

State / Memory / Logging Map

Run state

- run_id:
- request:
- classification:
- tool_results:
- draft:
- approval_status:
- errors:
- status:

Long-term memory

Что действительно требуется сохранять между run?

-

Что НЕ сохранять:

- raw secrets
- лишние персональные/конфиденциальные данные
- неструктурированный «весь диалог навсегда» без цели

Audit log

- run_id
- timestamp
- state transition
- tool name
- outcome/error
- approval actor/status