УДК 004.89

ИНТЕГРАЦИЯ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: ВОЗМОЖНОСТИ, ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ

Воробьева Д. В. [1]

студент,

Поволжский государственный университет телекоммуникаций и информатики,

Самара, Россия

Аннотация

Сопоставлены три способа встраивания больших языковых моделей в контур корпоративных информационных систем: обращение к внешнему поставщику, размещение модели на собственных мощностях и надстройка с поиском по внутренним хранилищам. Выбор архитектуры интеграции определяется требованиями к конфиденциальности данных, доступной вычислительной инфраструктурой и допустимым уровнем риска. Обоснована необходимость разграничения прав доступа, протоколирования действий модели и сохранения обязательного контроля со стороны человека. Показано, что преобладающей стала третья схема, и выделены ограничивающие её факторы – недостоверность отдельных ответов, уязвимость к внедрению вредоносных указаний и трудность оценки качества.

Ключевые слова: большие языковые модели, корпоративные информационные системы, информационная безопасность, LLM, управление корпоративными знаниями.

[1] Научный руководитель: **Куваева Е.Н.**, ст. преподаватель, Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия.
Kuvaeva E.N., Senior Lecturer, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia.

INTEGRATION OF LARGE LANGUAGE MODELS INTO CORPORATE INFORMATION SYSTEMS: OPPORTUNITIES, LIMITATIONS AND PROSPECTS

Vorobyeva D. V.
Student,
Povolzhskiy State University of Telecommunications and Informatics,
Samara, Russia

Abstract

Three ways of embedding large language models into corporate information systems are compared: calling an external provider, hosting a model on the company premises, and a superstructure with search over internal repositories. The choice of integration architecture is determined by data confidentiality requirements, the available computing infrastructure, and the acceptable level of risk. The necessity of segregating access rights, logging model actions, and maintaining mandatory human oversight is substantiated. The third scheme is shown to be prevalent, and its limiting factors are identified: unreliability of individual answers, vulnerability to injected malicious instructions, and the difficulty of quality assessment.

Keywords: large language models, corporate information systems, information security, LLM, corporate knowledge management.

Первая волна внедрений языковых моделей на предприятиях сводилась к помощникам, работавшим в стороне от учётных систем: сотрудник переносил данные в диалоговое окно вручную и так же вручную возвращал результат. Измеримого выигрыша это не давало, поскольку не устраняло главную издержку – переключение между приложениями. Эффект возникает тогда, когда модель получает доступ к данным систем документооборота и обслуживания клиентов, а её ответы включаются в существующие цепочки согласования. Цель работы – сопоставить подходы к такой интеграции и очертить ограничения каждого из них.

Практика применения сводится к четырём направлениям:

– извлечение реквизитов из договоров и обращений;

– первичная классификация заявок пользователей и подготовка проекта ответа для оператора;

– поиск по внутренним базам знаний [1, 2];

– разбор потока событий в задачах мониторинга информационной безопасности [3].

Общее свойство – модель не заменяет исполнителя, а сокращает подготовительную часть его работы.

Способы встраивания модели в контур предприятия сопоставлены в таблице 1. Обращение к внешнему поставщику требует наименьших вложений, но передаёт корпоративные сведения за пределы периметра. Для организаций, работающих с персональными данными, этот путь обычно закрыт. Размещение модели с открытыми весами на собственных мощностях снимает вопрос передачи данных, однако совокупная стоимость владения определяется здесь не столько закупкой ускорителей, сколько сопровождением и обновлением модели.

Таблица 1 - Сопоставление способов интеграции

Признак	**Внешний поставщик**	**Собственный контур**	**Надстройка с поиском**
Скорость запуска	Дни	Месяцы	Недели
Контроль над данными	Ограниченный	Полный	Полный
Стоимость входа	Низкая	Высокая	Средняя
Актуальность знаний	Низкая	Низкая	Высокая

Преобладающей стала третья схема: запрос сотрудника преобразуется в поисковый, по внутренним хранилищам отбираются подходящие фрагменты документов, и уже они вместе с исходным вопросом передаются модели [1; 5]. Схема позволяет опираться на сведения, отсутствовавшие в обучающей выборке, и сопровождать ответ ссылками на исходные документы. Её качество определяется не выбором модели, а подготовкой данных: разбиением

документов на смысловые фрагменты, поддержанием их актуальности, учётом прав доступа.

Первое ограничение – склонность моделей порождать правдоподобные, но неверные утверждения. Причиной этого являются особенности обучения и работы моделей: при формировании ответа они не определяют достоверность каждого утверждения напрямую, а предсказывают следующий токен с учетом уже имеющегося контекста. Обучающие данные могут содержать недостоверную, неполную или устаревшую информацию, а отсутствие доступа к актуальным внешним источникам и недостаток контекста в пользовательском запросе повышают вероятность формирования недостоверного ответа. Поиск с дополнением контекста снижает частоту таких случаев, но не устраняет их: если поисковая часть вернула неподходящие фрагменты, модель всё равно сформирует ответ [5]. Второе относится к безопасности: когда модель получает право обращаться к внутренним службам, во входных данных может оказаться текст, воспринимаемый ею как указание. Внедрение вредоносных инструкций через документы и записи в базах данных входит в число основных угроз для систем с языковыми моделями наряду с отравлением обучающих данных и утечкой сведений ограниченного доступа [2]. Разграничение прав самой модели, а не только пользователя, от имени которого она работает, становится обязательным требованием.

Третье ограничение – трудность объективной оценки: привычные показатели работоспособности мало говорят о полезности ответов, а экспертная проверка дорога и плохо масштабируется. Обследование промышленных внедрений показывает, что большинство систем не выходит за пределы ответов на вопросы по узкой предметной области и остаётся на стадии опытных образцов [4]. Четвёртое ограничение организационное: не определено, кто отвечает за решение, принятое сотрудником по подсказке модели. Пока это не закреплено во внутренних регламентах, работники избегают опоры на новый инструмент, и вложения не окупаются.

Отдельного внимания требует интеграция языковой модели с прикладными программными интерфейсами корпоративных систем. В отличие от информационного поиска, выполнение операций в системах документооборота, управления ресурсами и обслуживания клиентов связано с изменением записей и возникновением юридически значимых последствий. Поэтому модели не следует предоставлять прямой неограниченный доступ к функциям создания, изменения и удаления данных. Безопасная архитектура предполагает использование промежуточного программного слоя, который проверяет параметры запроса, учитывает полномочия пользователя, ограничивает перечень допустимых операций и требует подтверждения критически важных действий.

Результативность внедрения также зависит от организации жизненного цикла системы. Корпоративные документы, регламенты и справочные материалы постоянно изменяются, вследствие чего поисковый индекс и набор контрольных заданий должны регулярно обновляться. До промышленного запуска необходимо сформировать выборку типовых запросов, определить допустимый уровень ошибок и проверить ответы с участием специалистов предметной области. После внедрения требуется собирать обезличенную статистику запросов, фиксировать случаи отказа и недостоверных ответов, а также периодически пересматривать инструкции модели.

Языковые модели дают эффект там, где основную долю трудозатрат составляет работа с текстом. Наиболее устойчивым способом интеграции остаётся надстройка с поиском по внутренним хранилищам, сочетающая приемлемую стоимость с контролем над данными. Вместе с тем недостоверность отдельных ответов, уязвимость к внедрению вредоносных указаний и сложность оценки качества не позволяют рассматривать такие системы как самостоятельных исполнителей. Практический ориентир – закрепить за моделью роль подготовительного звена, оставив решение и ответственность за человеком, и подкрепить это разграничением прав, протоколированием и внутренними регламентами применения.

Библиографический список

1. Антонов И. В., Бруттан Ю. В. Применение больших языковых моделей для интеллектуального поиска и извлечения информации в корпоративных информационных системах // Компьютерные исследования и моделирование. – 2025. – Т. 17, № 5. – С. 871–888.

2. Евглевская Н. В., Казанцев А. А. Обеспечение безопасности сложных систем с интеграцией больших языковых моделей: анализ угроз и методов защиты // Экономика и качество систем связи. – 2024. – № 4 (34). – С. 129–144.

3. Частикова В. А., Бахтин А. С., Меркулов П. А. Разработка методики интеграции больших языковых моделей в процессы центра мониторинга информационной безопасности // Известия ЮФУ. Технические науки. – 2025. – № 4. – С. 57–69.

4. Brehme L., Dornauer B., Ströhle T., Ehrhart M., Breu R. Retrieval-augmented generation in industry: an interview study on use cases, requirements, challenges, and evaluation // arXiv preprint arXiv:2508.14066. – 2025.

5. Sharma C. Retrieval-augmented generation: a comprehensive survey of architectures, enhancements, and robustness frontiers // arXiv preprint arXiv:2506.00054. – 2025.