PYTHON · POWERSHELL · ИИ-АГЕНТЫ

Парк read-only агентов на своём ПК

как ИИ ищет заказы и не даёт натворить дел

Десять задач по расписанию, права только на чтение и тормоз на саморазвитие, который нельзя замкнуть кодом

```
GUARDRAILS.md :: Test-JobAllowed
delete
captcha
spam / newsletter
readonly: true
```

```
if (not $job.readonly) { return 'job is not marked readonly
Test-ProposalsAllowed -> false   # всегда
```

ЛИС практическая серия

Шадрин Данил

Парк read-only агентов на своём ПК

https://litres.ru/74708629
SelfPub; 2026

Аннотация

Как я собрал парк из десяти ИИ-агентов на обычном домашнем ПК: без подписок, без облаков и без права что-либо менять на машине. Внутри read-only режим для каждого агента, guardrails прописанные кодом, чёрный список слов который не пускает агента в опасную команду, лимиты бюджета и бортовой монитор, глушащий всю компанию пока хозяин играет в игру. Отдельно разбираю две грабли PowerShell 5.1 с BOM и ANSI кодовыми страницами, из-за которых скрипты молча ломались, и объясняю почему локальные модели на четырёх гигабайтах видеопамяти работают а Ollama нет. Книга для тех, кто хочет автоматизировать рутину на своём железе, а не отдавать доступ к компьютеру чужому сервису.

Содержание

Парк read-only агентов на своём ПК 4
Как ИИ сам ищет заказы, пишет сводки и не даёт натворить дел 4
От автора 4
Глава 1. Почему ровно read-only 5
Глава 2. Слова-блокаторы, то есть «не смей даже пытаться» 7
Конец ознакомительного фрагмента. 8

Шадрин Данил
Парк read-only агентов на своём ПК

Парк read-only агентов на своём ПК

Как ИИ сам ищет заказы, пишет сводки и не даёт натворить дел

От автора

Мне девятнадцать, я учусь на последнем курсе по специальности «Информационные системы и программирование» и подрабатываю фрилансом. Рабочих дней у меня в неделе меньше, чем у биржевого робота: лекции, домашки, иногда — игры, которые я не готов терять из-за скриптов. При этом заказы искать надо каждый день, а руки заняты.

Так появился парк агентов — десять маленьких задач, которые крутятся на моём же компьютере, читают открытые

страницы и складывают сводки. Я их не запускаю руками: они запускаются сами, по расписанию.

Сразу о честном: код, конфигурация, правила и тексты этого парка — мои, я их собирал и разбираю в них каждую строку. Текст книги как таковой был написан при помощи ИИ-агента, с которым я работаю каждый день: он черновик, я читаю, правлю и отвечаю за то, что в книге нет выдуманных фактов. Никаких «кейсов клиентов» тут не будет: их не существует. Будет реальный код с моей машины и реальные грабли, на которые я наступал.

Глава 1. Почему ровно read-only

Первое и главное ограничение парка родилось не из аккуратности, а из беды. Осенью выяснилось, что машина была заражена: кейлоггер плюс удалённый доступ, сервис-имплант и автозапуск, который я не видел в обычных списках. Импланты я снял, автозапуск вычистил, полную проверку защиты прогнал — но компьютер по-прежнему считаю скомпрометированным до переустановки Windows.

Из этого следует простое проектное решение: **агент имеет право только читать.**

Не «осторожно писать», не «писать в песочницу», а ровно читать публичное и локальное. Отклики на биржах, сообщения работодателям, публикации, платежи — всё это делает человек или основной агент в живом диалоге, где я вижу, что

именно уходит.

Это не метафора, а проверка кодом. В реестре у каждой задачи стоит флаг readonly: true, и без него задача не стартует:

```
function Test-JobAllowed($job) {
$txt = (('{0} {1} {2}' -f $job.id, $job.title, ($job.cmd -join ' '))).ToLower()
foreach ($flag in '-executionpolicy bypass', '-noprofile', '-windowstyle hidden', '-noninteractive') {
$txt = $txt.Replace($flag, ' ')
}
foreach ($w in $script:BlockedJobWords) {
if ($txt.Contains($w)) { return @{ ok = $false; why = "blocked word in job definition: '$w'" } }
}
if (-not $job.readonly) { return @{ ok = $false; why = 'job is not marked readonly' } }
foreach ($c in $job.cmd) {
if ($c -match '[;&|`$><]' -or $c -match '^--(forcelexec)') { return @{ ok = $false; why = 'suspicious argument: ' + $c } }
}
return @{ ok = $true; why = '' }
}
```

Строка if (-not $job.readonly) — это и есть ответ на вопрос «а если я завтра забудусь и дам агенту право писать?». Не забудусь: он не стартует.

Глава 2. Слова-блокаторы, то есть «не смей даже пытаться»

Второй слой — стоп-слова в самом определении задачи. Список живёт в GUARDRAILS.md и проверяется тем же Test-JobAllowed:

login password credential secret token cookie purchase buy pay invoice

withdraw deposit register signup delete remove-item format install uninstall

shutdown reboot registry import .reg captcha bypass proxy-rotation mass-invite

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.