



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

ИИ в работе сисадмина: ChatGPT и GigaChat на 10 ТИПОВЫХ задачах

Наш регламент: промпт-шаблоны, анонимизация данных,
GigaChat API для чувствительных контуров

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Инженеры тратят часы на рутину: расшифровку Event ID, разбор journalctl, написание PowerShell-обвязок, документацию и письма клиентам. Мы встроили ChatGPT и GigaChat в эти операции по регламенту: промпт-шаблоны, обязательная анонимизация, тест перед продом. Без регламента ИИ либо не используют, либо сливают в него реальные конфиги и IP клиентов.

Почему это важно бизнесу

- Час инженера уходит на гуглёж одного Event ID — при 8 инженерах это десятки часов в месяц
- Логи и конфиги с реальными IP, логинами и hostname в публичном чат-боте — утечка данных клиента
- Скрипт из ИИ без теста может массово изменить AD — простой и восстановление из бэкапа
- Недокументированная инфраструктура: уход инженера превращается в недельный разбор с нуля
- Клиенты с требованием «данные не покидают РФ» выпадают из ускорения без GigaChat-контура

Ключевые параметры реализации

128K

Контекст моделей GigaChat 2 в токенах — отфильтрованная выгрузка journalctl за смену влезает ц...

по докам GigaChat 2

30 мин

TTL access-токена GigaChat API — закладываем авто-рефреш в обвязку, иначе скрипты падают с 401

по докам GigaChat API

03.2023

С этой даты OpenAI API не обучается на присланных данных по умолчанию — поэтому автоматизацию...

по докам OpenAI API

10.x.x.x

Маска анонимизации: реальные IP, hostname и логины заменяем на условные до отправки в любую мо...

наш стандарт

80%

Долю инструкции/регламента закрывает генерация по тезисам инженера; 20% — скриншоты и проверка...

наш стандарт

5.1/7.4

Версию PowerShell и ОС всегда указываем в промпте — иначе модель выдаёт синтаксис не той эпохи

наш стандарт



Диагностика: логи Windows и Linux через ИИ

Что настраиваем

Серверы клиентов: Event Viewer на Windows Server 2019/2022, journalctl/syslog на Ubuntu/Debian

Как мы это делаем

- 1 Вывгружаем событие целиком: `Get-WinEvent -FilterHashtable @{LogName='Application';Id=1000} | Format-List *`, для Linux — `journalctl -u <служба> -p err --since '2 hour...`
- 2 Прогоняем через анонимизатор (sed-набор): IP → 10.x.x.x, hostname → server01, домен → corp.local, логины → user01
- 3 Шаблон промпта: роль «опытный администратор Windows Server/Linux», требование «начни с наиболее распространённых причин», просьба задавать уточняющие вопросы
- 4 Ответ — список гипотез по приоритету; каждую проверяем штатными средствами (`sfc /scannow`, `chkdsk`, сверка версий VC++ Redistributable, `nginx -t`), а не верим на слово
- 5 Подтверждённое решение — в базу знаний: событие, причина, фикс, ссылка на тикет

РЕЗУЛЬТАТ

Типовой разбор Event ID 1000/1001/7034 или пачки 502 в nginx сжимается с 1-2 часов гугления до 15-20 минут: модель сразу даёт ранжированный список гипотез, инженер только проверяет их по порядку.

КЛЮЧЕВОЙ НЮАНС

Ключ — предфилтрация: сырой journalctl без `-p err` и `--since` съедает контекст и топит причину в шуме. И фраза про распространённые причины в промпте обязательна — без неё модель уводит в экзотику раньше, чем в...



Чувствительный контур: GigaChat API внутри РФ

Что настраиваем

Клиенты с запретом передачи данных за периметр РФ (медклиники, юрфирмы) — своя обвязка через API Сбера

Как мы это делаем

- 1 Ключ авторизации в личном кабинете developers.sber.ru/studio; scope GIGACHAT_API_PERS для физлица, GIGACHAT_API_B2B или GIGACHAT_API_CORP для юрлица по договору
- 2 Ставим сертификат НУЦ Минцифры (Russian Trusted Root CA) в trust store хоста обвязки или передаём через `ca_bundle_file`
- 3 OAuth: POST <https://ngw.devices.sberbank.ru:9443/api/v2/oauth> с заголовком `RqUID (uuid4)`; токен живёт 30 минут — рефреш зашит в обвязку
- 4 Запросы на gigachat.devices.sberbank.ru/api/v1/chat/completions; для техразбора явно ставим `model: GigaChat-2-Pro` — по умолчанию отвечает Lite
- 5 Системный промпт с расширенным контекстом: версия ОС, состав стека, формат ответа — GigaChat требует больше вводных, чем ChatGPT

РЕЗУЛЬТАТ

Логи и конфиги клиента не покидают инфраструктуру РФ, при этом инженер получает тот же workflow: вставил лог — получил разбор. Скорость ниже, чем у ChatGPT, но требования клиента по данным закрыты документально.

КЛЮЧЕВОЙ НЮАНС

Две грабли из доки: без сертификата НУЦ Минцифры TLS-рукопожатие с API падает, а дефолтная модель — Lite, и на systemd-специфике она заметно слабее Pro. Обе лечатся конфигом, но их надо знать до внедрения.



Генерация скриптов и разбор GPO с контролем качества

Что настраиваем

PowerShell-автоматизация и аудит наследованных GPO в доменах AD клиентов

Как мы это делаем

- 1 В промпте фиксируем окружение: PowerShell 5.1 или 7.4, Windows Server 2022, модуль ActiveDirectory — отсекаем синтаксис старых версий
- 2 Полученный скрипт — через PSScriptAnalyzer (Invoke-ScriptAnalyzer) и прогон с -WhatIf на тестовом OU, только потом в прод
- 3 Каждый командлет и параметр сверяем: Get-Help <командлет> -Parameter * — модели выдумывают несуществующие ключи
- 4 Для аудита GPO: GPMC → Save Report в HTML, текст отчёта в модель с задачей «объясни, что политика делает, выдели опасные и нестандартные настройки»
- 5 Политики с прямыми правками реестра из ИИ-разбора не принимаем — проверяем вручную по ADMX-справочнику

РЕЗУЛЬТАТ

Скрипт «письма об истечении пароля AD за 7 дней с логом в C:\Logs» — 1,5 минуты генерации плюс полчаса проверки вместо половины дня. Наследованный домен с 23 недокументированными GPO разбираем за день вместо недели.

КЛЮЧЕВОЙ НЮАНС

ИИ даёт заготовку, а не продукт: без указания версии PowerShell в промпте получите командлеты эпохи 2.0, а без -WhatIf на тестовом OU — массовые изменения в AD с первого запуска. Проверка — часть регламента, н...



Подводные камни

✗ Реальные IP и логины в промпте

Инженер копирует лог как есть. Мы прогоняем через sed-анонимизатор (IP→10.x.x.x, host→server01) и работаем из-под Team-аккаунта, не личного

✗ Веб-чат вместо API для данных клиентов

Бесплатный ChatGPT может обучаться на переписке. Отключаем «Improve the model for everyone» в Data Controls; для рабочих задач — Team/API, где обучен...

✗ GigaChat отвечает моделью Lite

Без параметра model запрос уходит в GigaChat 2 Lite — для техразбора слабовато. В payload обвязки жёстко ставим GigaChat-2-Pro

✗ TLS-ошибка при вызове GigaChat API

API работает на сертификатах НУЦ Минцифры — без корня в trust store соединение падает. Ставим Russian Trusted Root CA или ca_bundle_file

✗ Выдуманные командлеты и ключи

Модели уверенно генерируют несуществующие параметры. Каждый командлет сверяем через Get-Help, скрипт — через PSScriptAnalyzer до запуска

✗ Скрипт сразу в прод

Всё, что трогает AD или делает массовые изменения, — сначала -WhatIf на тестовом OU. Один прогон без проверки — и восстанавливаем из бэкапа

✗ Сырой лог на сотни тысяч строк

Модель теряет причину в шуме и режет контекст. Сначала journalctl -p err --since / Get-WinEvent с фильтром, потом отправка

✗ Токен GigaChat протухает молча

Access-токен живёт 30 минут, SDK сам его не обновляет — в обвязке ловим 401 и перезапрашиваем OAuth с новым RqUID

Как правильно

МИНИМУМ

- Отключить обучение на данных в Data Controls у всех рабочих аккаунтов ChatGPT
- Правило анонимизации: IP, hostname, логины заменяются до отправки в любую модель
- 3-4 промпт-шаблона команды: Event Viewer, journalctl, PowerShell, письмо клиенту
- Запрет запуска ИИ-скриптов в прод без теста — зафиксирован в регламенте

НОРМАЛЬНО

- ChatGPT Team на команду: обучение выключено по умолчанию, общие проекты и шаблоны
- GigaChat API (scope B2B/CORP) для клиентов с требованием «данные не покидают РФ»
- PSScriptAnalyzer + прогон с -WhatIf на тестовом OU для всего генерённого PowerShell
- Sed-анонимизатор логов как шаг пайплайна, а не ручная замена по памяти

ХОРОШО

- Своя обвязка к обоим API с маршрутизацией: чувствительное → GigaChat, остальное → Op...
- Авто-рефреш OAuth-токена GigaChat и явный выбор модели (Pro/Max) по типу задачи
- База знаний: подтверждённые пары «событие → причина → фикс» из каждого ИИ-разбора
- ИИ-генерация документации встроена в закрытие тикета: тезисы → инструкция → скриншоты



Чек-лист самопроверки

☐ Отключено ли обучение на данных (Data Controls) во всех рабочих аккаунтах ChatGPT?

☐ Есть ли письменное правило анонимизации логов и конфигов перед отправкой в ИИ?

☐ Работают ли инженеры из-под корпоративного Team-аккаунта, а не личных?

☐ Определён ли контур для чувствительных данных — GigaChat API вместо зарубежных облаков?

☐ Установлен ли сертификат НУЦ Минцифры на хостах, ходящих в GigaChat API?

☐ Проверяется ли каждый ИИ-скрипт через PSScriptAnalyzer и -WhatIf до продакшена?

☐ Указывается ли в промптах версия PowerShell и ОС целевого сервера?

☐ Фильтруются ли логи (journalctl -p err, Get-WinEvent -FilterHashtable) перед отправкой?

☐ Попадают ли подтверждённые ИИ-диагнозы в базу знаний команды?

☐ Знает ли команда, что модель GigaChat по умолчанию — Lite, и когда нужна Pro?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Внедрим ИИ-регламент в ИТ-отдел: пром프트-шаблоны, анонимизация, правила теста скриптов
- Развернём контур GigaChat API под ключ: OAuth, сертификаты НУЦ Минцифры, выбор модели
- Настроим ChatGPT Team с выключенным обучением и общей библиотекой промптов команды
- Разберём наследованные GPO и недокументированную инфраструктуру с ИИ-ускорением
- Обучим инженеров: 10 рабочих сценариев с проверкой результата, а не слепым доверием

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** GigaChat API: авторизация и быстрый старт (OAuth, RqUID, scope) (developers.sber.ru — 2026)
- 02** GigaChat: выбор модели для генерации (Lite/Pro/Max, контекст 128K) (developers.sber.ru — 2026)
- 03** Использование сертификатов НУЦ Минцифры в GigaChat (developers.sber.ru — 2026)
- 04** OpenAI API: Data controls (обучение на данных выключено по умолчанию) (platform.openai.com — 2026)
- 05** Enterprise privacy at OpenAI (Team/Enterprise, retention) (openai.com — 2026)
- 06** PSScriptAnalyzer: правила и Invoke-ScriptAnalyzer (learn.microsoft.com — 2026)
- 07** Наш шаблон промптов L1-диагностики и sed-анонимизатор (itfresh.ru — v2)

Основано на официальной документации продуктов и нашей практике внедрения.

