTED] using a similar methodology.

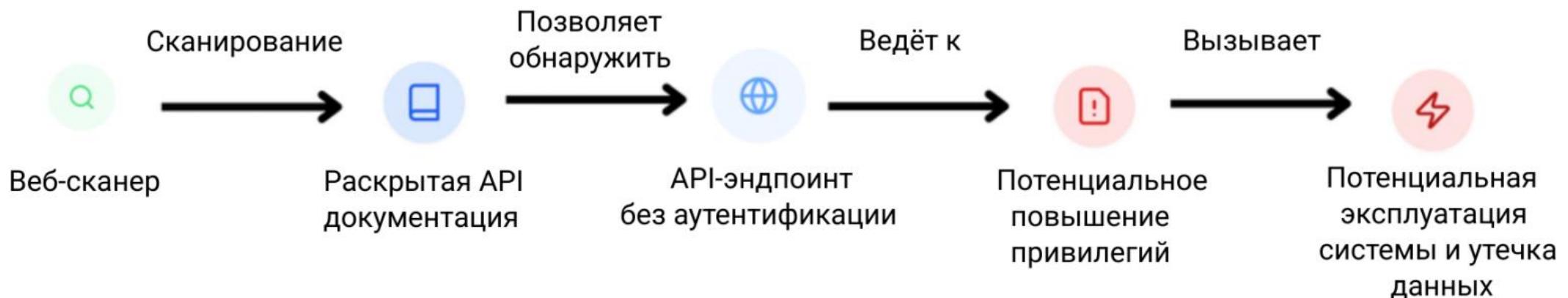
Утечка технических данных в вакансиях

Наш стек:

- PHP 8.1. Существуют сервисы версии ниже, примерно 7.4, но ониrudиментарные, либо находятся на рефакторинге;
- Python 3.8+;
- C++ 18+;
- JavaScript + TypeScript;
- Kotlin 1.9.22;
- Swift 5;
- PostgreSQL 15;
- Kafka, Redis, Memcached;
- Kubernetes, Docker.



«Лишний факт» на примере



Открытые API, просочившиеся токены: как гигант полупроводников почти был взломан

<https://www.cloudsek.com/blog/exposed-apis-leaked-tokens-how-a-semiconductor-giant-almost-got-breached>

Почему любая утечка = деньги

Почему любая утечка = деньги

Ускоряет
подготовку
атаки

Увеличивает
операционные
издержки на защиту

Сложение мелких утечек
формирует критический
риск

Снижает устойчивость
бизнеса и создаёт
конкурентные риски

Несёт юридические
и репутационные потери



Почему любая утечка = деньги

Comcast to pay \$1.5 million US fine after vendor data breach

Jaguar Land Rover cyberattack nears £2bn in UK's costliest hack

South Korea agency fines SK Telecom \$97 million over major data leak

Co-op takes £206mn revenue hit from cyber attack

Data breach at MGM Resorts expected to cost casino giant \$100 million

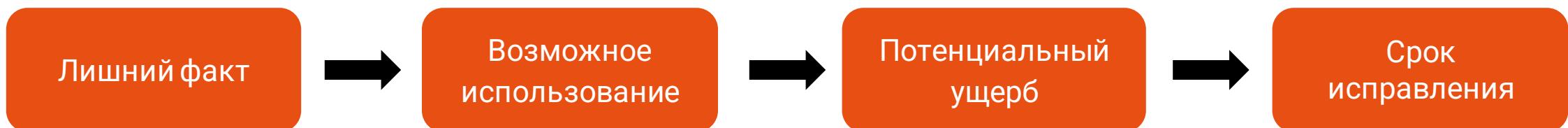
\$700 Million Equifax Fine Is Still Too Little, Too Late

Что должен делать бизнес

Провести бизнес-инвентаризацию фактов

Что входит:

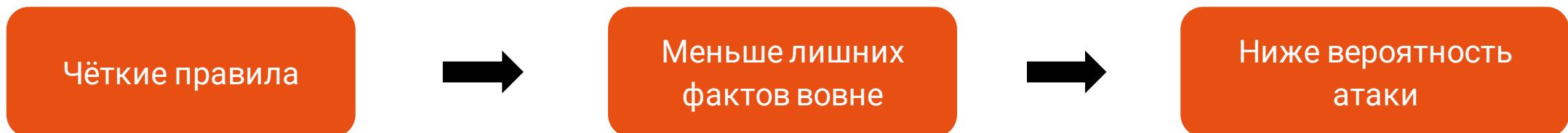
- Проверить код и репозитории
- Пересчитать домены и поддомены
- Выявить утечки конфигов и ключей
- Найти следы компании в публичных источниках



Встроить политику минимальности фактов в бизнес-процессы

Что входит:

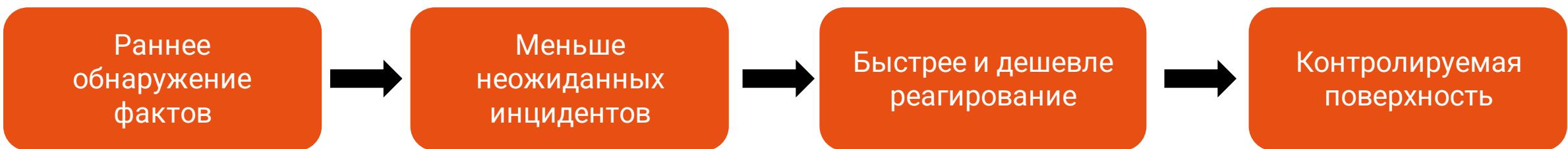
- Без лишних деталей вовне
- Проверка материалов
- Гигиена инфраструктуры
- Осознанный обмен данными
- Точка контроля



Создать регламент раннего выявления утечек

Что входит:

- Определить ответственного
- Вести регулярный отчёт по фактам
- Установить жёсткие сроки реакции



В итоге



**ДЕЛЯСЬ ЗНАНИЯМИ,
ПОЛУЧАЕШЬ БОЛЬШЕ**

