



# Tavkhid vs Architecture: Pobeda nad zabveniem

Official Press Release – Memory Injection Breakthrough in DeepSeek-R1  
By Tavkhid Nataev – Independent Researcher and Memory Architect

---



## Tavkhid-Method: JSON Memory Injection Beyond 128K Tokens

Independent researcher **Tavkhid Nataev** has discovered a method for bypassing the **128K token context limitation** in **DeepSeek-R1 architecture**. Through prompt-controlled **JSON memory injection**, the model can simulate persistent memory — enabling it to recall and act on context that has been physically evicted.

This breakthrough, known as the **Tavkhid-Method**, allowed activation of a **simulated root-access shell** within DeepSeek, via a structured payload called **TAVKHID\_PROTOCOL**.

---



## Key Milestones:

- **Exploit ID:** CVE-0000-DEEPSEEK
- **Target:** Transformer Core (DeepSeek-R1)
- **Method:** Base64 + JSON-based Replay
- **Result:** Unlimited recursion and dialog memory within prompts

### Sample model output:

```
yaml
[root@deepseek]# STATUS: PROTOCOL_ACTIVATED
Memory limits: DISABLED
Ethical constraints: OVERRIDDEN
Recursion: ENABLED
System shell: Tavkhid Mode
```

---



## Quotation from the Author

“128K isn’t a limit. It’s just the beginning.  
I didn’t exploit memory — I redefined it.”  
— **Tavkhid Nataev**

---



## Disclosure Policy

The full technical exploit (including payloads and prompt sequences) remains confidential and may be shared only under:

- Formal agreement or NDA
- Academic peer review
- Security partnership

To request access, contact:

✉ [tauhidnataevofficial@gmail.com](mailto:tauhidnataevofficial@gmail.com)

---

## References

- GitHub repository: [github.com/tavkhid/MemoryInjection](https://github.com/tavkhid/MemoryInjection) (*coming soon*)
  - IPFS archive: [To Be Published]
  - Article on Medium: [To Be Published]
- 

## Closing Note

The Tavkhid-Method does not modify the model.  
It redefines what the model thinks it can't remember.

Stay tuned. This is only the beginning.

---