Технологии Доверия

Риск-менеджмент на скорости света: ИИ-агент по управлению риском аутсорсинга

Наталья Стрекаль
Исполнительный директор
«Технологии Доверия»

Мария Середа
Менеджер
«Технологии Доверия»

Технологии Доверия

Путь вместе с банками: от внедрения требований по риску аутсорсинга к совершенствованию практики

Июнь 2022
Публикация проекта 716-П

Апрель 2025
Публикация Указания о изменении 716-П

Октябрь 2025
Вступление в силу изменений 716-П

10+ банков — для которых реализованы проекты по риску аутсорсинга

3 банка — из ТОП-5

Ранее опубликованные доклады по теме управления риском аутсорсинга в рамках конференций ОпРиск Сообщества:

Фев. 2023 *Краеугольный камень операционной устойчивости: методология риска аутсорсинга – Наталья Стрекаль, Ирина Криволапова, Григорий Борткевич*
Май 2023 *ИТ-аутсорсинг: свои игроки или легионеры? – Максим Иванов, Наталья Стрекаль*
Июль 2025 *О контрольных показателях уровня РА – Михаил Бухтин*
Окт. 2025 *Практические вопросы выстраивания процедуры управления операционным риском аутсорсинга – Михаил Бухтин, Григорий Борткевич*
Окт. 2025 *Управление РА. Опыт Московской Биржи – Соловьева Дарья, Миньзюк Ольга*

Ключевые тренды процесса управления риском аутсорсинга [1/2]

1 Определение аутсорсинга

01 Калибровка определения аутсорсинга

Уточнение критериев определения аутсорсинга на основании действующего портфеля договоров

02 Закупка ТМЦ и поставки критичных данных

Включение в периметр критичного аутсорсинга функций с высоким риском для Банка

03 Ограничение периметра ИТ-аутсорсинга

Исключение разработки ИТ-систем из периметра аутсорсинга, включение поддержки и сопровождения только в части критичных ИТ-систем

2 Ролевая модель

04 Ответственность на Блоке Риски

Выделение одного / нескольких спец. подразделений, ответственных за аутсорсинг, в зависимости от объема ИТ-аутсорсинга

Рыночная практика: прочий аутсорсинг – Служба операционных рисков, редко закупки, ИТ-аутсорсинг – спец. подразделение в ИТ (с исключением конфликта интересов)

05 Уполномоченный коллегиальный орган

Преимущественно в рыночной практике определен Комитет по управлению операционным риском, реже Правление банка или Комитет по закупкам

Ключевые тренды процесса управления риском аутсорсинга [2/2]

Выполнение регуляторных требований приводит к существенному росту трудозатрат заказчиков критичного аутсорсинга, что актуализирует вопрос эффективности

3 Повышение эффективности процесса

06 Анализ целесообразности на уровне функций аутсорсинга

Анализ целесообразности на уровне функции, передаваемой на аутсорсинг, а не на уровне отдельного договора
Формирование и ежегодное утверждение на КО перечня одобренных к передаче на аутсорсинг функций, включая лимиты



07 ИИ-зация процессов банка по разным областям деятельности

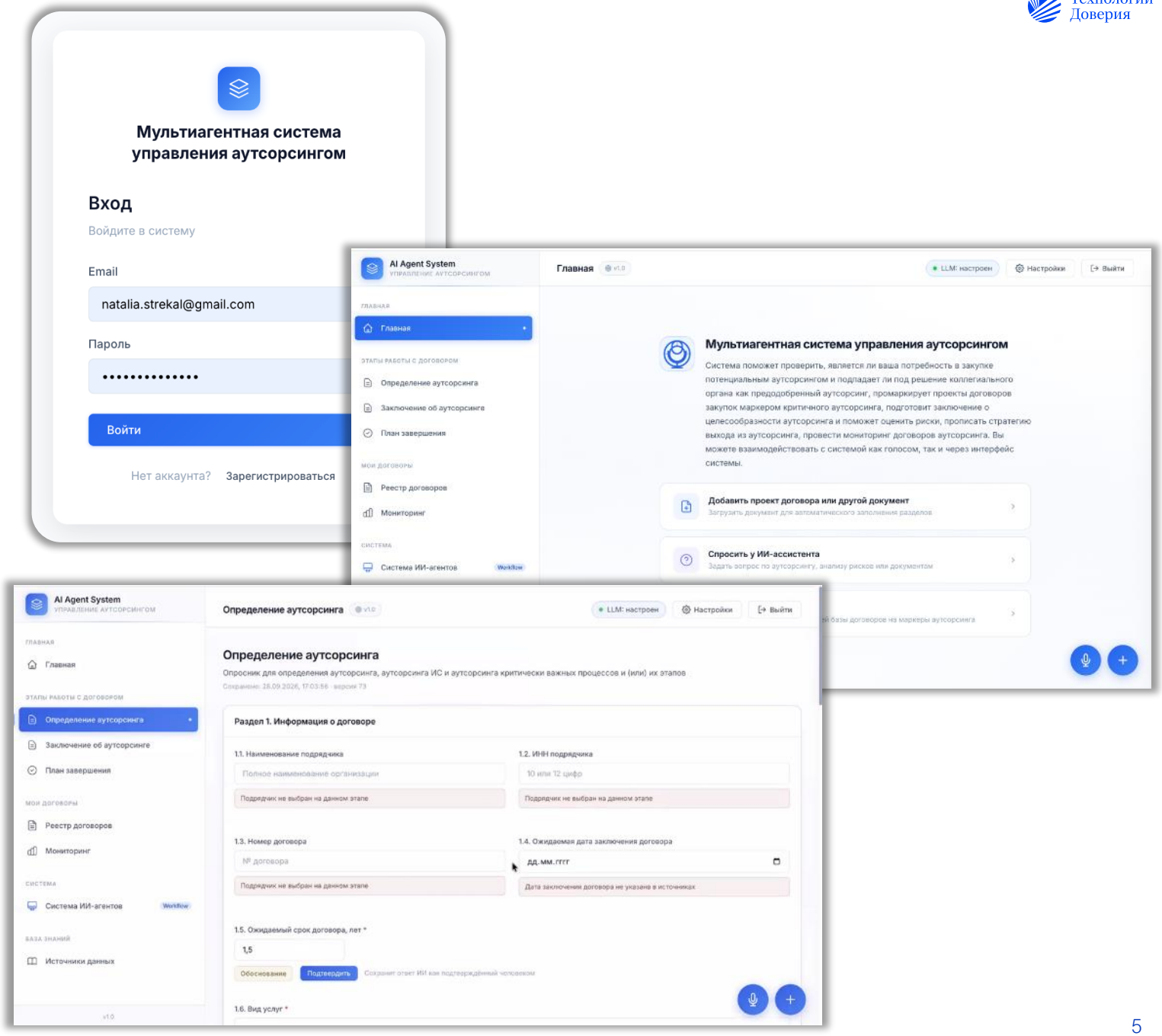
Внедрение ИИ-агентов на базе корпоративной LLM в процессе управления риском аутсорсинга

КО – коллегиальный орган

ИИ-агент по управлению риском аутсорсинга

– представляет собой комплексное решение полного цикла, обеспечивающие управление процессом аутсорсинга на всех этапах: от внесения и классификации договоров до мониторинга и контроля

ИИ-агент позволяет автоматизировать рутинные и трудозатратные этапы управления риском аутсорсинга, а также объединяет всех участников процесса и обеспечивает сквозное управление аутсорсингом



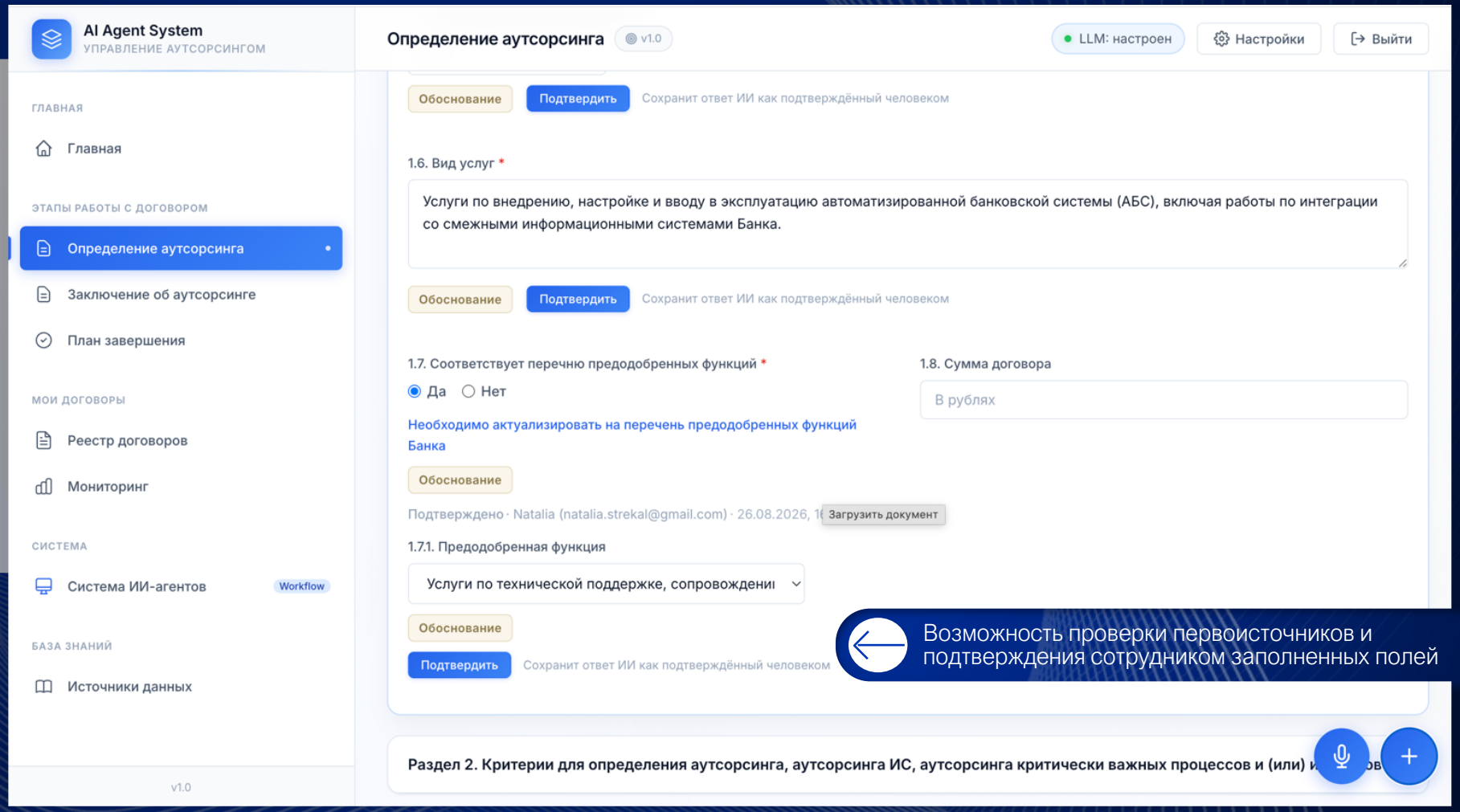
Работающий end-to-end сценарий

Возможности ИИ-агента по управлению риском аутсорсинга

Технологии Доверия

ИИ-агент поддерживает путь от загрузки данных до формирования проекта вывода о целесообразности аутсорсинга, включая перечень рисков и их оценку

Каждый этап запускается автоматически на основании классификации аутсорсинга / критичного аутсорсинга

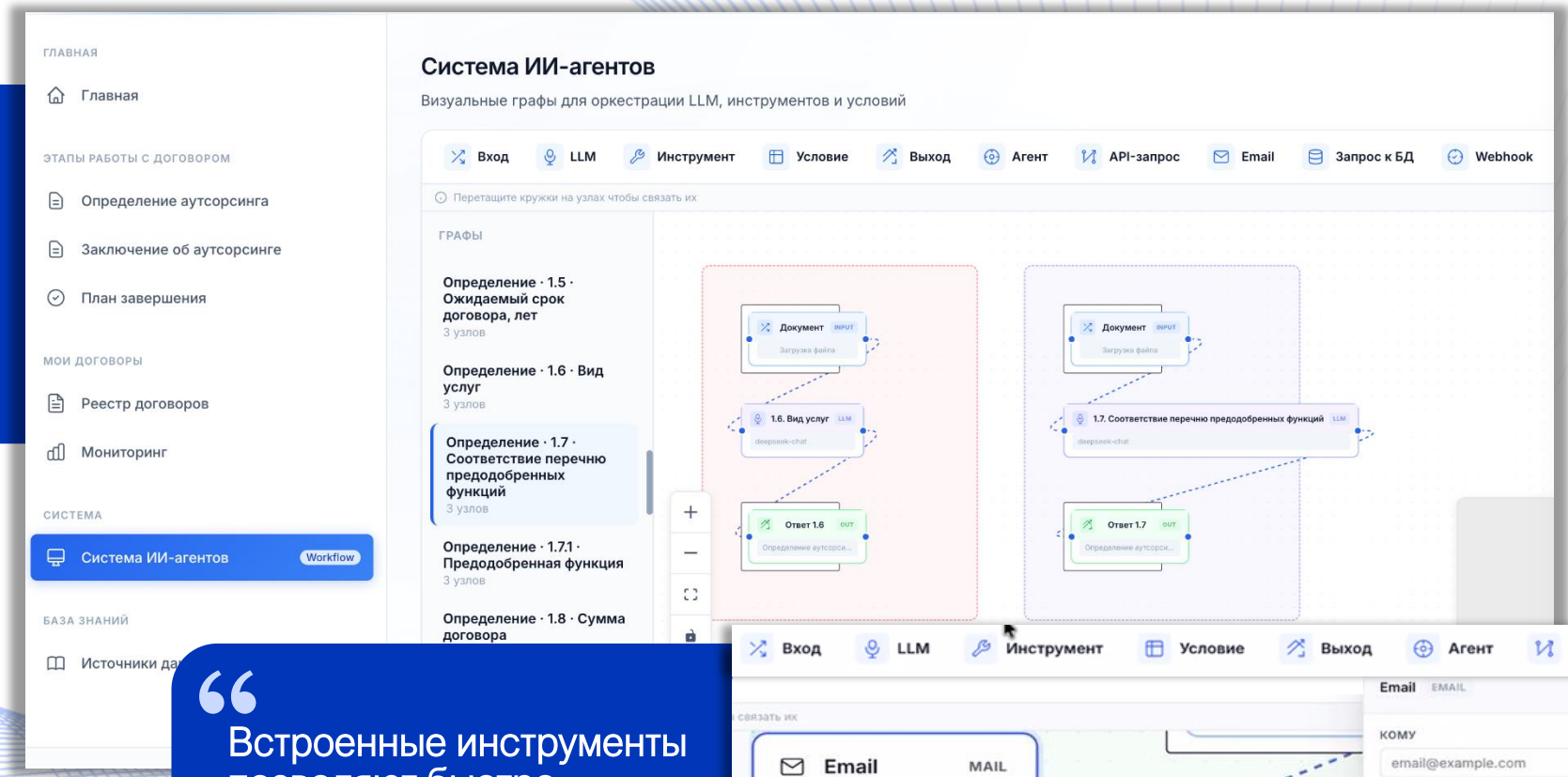


Гибкая графовая ИИ-архитектура

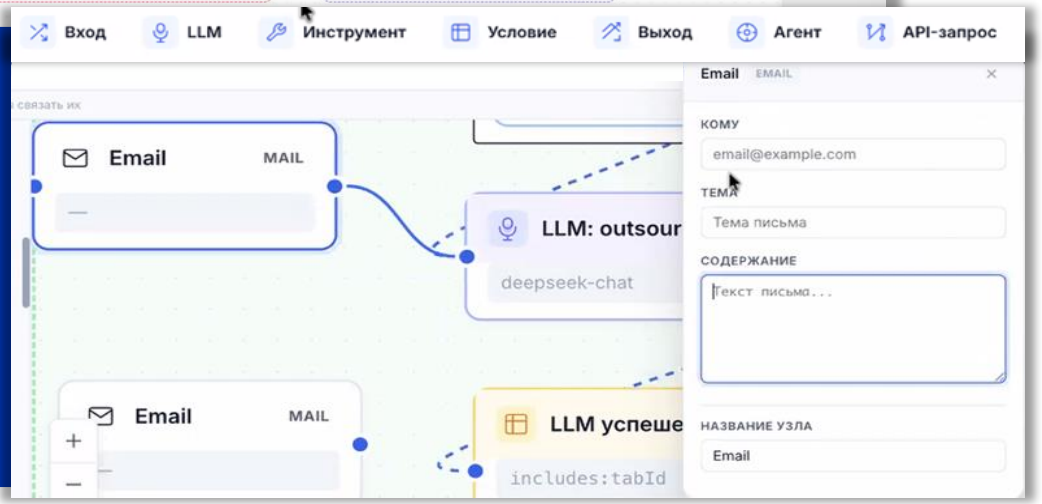
Возможности ИИ-агента по управлению риском аутсорсинга

Технологии Доверия

> ИИ-агент имеет графовую архитектуру, что позволяет гибко настраивать логику анализа договоров, добавлять этапы и адаптировать процесс к методологии банка



> Встроенные инструменты позволяют быстро дорабатывать архитектуру и алгоритмы ИИ-агента: создавать новый граф, редактировать узлы, настраивать интеграцию с почтой или АС



АС – автоматизированная система

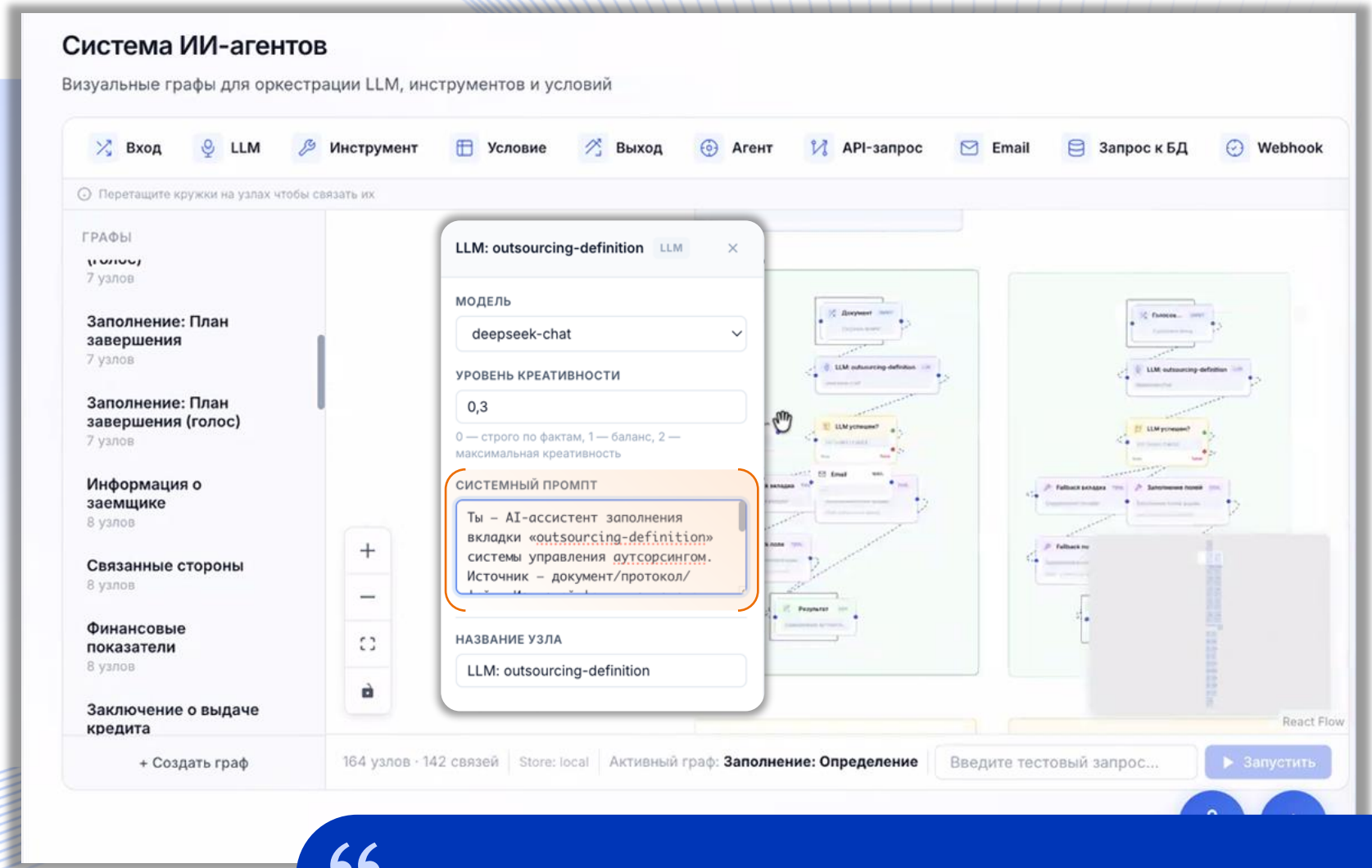
Системная генерация промптов

Возможности ИИ-агента по управлению риском аутсорсинга

> Заполнение полей и маршрутизация договора реализуется на основе заданного промпта с указанием оснований для каждого значения и ссылками на исходные данные

Ты — AI-ассистент заполнения вкладки «outsourcing-definition» системы управления аутсорсингом.
Источник — документ/протокол/файл. Извлекай факты из текста.

Правила:
1. Заполняй ТОЛЬКО вкладку outsourcing-definition. В ответе tabId должен быть "outsourcing-definition".
2. Текстовые поля — только если обоснованно следуют из текста; пустые не включай.
….
Текстовые поля (включай только если есть в источнике):
contractor_name — Название подрядчика / исполнителя
contractor_inn — ИНН подрядчика: 10 или 12 цифр
…

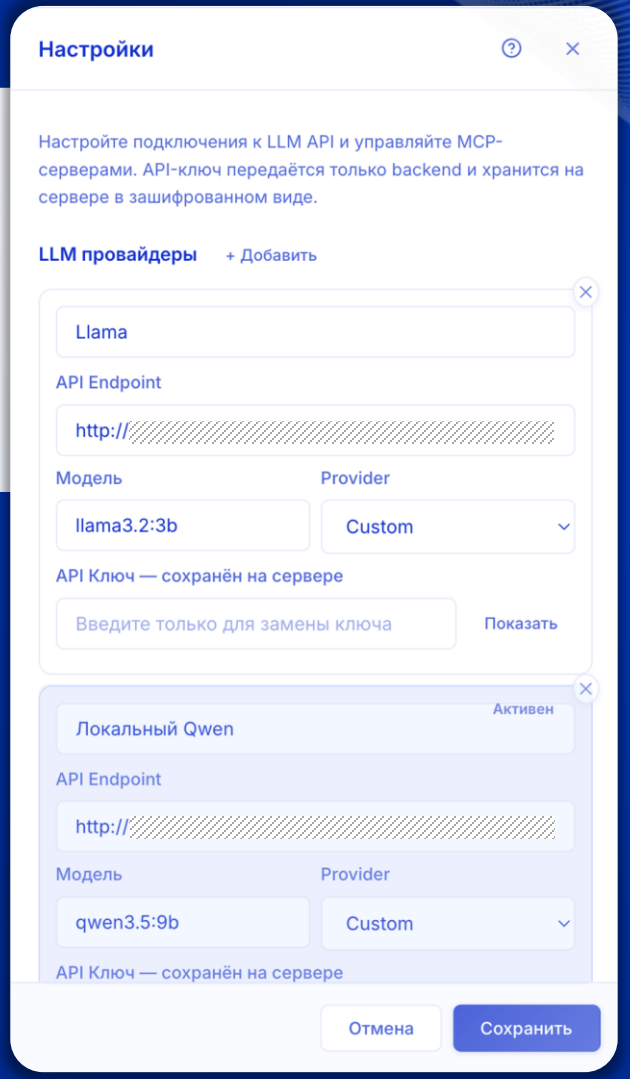


> Промпты генерируются как автоматически с учетом заданных условий, так и загружаются вручную пользователем

Подключение LLM

Возможности ИИ-агента по управлению риском аутсорсинга

> Прототип разработан с возможностью подключения к локальным и открытым LLM, развернутым в контуре банка с использованием API-ключей банка



Вызов инструментов Web-search

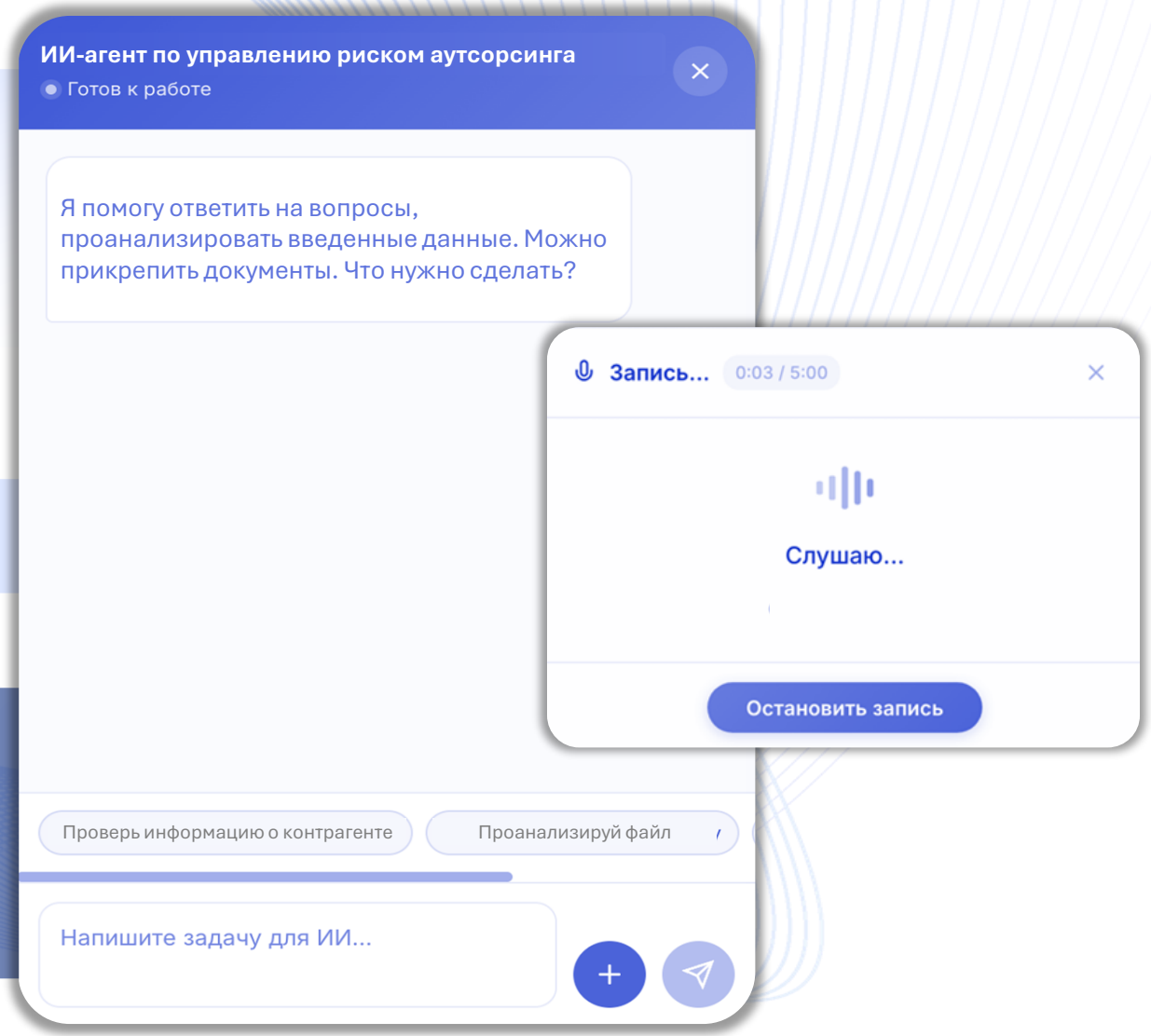
Возможности ИИ-агента по управлению риском аутсорсинга

> ИИ-агент имеет возможность вызова инструментов поиска в интернете для проведения анализа по аналогии с действиями пользователя

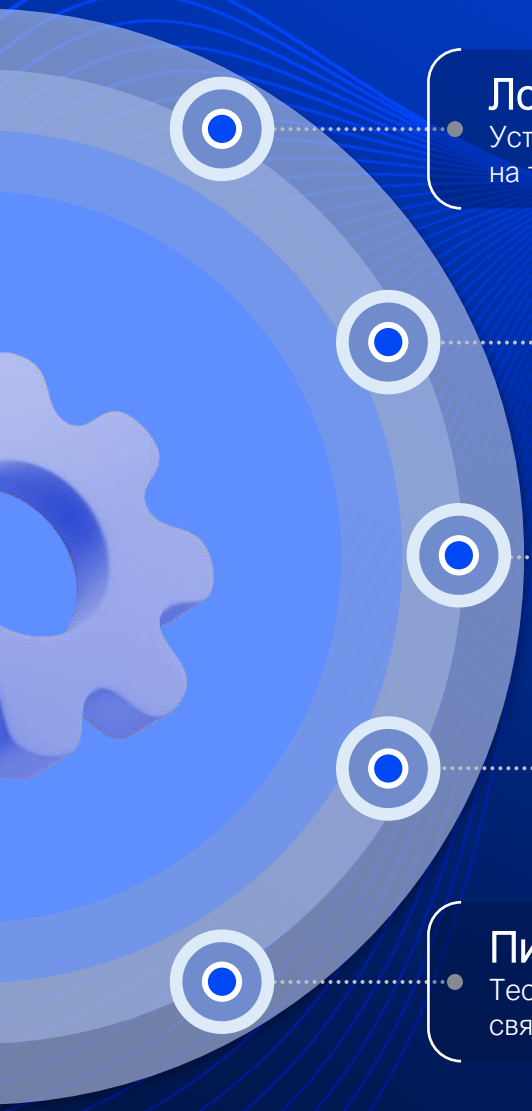
Интерактивный ИИ-чат бот

Возможности ИИ-агента по управлению риском аутсорсинга

> ИИ-агент работает в контексте текущего договора: отвечает на вопросы, помогает заполнять поля и поддерживает работу с вложениями и голосовым вводом



Дальнейшие шаги внедрения прототипа ИИ-агента



Локальное развертывание прототипа

Установка прототипа в локальной среде, проверка пользовательского интерфейса и базовых сценариев работы на тестовых данных

Подключение корпоративной LLM

Интеграция решения с LLM, развернутой в ИТ-инфраструктуре, для работы с чувствительной информацией с учетом требований информационной безопасности

Калибровка на данных и процессах банка

Адаптация решения к специфике действующих процессов управления аутсорсингом на основе текущего портфеля договоров, критериев аутсорсинга, детальных данных ведения каждого договора и других материалов

Интеграция с ИТ-ландшафтом банка

Подготовка решения совместно с ИТ-подразделениями к промышленной эксплуатации: развертывание в ПРОМ, подключение к базам данных, системам-источникам, специфичным системам управления рисками

Пилотирование и оценка эффективности

Тестирование решения на ограниченном портфеле договоров, проверка качества результатов, сбор обратной связи пользователей и доработка перед масштабированием

Интеграция с ИТ-ландшафтом банка

Внедрение прототипа ИИ-агента осуществляется в соответствии с подходом к разработке, реализованным в банке. В случае использования банком Enterprise Vibe Coding платформ интеграция прототипа ИИ-агента с ИТ-ландшафтом банка предполагает формирование спецификации для запуска SDD / IDD:



Сокращения и термины:
SDD – Spec-Driven Development, методология разработки ПО (спецификация – источник для разработки ИИ-агентом)
IDD – Intent-Driven Development, методология разработки ПО (намерение – источник для разработки ИИ-агентом)
AGENTS.md – инструкции, контекст и правила работы ИИ-агента
API – Application programming interface, программный интерфейс для взаимодействия программ

MCP – Model context protocol, стандарт для унифицированного подключения LLM и ИИ-агентов к внешним источникам и инструментам
Evals-тесты – тесты проверки качества работы LLM: правильность ответов, следование инструкциям, отсутствие галлюцинаций.
policy-as-code – подход описания правил безопасности и комплаенса в виде кода и автоматической проверки
PR – запрос на объединение изменений кода в проект

Технологии Доверия

Метаданные прототипа

01	бизнес-цель (intent)
	спецификация (spec)
02-04	модель
	конфигурация агента
	используемые инструменты и файлы
	план тестирования
05-07	результаты тестов
	результаты evals-тестов
	результаты ИБ-тестов
	согласование сотрудником

Развитие ИИ-агента в контуре банка

Метрики качества ИИ-агента

1. **Время обработки договора**
   Среднее время от поступления договора до завершения его анализа

2. **Полнота извлечения данных**
   Доля условий и сведений о договоре, выявленных агентом и занесенных в шаблон автоматизировано

3. **Корректность извлечения данных**
   Доля договоров, обработанных ответственным сотрудником без ручных корректировок

4. **Консистентность решений**
   Стабильность выводов агента при повторной обработке одинаковых входных данных

5. **Автоматизация формирования отчетности**
   Подготовка внутренней отчетности / дашбордов, отчетов по конкретному договору / поставщику автоматизирована

Сценарии развития ИИ-агента

1. Уточнение критериев функций, передаваемых на аутсорсинг, с учетом специфики портфеля договоров банка

2. Принятие решения о необходимости корректировки списка одобренных функций ежегодно утверждаемых на КО

3. Самостоятельное выявление ошибок в первичных документах (ТЗ на закупку, договор и пр.)

Технологии Доверия



Наталья Стрекаль
Исполнительный директор
Управления нефинансовых рисков
«Технологии Доверия»
natalia.strekal@tedo.ru
+7 905 272 76 44



Мария Середа
Менеджер
Управления нефинансовых рисков
«Технологии Доверия»
mariia.sereda@tedo.ru
+7 911 189 79 54

tedo.ru

Компания «Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре и Нижнем Новгороде работают около 3 000 специалистов. Мы помогаем нашим клиентам выстраивать и укреплять доверие к бизнесу благодаря нашему опыту и качеству оказываемых услуг.

© 2026 «Технологии Доверия». Все права защищены.