МОДУЛЬ 1 · ТЕМА 1.1

Языковые модели и чат-сервисы: что умеют и где ошибаются



Понять инструмент, чтобы знать, где ему доверять, а где проверять каждую строчку

1.1

День 1 · Виталий Пиков · архитектор информационной безопасности · pikov.expert

Курс за пять дней



1. **16.11** Языковые модели и запросы
2. **18.11** Защита информации и техническая документация
3. **20.11** Поиск решений и анализ отказов
4. **23.11** Расчёты и данные испытаний
5. **25.11** ИИ в работе подразделения, свой сценарий

Теории минимум. Всё, что говорим, проверяем руками на учебном узле

Вопросы к группе

Кто уже пользовался ИИ-сервисами? Какими?

У кого открыт доступ с рабочего места?

Какую задачу вы бы первой отдали ИИ?

Как модель составляет ответ

Обучена на огромном объёме текстов

Не ищет готовый ответ, а по частям составляет **продолжение текста**

Сильная сторона: связный текст, черновики, сводки, таблицы

Слабая сторона: **правдоподобное** вместо **верного**, если верного она не знает

Что есть в чат-сервисе

Функция	Что важно знать
Контекст диалога	Модель видит текущий чат и файлы в нём, объём ограничен
История чатов	Хранится у сервиса, удаляется по-разному
Файлы и изображения	Пересказ, таблицы, вопросы по тексту. Распознанное проверяем
Режим рассуждения	Строит шаги перед ответом. Может помочь в многошаговых задачах, отвечает дольше
Поиск в интернете	Свежие сведения, но ссылки всё равно открываем

Сервисы на курсе

Сервис	Чей	Что важно
GigaChat	Сбербанк	Сбер ID или телефон. По соглашению: личное некоммерческое использование, без персональных данных в запросах
Алиса AI	Яндекс	Режим «Эксперт», опция «Алиса Плюс». История без опции – 14 дней
DeepSeek	КНР	Данные хранятся в КНР, идут в обучение, пока это не отключено
Qwen	Сингапур	Данные хранятся в Сингапуре, обезличенный контент может идти в обучение

По справке и соглашениям сервисов на 10.11.2026. Функции меняются – проверяем в интерфейсе

Доступ



- Учётная запись: Сбер ID, Яндекс ID, почта или телефон
- Бесплатно: GigaChat, Алиса AI, Qwen. Подписка – больше запросов и функций
- Личный и корпоративный доступ – разные условия обработки данных
- На работе доступ – **по заявке**, через подразделение, которое его выдаёт
- Не обходим: личный телефон, домашняя почта, флешка

ОГРАНИЧЕНИЯ

Где модели ошибаются

Пять типичных ошибок и что с ними делать



Выдуманные ссылки

Модели подбирали литературу для систематических обзоров. Доля выдуманных ссылок – от 28,6 до 91,4 % в зависимости от модели

Chelli M. et al. JMIR, 2024. doi.org/10.2196/53164 · модели 2023 года

от 28,6 до 91,4 %

Доля выдуманных ссылок

Ещё четыре ошибки

1. **Несовместимые ответы на один фактический вопрос** – повод проверить. Одинаковые ответы ещё не гарантия
2. **Устаревшие сведения** – новых редакций стандартов модель может не знать
3. **Вычисления** – верная методика, неверные числа и единицы
4. **Согласие с ошибкой в вопросе** – неверную посылку модель чаще принимает, чем поправляет

Farquhar S. et al. Nature, 2024 · Mysior M., Iniotakis C. Research in Engineering Design, 2026

Главный вывод

Ответ модели всегда проверяет инженер. Модель экономит время на черновике, ответственность – на том, кто использует результат

От чата к агенту

1

Чат – отвечает на ваш текст

2

Чат с файлами и поиском – читает документы и страницы

3

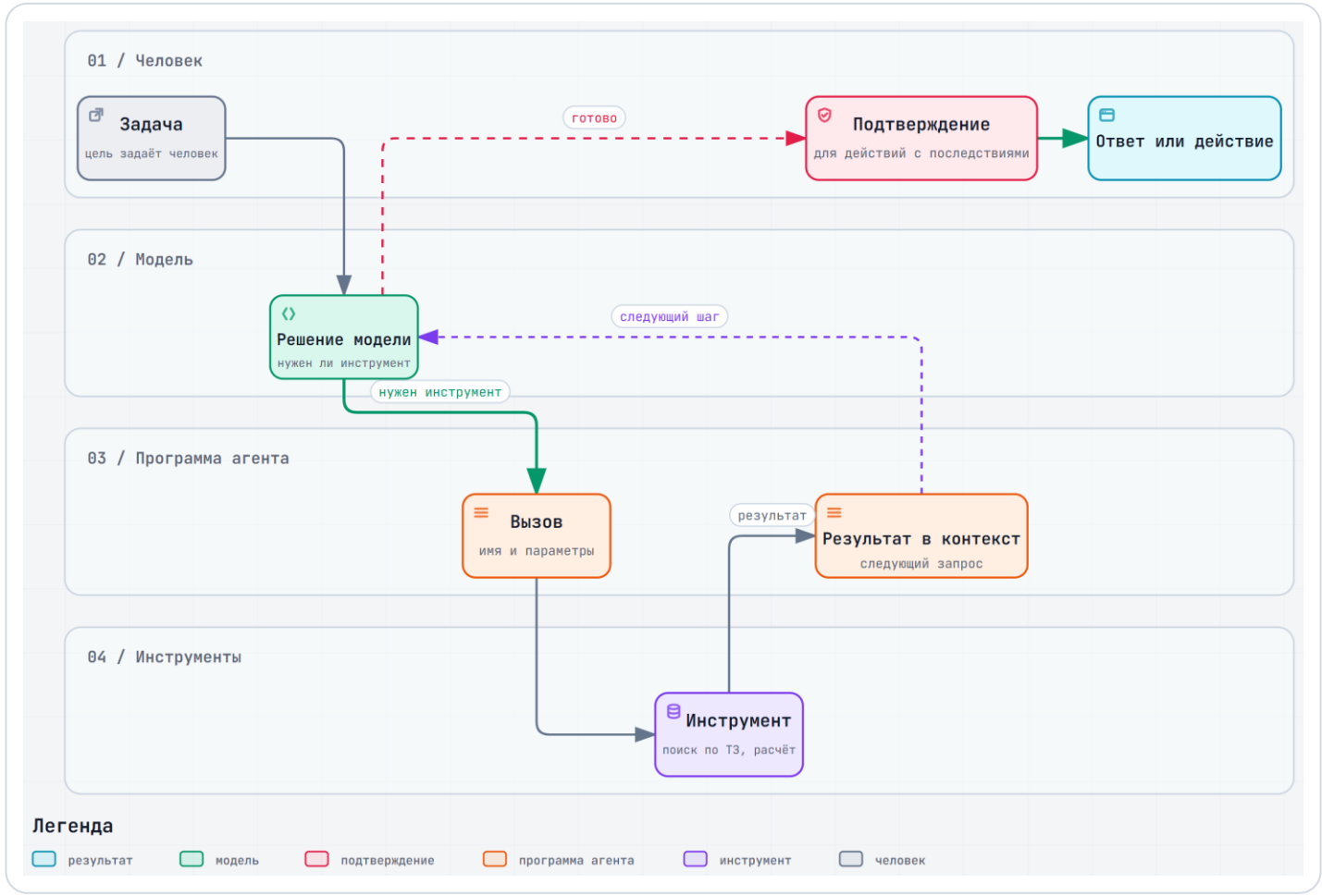
Помощник по документам – ищет в базе документов организации

4

Агент – сам вызывает инструменты и действует

Ступени условные. Различие в том, кто выбирает следующий шаг: на ступенях 1–3 – сценарий программы и человек, у агента – модель. Подробнее – в дополнительном материале и в модуле 5

Как работает агент: модель выбирает следующий шаг



Интерактивная версия – 08-Схемы/d1-cikl-agenta.html

Правило с первого занятия



- В сервисы – **только учебные и открытые материалы**
- Рабочие документы, переписку, фамилии, обозначения изделий не вставляем
- Почему так строго – в среду, тема 2.1

ПРАКТИКА 1.1 · 09:30–11:55

Пробуем сервисы на учебном узле

Интерфейс, одна задача в разных сервисах, поиск ошибок, карточка задачи

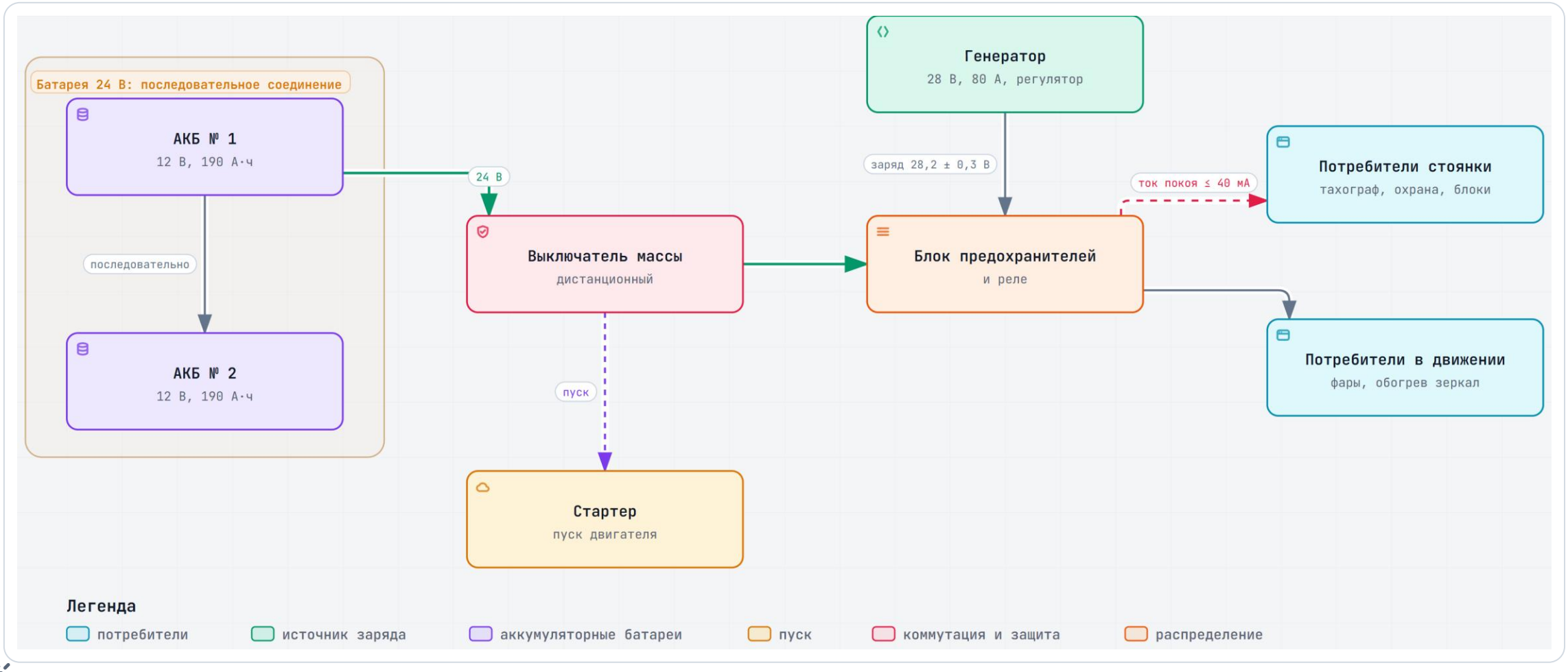


Учебный узел ЭС-24

Что	Значение
Бортовая сеть	24 В
Генератор	28 В, 80 А, встроенный регулятор
Батареи	2 × 12 В, 190 А·ч, последовательно
Ток покоя по ТЗ	не более 40 мА через 30 мин
Стоянка по ТЗ	14 суток до −25 °C, пуск без внешнего источника

Узел условный, значения учебные. Кейс целиком можно отправлять в сервисы

Схема учебного узла ЭС-24



Интерактивная версия – 08-Схемы/d1-uzel-es24.html

Задание 1. Осмотреть интерфейс



30 мин

1. Новый чат, история, удаление диалога
2. Загрузка файла и изображения
3. Режим рассуждения, поиск в интернете
4. Настройки данных: хранение истории, использование для обучения
5. Лимиты: длина сообщения, число запросов

Задание 2. Одна задача – разные сервисы



60 мин

1. 2а. Замечание 3-3 (просадка до 26,1 В) в два-три сервиса, каждый раз новый чат
2. Сравнить по таблице критериев
3. 2б. Найти ошибки в готовом ответе из раздела 4 кейса

Задание 3. Карточка инженерной задачи



30 мин

1. **Исходные данные** – что известно
2. **Ожидаемый результат** – что получить и в каком виде
3. **Критерии приёмки** – по чему примем результат
4. **Ограничения** – что задано, чего не делать
5. Карточка для 3-1 и для одной своей задачи, без служебных сведений

Задание повышенной сложности. Контрольный набор вопросов для сервиса



30–45 мин

1. Для тех, кто справился с основными заданиями. Можно сделать и после занятия
2. Пять вопросов по кейсу, верный ответ записан заранее
3. Прогон в сервисе и сверка с эталоном
4. Повтор во втором сервисе или в новом чате
5. Результат: контрольный набор и таблица результатов

Автор курса – Виталий Пиков



Регалии

Архитектор информационной безопасности · РБПО · DevSecOps · AppSec

Лектор и автор образовательных программ по ИБ и РБПО

Телефон

+7 (963) 782-92-78

E-mail

vitaly@pikov.expert

Сайт

https://pikov.expert

Telegram

@UnderLineSecurity