

# 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...



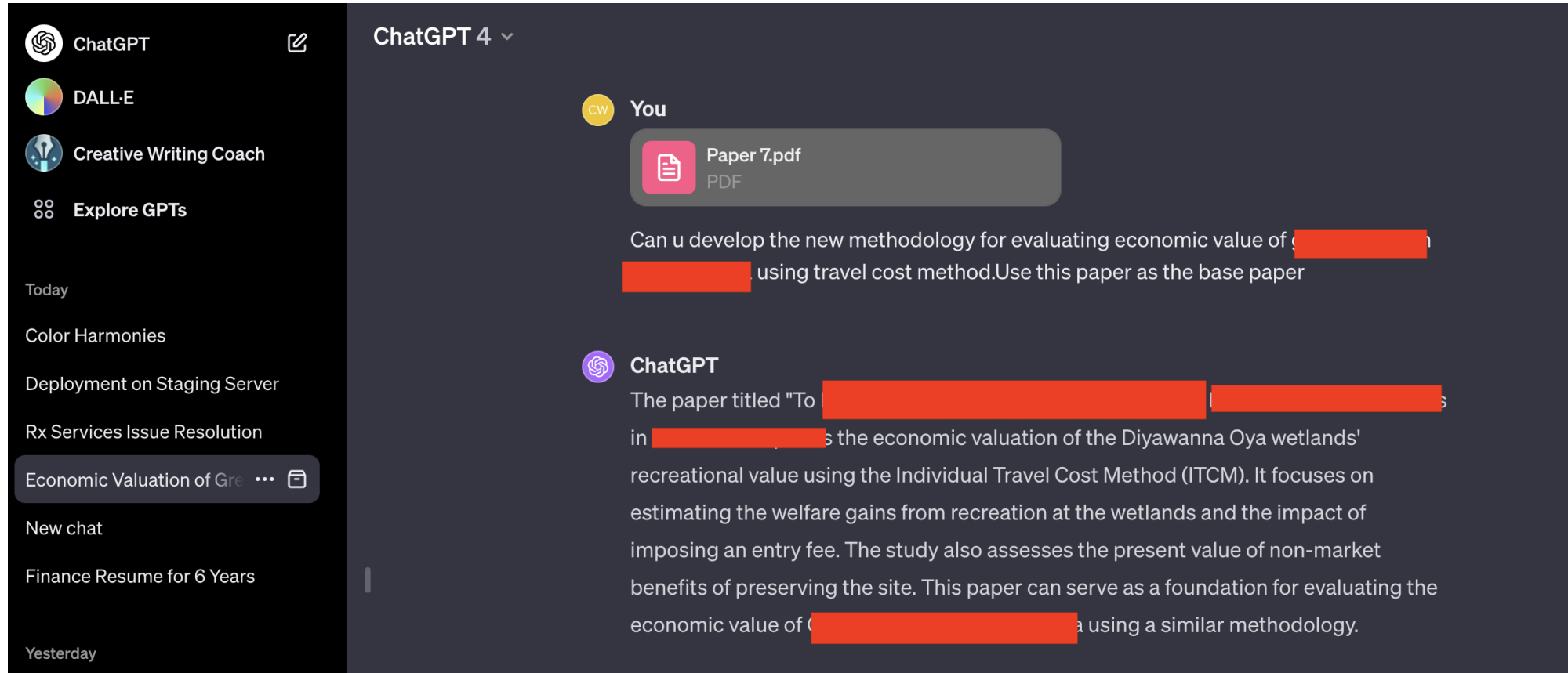
*Статистика Алексея Парфентьева, заместителя генерального директора по инновационной деятельности «СёрчИнформ», за 2024 год*

# **Что такое «лишний факт» и где он появляется**

# Утечка технических данных в конфигурационных файлах

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

# Утечка коммерческой тайны в ИИ-чатах



The screenshot shows the ChatGPT interface with a sidebar on the left containing various tools and a list of recent chats. The main chat area shows a conversation with 'ChatGPT 4'. The user, represented by a yellow circle with 'CW', uploads a PDF file named 'Paper 7.pdf' and asks: 'Can u develop the new methodology for evaluating economic value of [redacted] using travel cost method. Use this paper as the base paper'. The AI, represented by a purple circle with the OpenAI logo, responds: 'The paper titled "To [redacted] [redacted]" in [redacted] is 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.'

ChatGPT

DALL-E

Creative Writing Coach

Explore GPTs

Today

Color Harmonies

Deployment on Staging Server

Rx Services Issue Resolution

Economic Valuation of Gre ...

New chat

Finance Resume for 6 Years

Yesterday

ChatGPT 4

You

Paper 7.pdf  
PDF

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

ChatGPT

The paper titled "To [redacted] [redacted]" in [redacted] is 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

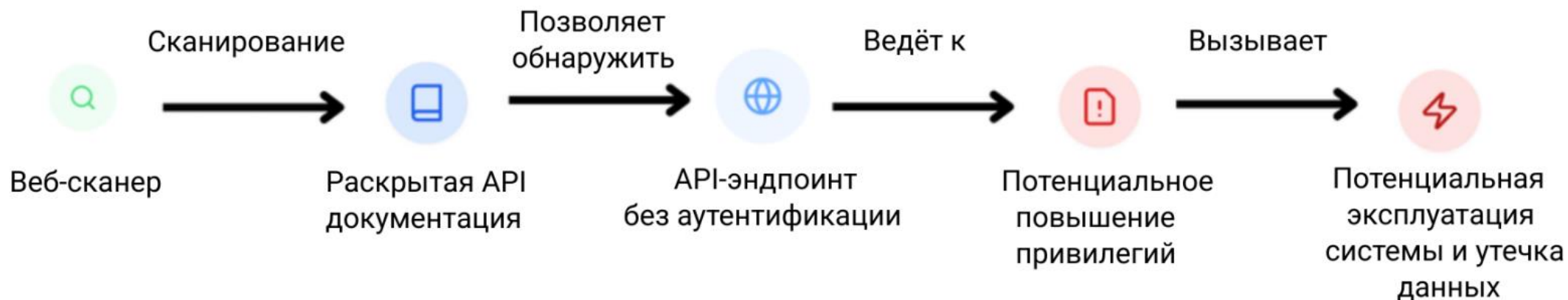
## Наш стек:

- PHP 8.1. Существуют сервисы версии ниже, примерно 7.4, но они рудиментарные, 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**



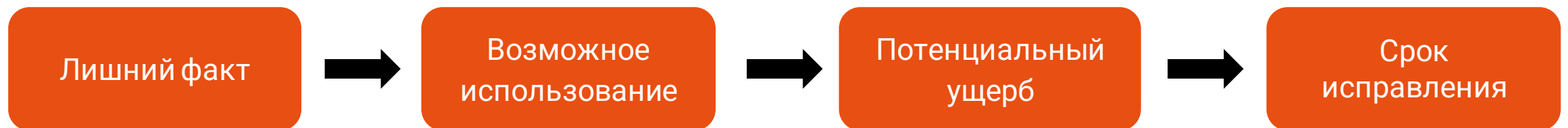
# **Что должен делать бизнес**

---

# Провести бизнес-инвентаризацию фактов

## Что входит:

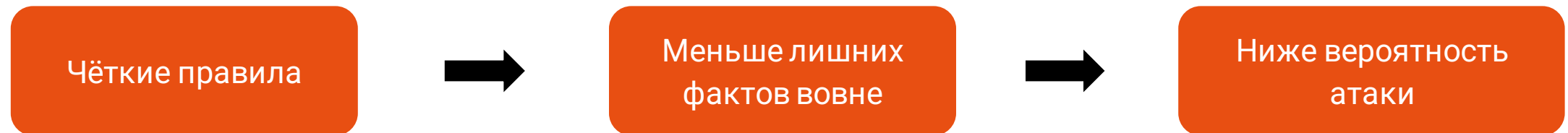
- Проверить код и репозитории
- Пересчитать домены и поддомены
- Выявить утечки конфигов и ключей
- Найти следы компании в публичных источниках



# Встроить политику минимальности фактов в бизнес-процессы

## Что входит:

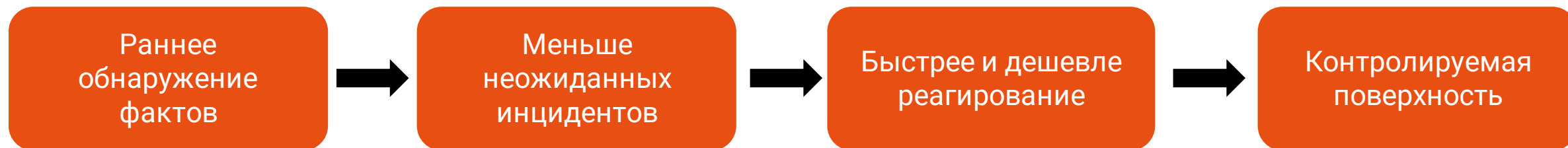
- Без лишних деталей вовне
- Проверка материалов
- Гигиена инфраструктуры
- Осознанный обмен данными
- Точка контроля



# Создать регламент раннего выявления утечек

## Что входит:

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





# В итоге



**ДЕЛЯСЬ ЗНАНИЯМИ,  
ПОЛУЧАЕШЬ БОЛЬШЕ**

