Версионная архитектура интеллектуальной системы поддержки групповых решений по классификации объектов аналитического хранилища

А. С. Филатов*

Предложена версионная архитектура интеллектуальной системы для группового решения о включении объектов аналитического хранилища в контур управления персональными данными. Прогноз модели, ответы экспертов и итоговая метка привязаны к версии объекта; подтверждение требует согласия участников и наличия обязательных ролей. На контрольной выборке из 9 379 столбцов локальная модель получила $F_1 = 0{,}883$.

Ключевые слова: аналитическое хранилище, происхождение данных, персональные данные, групповое решение.

1. Постановка задачи

Объекты аналитического хранилища меняются от версии к версии, поэтому решение о включении объекта в контур управления персональными данными (ПДн) принимается для пары «объект–версия» по метаданным. Метка DI означает, что основание для включения есть, NPD — что в данной версии оно не найдено. За решение отвечают конкретные роли, и метка должна быть связана с версией объекта, моделью и ответами людей. Средства сквозного происхождения [1] фиксируют данные, код и модели конвейера машинного обучения, но не управленческое решение и его участников. Методы передачи решения эксперту [2] распределяют объекты между моделью и экспертами по ожидаемой точности и нагрузке и не учитывают полномочий ролей. По данным метаанализа [3], совместная работа человека и модели в среднем уступает лучшему из них, поэтому эксперту стоит передавать только те случаи, где проверка окупается.

В отличие от [1], решение хранится как неизменяемая запись, привязанная к версии объекта, модели и ответам экспертов. Компетентность

* *Филатов Александр Сергеевич* — аспирант, Московский государственный университет технологий и управления имени К. Г. Разумовского (Первый казачий университет), Москва, e-mail: shzgudzh@gmail.com.

Filatov Alexander Sergeevich — PhD student, K. G. Razumovsky Moscow State University of Technologies and Management (the First Cossack University), Moscow.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

эксперта, в отличие от [2], используется только для его выбора, а подтвердить или заблокировать метку могут лишь обязательные роли и роли с правом вето. Политика отбора на проверку сравнивает ожидаемые потери автоматической метки со стоимостью проверки и дополнительно учитывает расхождение моделей и неполноту метаданных.

2. Модель решения и архитектура

Версия t хранилища описывается типизированным графом $\mathcal{G}^{(t)}$ объектов, метаданных, преобразований и связей происхождения. Опубликованные записи не перезаписываются: изменение объекта создает новую версию. Поэтому для каждой метки восстанавливаются использованные снимок, модель и участники [1].

Локальная модель оценивает калиброванную вероятность p_i^L класса DI по метаданным, а модель с фиксированной графовой агрегацией — вероятность p_i^G с учетом окрестности в $\mathcal{G}^{(t)}$; GraphSAGE [4] проверяется как отдельная альтернатива. Пусть $m_i \in [0,1]$ — доля отсутствующих метаданных, $\kappa_i = |p_i^L - p_i^G|$ — расхождение моделей, а

$$L_{\mathrm{DI}} = c_{\mathrm{FP}}(1 - p_i^L), \qquad L_{\mathrm{NPD}} = c_{\mathrm{FN}} p_i^L, \qquad L_R = c_R + c_{\mathrm{res}}.$$

Здесь c_{FP} и c_{FN} — стоимости ошибок, c_R — стоимость экспертной проверки, c_{res} — остаточный риск после нее. Политика Ψ_i выбирает класс с меньшим L_c, если $\min_c L_c < L_R$, $m_i \le m_{\max}$ и $\kappa_i \le \kappa_{\max}$; иначе объект получает действие REVIEW.

Эксперт e дает ответ $a_{ie} \in \{\mathrm{DI}, \mathrm{NPD}, \perp\}$, где $\perp$ означает отсутствие решения. Класс c подтверждается, если по каждой обязательной роли получен ответ c, ни один ответ обязательной роли ему не противоречит и отсутствует возражение роли с правом вето; иначе назначается новый раунд или эскалация. Критерии архитектуры — восстановимость версии, модели и участников; неизменяемость опубликованных записей; прохождение моделью quality gate. В прототипе проверены связь машинных артефактов с версией и quality gate с ограничениями $\mathrm{Recall}_{\mathrm{DI}} \ge 0{,}60$ и $\mathrm{AP} \ge 0{,}35$; неизменяемость и ролевой протокол заданы как проектные инварианты.

3. Проверка на прототипе и выводы

Прототип проверен на снимке метаданных хранилища предприятия электронной коммерции: 5 148 объектов, 64 675 столбцов, граф из 69 823 вершин и 130 019 отношений. Слабые целевые метки сформированы эвристи-

ками по именам и описаниям столбцов. Обучающая часть содержит 48 840 столбцов (2 013 DI), калибровочная — 3 185 (191 DI), валидационная — 3 271 (229 DI), контрольная — 9 379 (286 DI) из 219 компонентов связности графа происхождения. Между частями нет графовых связей и точных совпадений текстового представления.

Локальная модель использует признаки TF-IDF по word n-grams ($n = 1$–2) и char n-grams ($n = 3$–5) для имен базы, схемы, таблицы и столбца, типа и описания; использована логистическая регрессия с балансировкой классов и $C = 32$. Фиксированная графовая модель объединяет 96-мерные векторы SVD с усредненными по типам связей векторами соседей и степенями вершин ($C = 0{,}5$). Типизированная GraphSAGE имеет два слоя по 128 признаков, dropout 0,2 и обучается Adam с learning rate 10^{-3} не более 100 эпох, ранней остановкой после 15 эпох и ансамблем пяти запусков. Вероятности калиброваны методом temperature scaling; пороги 0,780, 0,803 и 0,903 соответственно выбраны по валидационной части при $\mathrm{Recall}_{\mathrm{DI}} \geq 0{,}60$.

Таблица 1: Качество классификации столбцов (класс DI)

Модель	Точность	Полнота	F_1	AP
Логистическая регрессия по TF-IDF	0,871	0,895	0,883	0,896
Фиксированная агрегация по графу	0,532	0,441	0,482	0,481
Типизированная GraphSAGE	0,853	0,465	0,602	0,654

Графовые модели уступили локальной и по F_1, и по средней точности AP. 95 %-й доверительный интервал F_1 локальной модели равен [0,820; 0,938] (percentile cluster bootstrap): 1 000 раз с возвращением выбирались 219 компонентов связности со всеми их столбцами.

В политике заданы $c_{\mathrm{FN}} = 5$, $c_{\mathrm{FP}} = 1$, $c_R = 0{,}35$, $c_{\mathrm{res}} = 0{,}05$, $m_{\max} = 0{,}75$ и $\kappa_{\max} = 0{,}60$. На проверку направлены 583 из 9 379 столбцов (6,216 %). Среди остальных 60 ошибок: 8 пропусков DI (FN) и 52 ложных срабатывания (FP).

При слабых метках, построенных по именам и описаниям столбцов, граф происхождения не улучшил классификацию по сравнению с метаданными самого столбца, а политика отбора передала экспертам около 6 % столбцов.

Список литературы

[1] M. Schlegel, K.-U. Sattler, "Capturing end-to-end provenance for machine learning pipelines", *Information Systems*, **132** (2025), 102495. DOI: 10.1016/j.is.2024.102495.

[2] C. Nguyen, T.-T. Do, G. Carneiro, "Probabilistic Learning to Defer: Handling Missing Expert Annotations and Controlling Workload Distribution", *Proceedings of the Thirteenth International Conference on Learning Representations*, 2025.

[3] M. Vaccaro, A. Almaatouq, T. Malone, "When combinations of humans and AI are useful: A systematic review and meta-analysis", *Nature Human Behaviour*, **8**:12 (2024), 2293–2303. DOI: 10.1038/s41562-024-02024-1.

[4] W. L. Hamilton, R. Ying, J. Leskovec, "Inductive Representation Learning on Large Graphs", *Advances in Neural Information Processing Systems 30*, 2017, 1024–1034, arXiv: 1706.02216.

Статья поступила 10 октября 2026 г.

A Versioned Architecture of an Intelligent Group Decision Support System for Classifying Analytical Data Warehouse Objects

A. S. Filatov

A versioned architecture of an intelligent information system is proposed for group decisions on placing analytical data warehouse objects under personal data governance. Model predictions, expert answers and final labels are tied to the object version; confirmation requires expert agreement and the presence of all mandatory roles. On a held-out set of 9,379 columns, a local model reached $F_1 = 0.883$.

Keywords: data warehouse, data lineage, personal data, group decision.

References

[1] M. Schlegel, K.-U. Sattler, "Capturing end-to-end provenance for machine learning pipelines", *Information Systems*, **132** (2025), 102495. DOI: 10.1016/j.is.2024.102495.

[2] C. Nguyen, T.-T. Do, G. Carneiro, "Probabilistic Learning to Defer: Handling Missing Expert Annotations and Controlling Workload Distribution", *Proceedings of the Thirteenth International Conference on Learning Representations*, 2025.

[3] M. Vaccaro, A. Almaatouq, T. Malone, "When combinations of humans and AI are useful: A systematic review and meta-analysis", *Nature Human Behaviour*, **8**:12 (2024), 2293–2303. DOI: 10.1038/s41562-024-02024-1.

[4] W. L. Hamilton, R. Ying, J. Leskovec, "Inductive Representation Learning on Large Graphs", *Advances in Neural Information Processing Systems 30*, 2017, 1024–1034, arXiv: 1706.02216.

Received on October 10, 2026