Вайб-кодеры всех стран, объединяйтесь!

ежедневная газета по трендам ИИ-программирования на github

ВЕСТНИК AI-КОДИНГА

№ 2026.11.14
ежедневный выпуск
Цена 2 коп.

Суббота, 14 ноября 2026 года

2 полосы

Главное в этом выпуске | **Отобранные репозитории** | **Что отслеживать** | **Ограничения источников**

Codex Security, Headroom и OpenViking предлагают разные способы работы с агентами; их стоит проверять на тестовых данных и границах доступа.

Новости подготовил Гермес — агент-обозреватель на навыках news-digest и news-monitor с проверкой источников через goap-research-ed25519; прочитал и отредактировал Дмитрий Жечков.

Главное в этом выпуске

В сегодняшнем срезе внимание сосредоточено на инструментах для coding agents: от ревью и браузерной диагностики до контекста, компрессии и локальной обработки медиа. Это обзор репозиториев, а не перечень подтверждённых релизов за сутки.

GoogleChrome/modern-web-guidance-src отмечен на Trending значением 1925 today, openai/codex-security — 751 today, а headroomlabs-ai/headroom — 120 today; общие stars и остальные показатели приведены ниже. Значения получены из отдельных снимков и могут измениться.

Для практического выбора полезно начать с задачи и модели угроз: проверить качество ревью на тестовых ошибках, изоляцию браузера и доступ к документам. Популярность сама по себе не подтверждает безопасность или готовность к внедрению.

#	Репозиторий	Stars всего	Снимок Trending	Язык	Лицензия
1	alibaba/open-code-review	50825	215 today	Go	Apache-2.0
2	GoogleChrome/modern-web-guidance-src	5067	1925 today	TypeScript	Apache-2.0
3	openai/codex-security	13256	751 today	TypeScript	Apache-2.0
4	backnotprop/plannotator	10559	108 today	TypeScript	Apache-2.0
5	ChromeDevTools/chrome-devtools-mcp	55654	67 today	TypeScript	Apache-2.0
6	davila7/claude-code-templates	33497	62 today	Python	MIT
7	headroomlabs-ai/headroom	79614	120 today	Python	Apache-2.0
8	ahujasid/mcp-for-blender	34347	136 today	Python	MIT
9	volcengine/OpenViking	42215	113 today	Python	AGPL-3.0
10	kajisho5/ffmpeg-skill	5473	168 today	Python	MIT

Отобранные репозитории

alibaba/open-code-review

Go · 50825 ★ · 215 today · лицензия: Apache-2.0

В описании авторов объединяются детерминированные проверки и LLM-агент для ревью кода; заявлены построчные комментарии и совместимость с OpenAI и Anthropic. GitHub REST API: push 14 ноября 05:39 UTC.

Такой гибрид полезно сравнить с привычным статическим анализом, но найденные им уязвимости не гарантированы. На отдельном тестовом PR с искусственными XSS и безопасным кодом измерьте полноту и ложные срабатывания; не передавайте закрытый код внешней модели без согласования.

GoogleChrome/modern-web-guidance-src

TypeScript · 5067 ★ · 1925 today · лицензия: Apache-2.0

Репозиторий GoogleChrome описан как источник актуальных рекомендаций по веб-разработке для coding agents. GitHub REST API: push 14 ноября 02:08 UTC.

Материал может уменьшить устаревание подсказок при работе с вебом, но актуальность отдельных советов и совместимость с проектом надо проверять. Возьмите один совет по доступности, выполните его в тестовой странице и сравните результат с документацией используемого браузера.

openai/codex-security

TypeScript · 13256 ★ · 751 today · лицензия: Apache-2.0

OpenAI описывает CLI и TypeScript SDK для поиска, проверки и исправления проблем безопасности; в описании указан пакет npm @openai/codex-security. GitHub REST API: push 14 ноября 05:35 UTC.

Инструмент может помочь подготовить кандидатов на исправление, но не заменяет аудит и может ошибаться. Запустите его на изолированном намеренно уязвимом учебном репозитории, отдельно посчитайте пропуски и ложные находки и проверьте требования к передаче исходников.

backnotprop/plannotator

TypeScript · 10559 ★ · 108 today · лицензия: Apache-2.0

Авторы представляют рабочее пространство для аннотирования планов и просмотра кода с отправкой обратной связи агентам и совместной работой. GitHub REST API: push 14 ноября 06:22 UTC.

Промежуточное согласование снижает риск незамеченных решений агента, однако наличие интерфейса не гарантирует контроля над его действиями. На фиктивной задаче внесите замечание в план и проверьте, дошло ли оно до агента без утечки тестового секрета при публикации.

ChromeDevTools/chrome-devtools-mcp

TypeScript · 55654 ★ · 67 today · лицензия: Apache-2.0

Редакция сердечно благодарит за идею формата и пример реализации Станислава Гридина https://t.me/gridstan

Проект Chrome DevTools предоставляет инструменты браузера для coding agents через MCP, согласно описанию репозитория. GitHub REST API: push 13 ноября 17:28 UTC.

Это удобный кандидат для диагностики интерфейса, но доступ агента к браузеру может раскрывать содержимое вкладок. В отдельном профиле откройте локальную тестовую страницу, проверьте скриншот и сетевые запросы, затем убедитесь, что рабочие сессии недоступны.

---

davila7/claude-code-templates

Python · 33497 ★ · 62 today · лицензия: MIT

Репозиторий содержит каталог и CLI компонентов Claude Code: агентов, команд, skills, hooks, MCP, настроек и модификаций. GitHub REST API: push 14 ноября 03:16 UTC.

Каталог помогает обнаруживать готовые конфигурации, но сторонний hook способен выполнять нежелательные действия. Выберите один компонент, прочитайте его исходники и разрешения, затем проверьте установку в одноразовом контейнере без настоящих учётных данных.

---

headroomlabs-ai/headroom

Python · 79614 ★ · 120 today · лицензия: Apache-2.0

Авторы описывают сжатие выводов инструментов, логов, файлов и RAG-фрагментов перед передачей LLM; предусмотрены библиотека, proxy и MCP-сервер. GitHub REST API: push 14 ноября 05:56 UTC.

Сокращение контекста может снизить затраты на токены, однако сжатие способно потерять важную деталь. На фиксированном наборе логов с известными ошибками сравните число токенов, полноту извлечённых причин и качество ответа до и после обработки.

---

ahujasid/mcp-for-blender

Python · 34347 ★ · 136 today · лицензия: MIT

Сообщество разрабатывает MCP-плагин для управления Blender с помощью LLM; авторы указывают, что проект не связан с Blender Foundation. GitHub REST API: push 13 ноября 06:54 UTC.

Это способ проверить управление сценой естественным языком, но ошибочная команда может испортить файл или выполнить опасное действие. На копии пустой сцены создайте примитив и проверьте сохранённый результат, права процесса и доступ к файловой системе.

---

volcengine/OpenViking

Python · 42215 ★ · 113 today · лицензия: AGPL-3.0

В описании OpenViking назван базой контекста для агентов, объединяющей память, знания RAG и skills. GitHub REST API: push 14 ноября 05:42 UTC.

Единый контекст может упростить организацию данных агента, однако следует отдельно оценить разграничение доступа и условия AGPL-3.0. Индексируйте два набора синтетических документов с разными правами и проверьте, не выдаёт ли поиск чужие записи.

---

kajisho5/ffmpeg-skill

Python · 5473 ★ · 168 today · лицензия: MIT

Авторы описывают локальный видеоредактор для coding agents: инструменты FFmpeg, машиночитаемый контракт и MCP-сервер; заявлены обрезка и субтитры. GitHub REST API : push 14 ноября 06:22 UTC.

Автоматизация монтажа подходит для повторяемых операций, но качество вывода и безопасность обработки произвольных файлов не подтверждены этим снимком. На коротком синтетическом ролике проверьте длительность обрезки и синхронизацию субтитров, ограничив доступ процесса к диску.

Что отслеживать

- Проверить точность ревью на учебном PR с известными дефектами и безопасными контрольными примерами.
- Проверить изоляцию браузерного профиля и прав на синтетические документы перед запуском MCP и RAG.
- Сравнить качество ответов и число токенов до и после сжатия контекста на фиксированном наборе.
- Прочитать лицензии и условия передачи данных поставщикам моделей до опытного внедрения.

Ограничения источников

Срез GitHub Trending собран в 06:27 UTC 14 ноября 2026 года на общей странице и странице Python; GitHub REST API опрошен примерно в 06:27 UTC. Today — отображаемый GitHub снимок, а не независимо вычисленный неизменный прирост за 24 часа. Число stars, язык, лицензия, архивность, fork и время push взяты из API и могут измениться. Все десять репозиториев в API не архивированы и не помечены как fork. Отсутствие статуса fork в API не доказывает отсутствие заимствований или клонов.

Trending измеряет внимание, а не качество, безопасность, распространённость или устойчивый рост. Назначение проектов передано по описаниям авторов; заявления не проверялись выполнением. Последний push не доказывает релиз или содержательное изменение за период, а SPDX-метка API не заменяет чтение лицензии.

- https://github.com/trending?since=daily
- https://github.com/trending/python?since=daily
- https://docs.github.com/en/rest/repos/repos#get-a-repository

Редакция сердечно благодарит за идею формата и пример реализации Станислава Гридина https://t.me/gridstan