

ОБЪЯСНИМЫЕ LLM-СИСТЕМЫ В ЭЛЕКТРОННОМ ПРАВИТЕЛЬСТВЕ УЗБЕКИСТАНА: ОБЗОР ПОДХОДОВ К БЕЗОПАСНОЙ РАБОТЕ С ГОСУДАРСТВЕННЫМИ ДАННЫМИ

Gaipnazarov Rustam¹[0000-0002-0049-8967]

Kuznetsova Viktoriya²[0009-0004-1329-9694]

Хусайдинова Дилобар³[0009-0001-6162-4330]

¹*Tashkent University of information technologies named after Muhammad al Kwarazmi, Faculty of Computer Engineering, Teacher, Tashkent 100084, Amir Temur Avenue 108, Uzbekistan*

r.gaipnazarov@tuit.uz

²*Tashkent University of information technologies named after Muhammad al Kwarazmi, Faculty of Computer Engineering, Teacher, Tashkent 100084, Amir Temur Avenue 108, Uzbekistan*

kvb966@yandex.ru

³*Tashkent University of information technologies named after Muhammad al Kwarazmi, Faculty of Computer Engineering, Teacher, Tashkent 100084, Amir Temur Avenue 108, Uzbekistan*

d.xusaydinova@tuit.uz

Аннотация (Abstract)

Развитие больших языковых моделей привело к появлению нового класса интеллектуальных систем, способных работать с естественным языком, структурированными таблицами, документами и мультимодальными данными. Для электронного правительства это открывает заметные возможности: упрощение взаимодействия с государственными сервисами, ускорение поиска информации, автоматизацию аналитических задач и повышение доступности цифровых услуг. Вместе с тем в государственном секторе требования к таким системам существенно строже, чем в коммерческой среде. Здесь важны не только точность и удобство, но и объяснимость, проверяемость, безопасность обработки данных, соблюдение ролевых ограничений и возможность человеческого контроля. В современных исследованиях уже прослеживается переход от прямого использования LLM к более сложным архитектурам, где языковая модель взаимодействует с базами данных, внешними инструментами и специализированными модулями через промежуточные слои управления. В локальных публикациях по Узбекистану отдельно подчеркиваются значение кибербезопасности, необходимость защищённого обращения с данными и растущая роль ИИ в прикладных системах управления.

Цель работы состоит в формировании концептуальной модели explainable LLM-системы для электронного правительства Узбекистана на основе обзорно-аналитического синтеза современных исследований. В статье использованы методы сравнительного анализа, содержательной классификации и концептуального проектирования. В результате выделены ключевые архитектурные принципы explainable LLM-систем: реляционный семантический слой, промежуточный контур контроля доступа, модульное агентное разбиение задач, прослеживаемость происхождения результата, человеческая верификация и аудит. На этой основе предложена архитектура безопасной LLM-системы для работы с государственными данными. Полученные результаты могут использоваться как теоретическая и проектная основа при создании интеллектуальных помощников для государственных порталов, межведомственных информационных систем и аналитических сервисов.

Ключевые слова: LLM, электронное правительство, explainable AI, базы данных, кибербезопасность, государственные данные, Узбекистан.

Введение (Introduction)

Электронное правительство давно перестало быть просто цифровой витриной государственных услуг. За привычными пользовательскими интерфейсами сегодня стоят распределённые базы данных, аналитические модули, межведомственные обмены, архивы документов и потоки неструктурированной информации. На этом фоне естественно растёт интерес к языковым системам, способным принимать запросы в свободной форме, объяснять процедуры, находить релевантные сведения и помогать в работе с большими объёмами данных. Однако в государственном секторе сама постановка задачи оказывается сложнее, чем в обычных чат-интерфейсах. Если модель взаимодействует с государственными данными, она начинает работать в пространстве, где цена ошибки заметно выше: неверный ответ может исказить административную процедуру, нарушить режим доступа или подорвать доверие к цифровому сервису.

Современные исследования на стыке LLM и систем управления данными хорошо показывают, почему вопрос объяснимости здесь выходит на первый план. В работе о KathDB подчёркивается, что традиционные DBMS обеспечивают строгую семантику и эффективную оптимизацию запросов, но плохо приспособлены к работе с мультимодальными данными и естественным языком, тогда как многие новые LLM-ориентированные решения жертвуют объяснимостью ради гибкости [1]. В исследовании iPDB, напротив, демонстрируется возможность встраивания LLM-предикатов внутрь SQL-контуров, что расширяет выразительность запросов, но одновременно делает проблему контроля и оптимизации ещё более чувствительной [2]. В ReFuGe языковые агенты работают уже не как единичный генератор ответа, а как распределённый механизм выбора схемы, генерации признаков и фильтрации результатов в реляционных базах данных [3]. В X-GridAgent агентная архитектура строится вокруг планирования, координации и исполнения задач через профессиональные инструменты и базы знаний, что особенно важно для критически важных доменов [4].

Для Узбекистана такой поворот к интеллектуальным цифровым системам имеет практическое значение. В локальной публикации по информационной безопасности и защите программного обеспечения подчёркивается роль ISO/IEC 27001, законов об информатизации и электронном правительстве, а также важность криптографии, безопасного программирования, национальных стратегий кибербезопасности и культуры безопасного обращения с данными [5]. В другой работе, посвящённой интеллектуальному управлению городским транспортом в Узбекистане, показано, что интеграция больших данных и ИИ уже рассматривается как реальный путь повышения эффективности управления сложными городскими процессами [6]. Наконец, в публикации об оптимизации баз данных с помощью искусственного интеллекта подчёркивается, что современные БД становятся объектом интеллектуального управления, а автоматизация работы с индексами и запросами рассматривается как ответ на рост нагрузки и усложнение информационных систем [7].

На этом фоне возникает исследовательский вопрос: какой должна быть explainable LLM-система для электронного правительства Узбекистана, если её задача заключается не только в удобном взаимодействии с пользователем, но и в безопасной, контролируемой и

проверяемой работе с государственными данными? Ответ на этот вопрос и составляет основное содержание настоящего исследования.

Методы (Methods)

Работа выполнена в обзорно-аналитическом дизайне с опорой на концептуальное моделирование. В качестве корпуса источников использованы семь материалов, загруженных пользователем: четыре современные англоязычные публикации, посвящённые explainable DBMS, LLM-предикатам, агентным архитектурам и генерации признаков в реляционных базах данных [1–4], а также три русско- и узбекоязычные публикации, связанные с информационной безопасностью, искусственным интеллектом в транспортной инфраструктуре Узбекистана и интеллектуальной оптимизацией баз данных [5–7].

На первом этапе был выполнен содержательный анализ источников с выделением повторяющихся понятий, архитектурных решений и рисков. На этом этапе внимание сосредоточивалось на пяти аналитических осях: способ интеграции LLM с базами данных; наличие или отсутствие промежуточного управляющего слоя; механизмы объяснения результатов; роль внешних инструментов и специализированных серверов; способы снижения ошибок и повышения доверия [1–4]. Для локальных публикаций отдельно анализировались положения, связанные с информационной безопасностью, применением ИИ в управленческих системах и задачами защиты данных в условиях Узбекистана [5–7].

На втором этапе проводилось сравнительное сопоставление выделенных решений. В центре внимания находились не предметные области самих работ, а их переносимые архитектурные идеи. Так, из KathDB извлекались принципы реляционного семантического слоя, трассировки происхождения результата и human-AI interaction [1]. Из iPDB — подход к встраиванию LLM в запросный контур и связанная с этим проблема стоимости, латентности и контроля семантических операций [2]. Из ReFuGe — идея разделения функций между несколькими специализированными агентами и итеративного цикла самоулучшения [3]. Из X-GridAgent — трёхслойная агентная архитектура и принцип обращения к внешним профессиональным инструментам через координационный слой [4]. Из локальных публикаций выделялись требования к защищённости данных, использованию криптографии, ролевому разграничению и ориентации ИИ-систем на реальные задачи управления в Узбекистане [5–7].

На третьем этапе выполнялся синтез результатов в виде концептуальной архитектуры explainable LLM-системы для электронного правительства. Здесь использовался метод проектного обобщения: вместо эмпирической проверки модели строилась теоретическая архитектура, согласующаяся с рассмотренными публикациями и учитывающая специфику государственного сектора. Такой подход оправдан для тезисов обзорно-аналитического типа, где основным результатом является не эксперимент, а содержательно обоснованная модель.

Результаты (Results)

Проведённый анализ показал, что современные LLM-системы, ориентированные на работу с данными, можно условно разделить на три направления. Первое направление строится вокруг explainable DBMS, где задача состоит в том, чтобы не потерять реляционную строгость и прослеживаемость результата при добавлении мультимодальных и языковых модулей. В KathDB эта проблема решается через единый реляционный семантический слой, поэтапное разложение запроса, пользовательскую верификацию и

хранение lineage-информации, позволяющей объяснять как отдельные кортежи, так и весь вычислительный конвейер [1]. Это направление особенно важно для электронного правительства, поскольку показывает, что объяснимость должна строиться не поверх результата, а внутри архитектуры.

Второе направление связано с расширением SQL и запросных механизмов за счёт LLM-предикатов и семантических операций. iPDB демонстрирует, что языковая модель может использоваться как часть выборки, соединения и группировки, а сама система способна уменьшать стоимость и задержки за счёт дедупликации промптов, пакетной обработки, параллелизации и переупорядочивания семантических предикатов [2]. Вместе с тем именно эта работа показывает и пределы прямого сближения LLM и баз данных. Чем глубже языковая модель встроена в запросный контур, тем больше требуется контролировать маршрутизацию, стоимость, допустимые операции и число вызовов. Для государственного сектора это означает необходимость специального ограничительного слоя между пользовательским запросом и выполнением операций над чувствительными данными.

Третье направление представлено агентными архитектурами. ReFuGe показывает, что одна модель не обязана выполнять все функции сразу; вместо этого разные агенты могут отвечать за выбор релевантных таблиц, генерацию признаков и фильтрацию результатов [3]. X-GridAgent развивает эту идею дальше и строит трёхуровневую архитектуру из слоёв планирования, координации и действия, где LLM не подменяет профессиональные инструменты, а организует их использование через внешний серверный контур [4]. Для электронного правительства это особенно важно: надёжность достигается не тем, что LLM умеет “самостоятельно всё понять”, а тем, что она работает в окружении контролируемых модулей, каждый из которых отвечает за ограниченный класс операций.

Сопоставление международных работ с локальными публикациями позволило выделить несколько общих требований к explainable LLM-системе в государственном секторе Узбекистана. Во-первых, система должна исходить из принципа защищённости данных по умолчанию. Локальная статья по информационной безопасности подчёркивает значимость безопасного программирования, криптографической защиты, системных мер кибербезопасности и соответствия таким нормативным основам, как ISO/IEC 27001 и закон об электронном правительстве [5]. Во-вторых, ИИ-система должна проектироваться как прикладной инструмент управления, а не как абстрактный эксперимент. Это хорошо видно на примере статьи о транспорте, где ИИ и большие данные включаются в архитектуру реального городского управления и локализуются под условия Ташкента [6]. В-третьих, БД в современных системах уже сами становятся объектом интеллектуального управления, что подтверждается публикацией об оптимизации индексов и SQL-запросов на основе reinforcement learning [7]. Следовательно, электронное правительство сталкивается не с одной новой технологией, а с наложением двух процессов: интеллектуализации данных и интеллектуализации интерфейса доступа к ним.

На основании этого синтеза предложена концептуальная архитектура explainable LLM-системы для электронного правительства Узбекистана. На входе располагается интерфейс естественного языка, принимающий запрос гражданина или сотрудника. Далее запрос поступает в модуль классификации, который определяет категорию задачи, чувствительность данных и допустимый режим ответа. После этого включается policy-gateway, проверяющий роль пользователя, доступный уровень детализации и разрешённый

маршрут обработки. Следующий слой представляет собой безопасный контур доступа к данным: вместо прямого обращения к государственным БД LLM взаимодействует только с разрешёнными представлениями, API, шаблонами запросов или специализированными сервисами. Над этим слоем находится модуль сборки ответа и модуль объяснения. Первый формирует результат, второй показывает, из каких источников получен ответ, какие ограничения применялись, почему часть сведений была скрыта и какие этапы обработки были выполнены. Все действия фиксируются в модуле аудита. Для чувствительных сценариев финальный ответ дополнительно передаётся на человеческую верификацию. Такая архитектура объединяет реляционную прослеживаемость [1], ограниченную семантическую обработку запросов [2], агентное разбиение функций [3] и координацию через внешний инструментальный слой [4] с локальными требованиями безопасности [5–7].

Обсуждение (Discussion)

Полученные результаты позволяют сделать несколько выводов, имеющих значение не только для теории, но и для практики проектирования цифрового государства. Первый вывод заключается в том, что explainability в LLM-системах нельзя понимать как способность модели “объяснить себя” в текстовой форме. Такой подход слишком слаб для государственного сектора. В проанализированных работах объяснимость возникает там, где архитектура сохраняет структуру запроса, фиксирует происхождение промежуточных результатов, позволяет человеку вмешиваться в ход выполнения и отделяет языковую интерпретацию от критических операций над данными. Для электронного правительства это означает, что объяснение должно относиться не только к содержанию ответа, но и к маршруту его получения.

Второй вывод состоит в том, что LLM не следует рассматривать как автономный субъект доступа к государственным данным. Хотя iPDB показывает техническую возможность тесной интеграции LLM и SQL, такая близость увеличивает риски бесконтрольного исполнения семантических операций и усложняет обеспечение предсказуемости. Поэтому для государственного сектора более реалистичной выглядит модель, где языковая система работает через промежуточный контур ограничителей. В таком контуре запрос сначала переводится в допустимую форму, затем проходит через механизмы ролевой проверки и только после этого попадает к данным.

Третий вывод касается роли агентности. В ReFuGe и X-GridAgent убедительно показано, что сложная задача лучше решается не одной моделью, а системой специализированных модулей, распределяющих обязанности между выбором схемы, планированием, координацией и исполнением. Для электронного правительства этот принцип особенно полезен, потому что он позволяет разнести ответственность между компонентами системы. Один модуль отвечает за смысл запроса, другой — за соответствие политике доступа, третий — за выполнение допустимой операции, четвёртый — за объяснение и аудит. Такой подход снижает зависимость от единственной модели и делает систему лучше управляемой.

Четвёртый вывод касается узбекского контекста. Локальные публикации показывают, что дискуссия о безопасности данных, о роли ИИ в управлении и об интеллектуализации инфраструктуры уже идёт не на абстрактном, а на прикладном уровне. Поэтому разговор об explainable LLM для электронного правительства Узбекистана не является преждевременным. Напротив, именно сейчас существует шанс задать правильную

архитектурную рамку до того, как языковые интерфейсы будут встроены в чувствительные государственные процессы без достаточных ограничителей.

При этом у предложенной модели есть ограничения. Настоящая работа носит обзорно-аналитический характер и не включает эмпирическую валидацию архитектуры на реальных государственных данных. Кроме того, часть использованных международных работ относится к другим предметным областям — мультимодальным данным, прогнозным задачам на реляционных БД и анализу энергосистем. Однако их ценность для настоящего исследования заключается не в предметной специфике, а в переносимых принципах проектирования: модульности, прослеживаемости, промежуточных слоях управления и участия человека. Именно эти принципы и представляются наиболее перспективными для адаптации в электронном правительстве Узбекистана.

Заключение (Conclusion)

Проведённый обзор показал, что внедрение больших языковых моделей в электронное правительство требует перехода от простой модели “интеллектуального помощника” к архитектуре, в которой объяснимость и безопасность изначально заложены в контур работы системы. Современные исследования на стыке LLM, агентных архитектур и систем управления данными подтверждают, что наибольшую устойчивость демонстрируют решения, где языковая модель не получает прямой и неконтролируемый доступ к данным, а действует через промежуточные механизмы семантической интерпретации, ролевой фильтрации, внешних инструментов и модулей объяснения.

Для условий электронного правительства Узбекистана такой подход имеет особую значимость. Локальные публикации показывают, что вопросы кибербезопасности, защищённого программного обеспечения, интеллектуального управления данными и применения ИИ в инфраструктурных и базоданных системах уже приобрели прикладной характер. Это означает, что обсуждение explainable LLM для государственных данных не является теоретическим упражнением. Напротив, оно связано с будущей архитектурой государственных цифровых сервисов, в которых от системы требуется не только удобство и скорость ответа, но и соблюдение правовых, организационных и технических ограничений.

На основе выполненного анализа предложена концептуальная модель explainable LLM-системы для электронного правительства Узбекистана, включающая интерфейс естественного языка, модуль классификации запроса, policy-gateway, безопасный слой доступа к данным, модуль объяснения, журнал аудита и механизм human-in-the-loop. Научная ценность предложенной модели состоит в синтезе международных архитектурных подходов и локального контекста информационной безопасности. Практическая ценность заключается в том, что данная модель может служить ориентиром при разработке интеллектуальных государственных порталов, аналитических сервисов и межведомственных систем, работающих с чувствительными данными.

К итогу, explainable LLM-системы в электронном правительстве Узбекистана следует проектировать не как автономный “чёрный ящик”, а как контролируемый интеллектуальный слой над государственными данными. Дальнейшие исследования целесообразно направить на разработку формальных политик доступа, моделей оценки объяснимости, механизмов верификации ответов и пилотных сценариев внедрения в реальных цифровых сервисах государства.

References

1. Xiao G., Zhang E., Sullivan N., Hansen W., Balazinska M. *KathDB: Explainable Multimodal Database Management System with Human-AI Collaboration*. Vision Paper. CIDR 2026.
2. Kumarasinghe U., Liu T., Liu C., Aref W. G. *iPDB - Optimizing SQL Queries with ML and LLM Predicates*. 2026.
3. Kim K., Lee G., Kim J., Choi D., Kang S., Shin K. *ReFuGe: Feature Generation for Prediction Tasks on Relational Databases with LLM Agents*. Proceedings of the ACM Web Conference 2026.
4. Wen Y., Chen X. *X-GridAgent: An LLM-Powered Agentic AI System for Assisting Power Grid Analysis*. 2025.
5. Gaipnazarov R., Azimov Sh., Shukrullayev F. *Axborot xavfsizligi va dasturiy ta'minotda himoya vositalari*. DIGITAL TRANSFORMATION: A NEW ERA IN INFORMATION TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND THE ECONOMY") (RITM-2025)", Toshkent, 16-17 aprel 2025-yil
6. Хужакулов Т. А., Гаипназаров Р. Т., Азимов Ш. *Большие данные (Big Data) и искусственный интеллект (AI) для интеллектуального управления городским транспортом в Узбекистане*. DIGITAL TRANSFORMATION: A NEW ERA IN INFORMATION TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND THE ECONOMY") (RITM-2025)", Toshkent, 16-17 aprel 2025-yil
7. Гаипназаров Р., Jo'raboyev F., Mamatqulov M. *Оптимизация баз данных с помощью искусственного интеллекта (ИИ): автоматическое управление индексами и запросами с использованием reinforcement learning*. DIGITAL TRANSFORMATION: A NEW ERA IN INFORMATION TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND THE ECONOMY") (RITM-2025)", Toshkent, 16-17 aprel 2025-yil