УДК 004.91+004.031.42

ОПТИМИЗАЦИЯ ИНФРАСТРУКТУРЫ ВЗАИМОДЕЙСТВИЯ В ИНТЕЛЛЕКТУАЛЬНОЙ СРЕДЕ WEB 3.0

OPTIMIZATION OF THE INTERACTION INFRASTRUCTURE IN THE INTELLIGENT WEB 3.0 ENVIRONMENT

Бурый А.С., д-р техн. наук, ФГБУ «Институт стандартизации» (Москва, Россия)

Хамидуллин А.Р., аспирант, ФГБУ «Институт стандартизации» (Москва, Россия)

Анисимов Н.Р., канд. физ.-мат. наук, ФГБУ «Институт стандартизации» (Москва, Россия)

Buryi, A.S., Dr.Sc. (Technology), Russian Standardization Institute (Moscow, Russia)

Khamidullin, A.R., graduate student, Russian Standardization Institute (Moscow, Russia)

Anisimov, N.R., PhD in Physics and Mathematics, Russian Standardization Institute (Moscow, Russia)

Целью исследования является снижение совокупного риска внесения недостоверных данных в распределенные базы данных Web 3.0 агентами искусственного интеллекта (ИИ), за счет разработки математической модели динамической фильтрации информационных потоков и оптимизации пороговых параметров контура человеческого контроля в условиях ограниченного временного ресурса оператора.

Методы: методологическую основу исследования составляет системный анализ информационных процессов в децентрализованных средах, методы теории эргатических систем, аппараты математического моделирования и теории принятия решений в условиях риска и временных ограничений».

Представлена и проанализирована синергия сотрудничества между агентами искусственного интеллекта и блокчейном в распределенных сетях Web 3.0. Показана роль метрик доверия в задачах формирования распределенных баз данных.

The aim of the study is to reduce the cumulative risk of introducing inaccurate data into distributed Web3 databases by AI agents by developing a mathematical model for dynamic filtering of information flows and optimizing the threshold parameters of the human control contour in conditions of a limited time resource of the operator.

Methods: the methodological basis of the research is a systematic analysis of information processes in decentralized environments, methods of ergatic systems theory, mathematical modeling and decision theory in conditions of risk and time constraints.

The synergy of cooperation between artificial intelligence agents and blockchain in distributed Web 3.0 networks is presented and analyzed. The role of trust metrics in the tasks of forming distributed databases is shown.

Ключевые слова: Web 3.0, агент ИИ, блокчейн, распределенная база данных, многоагентное взаимодействие, динамическая фильтрация, контур человеческого контроля.

Keywords: Web 3.0, AI agent, blockchain, distributed database, multi-agent interaction, dynamic filtering, Human-in-the-Loop.

Для цитирования: Бурый А.С., Хамидуллин А.Р., Анисимов Н.Р. Оптимизация инфраструктуры взаимодействия в интеллектуальной среде Web 3.0 // Информационно-экономические аспекты стандартизации и технического регулирования. 2026. № 5 (92). С. 79–84.

For citation: Buryi A.S., Khamidullin A.R., Anisimov N.R. Optimization of the interaction infrastructure in the intelligent Web 3.0 environment. Information and economic aspects of standardization and technical regulation, 2026, no. 5(92), pp. 79–84. (In Russ.).

ВВЕДЕНИЕ

Быстроразвивающийся рынок Web3.0 (по прогнозам – это более 81 млрд долларов США к 2033 году[1]) предлагает преобразующий переход от традиционных централизованных онлайн-платформ к децентрализованной интернет-экосистеме, управляемой пользователями. Ключевыми элементами Web 3.0 выступают: децентрализация информационных процессов, использование сквозных технологий распределенных реестров (блокчейн) и интеллектуализация систем управления, в частности на основе смарт-контактов [1]. Перспективой следующего этапа эволюции – Web 4.0 заявлено развитие интеллектуальности (разумности) веб-технологий, в том числе и за счет активного применения интеллектуальных агентов [1, 2]. Не смотря на перспективы Web 4.0, полная реализация Web3.0 еще не достигнута. Различные инициативы и проекты активно создают необ-

[1] Размер мирового рынка Web3.0, тенденции роста, доля отрасли и прогноз на 2026–2034 гг. Доступно онлайн: https://www.verifiedmarketreports.com/ru/product/web3-0-market/ (дата обращения: 10.10.2026).

ходимую инфраструктуру и инструменты для децентрализованной сети [3].

В условиях интенсивной динамики роста объемов обрабатываемых данных и жестких требований к пропускной способности систем обработки транзакций традиционные централизованные архитектуры баз данных (БД) характеризуются деградацией масштабируемости и подверженностью уязвимостям. Перспективным подходом к нивелированию данных ограничений является распределение функций сбора, анализа и локальной фиксации данных между автономными агентами искусственного интеллекта (агенты ИИ), функционирующими в облачных и периферийных узлах сети [4]. При этом для обеспечения децентрализованной координации, верификации состояния агентов и достижения консистентности данных в гетерогенной среде целесообразно использование технологии распределенного реестра (блокчейн) [5].

Блокчейн – это децентрализованная распределенная база данных, которая безопасно хранит данные на нескольких узлах. Блокчейн обеспечивает прозрачность, безопасность и децентрализацию, что способствует росту ряда ключевых приложений Web3, таких как децентрализованные финансы (DeFi) и децентрализованные автономные организации (DAO). [6].

Однако масштабное внедрение агентов ИИ в процессы формирования распределенных баз данных (РБД) порождает фундаментальное научное противоречие между высокой степенью автономии децентрализованных систем и рисками принятия некорректных или деструктивных решений на основе невалидированной информации. Возникает критическая необходимость формализации понятия «доверие» к источникам данных и построения математических моделей, регулирующих информационный обмен между человеком-оператором и искусственным интеллектом [7]. Наличие «галлюцинаций» больших языковых моделей [8, 9] и алгоритмические сбои агентов ИИ исключают возможность их полностью автономной работы в критически важных инфраструктурах, что обуславливает актуальность интеграции контура человеческого контроля (Human-in-the-Loop, модели HITL).

Существующие подходы к оценке доверия в распределенных системах зачастую носят качественный характер или перегружают когнитивный ресурс человека-оператора, требуя тотального аудита регистрируемых транзакций. Для минимизации рисков ошибочных решений без потери пропускной способности Web3-среды необходима разработка моделей динамической фильтрации информационных потоков на основе суженного вектора измеряемых метрик доверия. Это позволит перераспределить вычислительную и экспертную нагрузку, направляя ресурс человека исключительно на верификацию высо-корисковых данных.

Целью исследования является снижение совокупного риска внесения недостоверных данных в распределенные базы данных Web 3.0 агентами ИИ за счет разработки математической модели динамической фильтрации информационных потоков и оптимизации пороговых параметров контура человеческого контроля в условиях ограниченного временного ресурса оператора.

1. ФОРМАЛИЗАЦИЯ КОМПОНЕНТОВ ИНФОРМАЦИОННОЙ СРЕДЫ

С позиций системного анализа и теории сложных информационно-управляющих систем интеллектуальная среда Web 3.0, функционирующая в условиях транзакционного обмена данными между децентрализованными агентами искусственного интеллекта (ИИ) и РБД, формализуется в виде кортежа:

$$S = \langle A, D(t), T_A(t), U \rangle, \quad (1)$$

где

a) $A = \{a_i | i = 1, \dots, N\}$ – динамически изменяющееся множество автономных интеллектуальных агентов (агенты ИИ), поставляющих данные в Web3-среду; каждый агент a_i обладает собственной целевой функцией, моделью принятия решений (например, на основе больших языковых моделей [8, 10], экспертная система) и осуществляет генерацию информационных потоков (транзакций) для записи в РБД;

b) $D(t) = \{d_1, d_2, \dots, d_k, \dots, d_M\}$ – распределенная база данных (блокчейн), которая на момент времени t задается, как множество верифицированных и консенсусно принятых записей (транзакций);

c) суженный динамический вектор метрик доверия к агенту ИИ a_i (или генерируемым им данным) вида

$$T_A(t) \to \{T_i(t) = \langle v_i, h_i \rangle \in [0,1]^2, a_i \in A\}, \quad (2)$$

причем для контура человеческого контроля выделим две ключевые измеряемые метрики:

– v_i – *верифицируемость* (вероятность того, что результат работы агента a_i содержит полную и проверяемую трассировку шагов логического вывода (проверка следа происхождения данных);

– h_i – историческая безошибочность (статистическая доля транзакций агента a_i, успешно прошедших верификацию за скользящее временное окно $\Delta\tau$);

– для каждой поступающей транзакции d_k от агента a_i рассчитывается индивидуальный квантифицированный риск[2]:

$$R(d_k) = P_{err}(T_i) \times C(d_k), \quad (3)$$

где $P_{err}(T_i)$ – априорная вероятность ошибки агента на основе вектора T_i, а $C(d_k)$ – цена ошибки (потери/стоимость транзакции в Web 3.0);

[2] Состав категорий угроз включает нарушение конфиденциальности, целостности, прав доступа, неавторизо-ванные транзакции и действия.

d) параметр $U \in [0,1]$ определяет границу автоматического принятия решений: если $R(d_k) \leq U$, транзакция фиксируется в $D(t)$ автоматически («контур автономии»); в противном случае транзакция перенаправляется в «контур человеческого контроля» (Human-in-the-Loop, HITL) для ручной верификации оператором.

Ограничение вектора T_i до двух метрик создает локальную погрешность аппроксимации «истинного» доверия (из-за игнорирования контекстуальных факторов, таких как аномалии сетевой задержки или скоординированные Sybil-атаки). Однако в условиях Web 3.0 и дефицита времени оператора эта погрешность компенсируется следующими факторами: а) расчет v_i и h_i требует минимальных временных затрат при обращении к смарт-контракту, что критически важно для динамической фильтрации в реальном времени; б) на длинных интервалах времени показатель исторической безошибочности h_i аккумулирует в себе латентные переменные других метрик (если агент подвергся атаке или вызывает сбои, его h_i стремительно падает).

2. МАТЕМАТИЧЕСКАЯ ПОСТАНОВКА ЗАДАЧИ ОПТИМИЗАЦИИ РИСКА

Целью управления является нахождение оптимального динамического порога $U^*(t)$, минимизирующего совокупный риск внесения недостоверных данных при жестком ограничении на пропускную способность системы, обусловленную временным ресурсом оператора.

Пусть за интервал времени Δt в систему поступает поток транзакций $M = \{d_1, d_2, \dots, d_m, \dots, d_M\}$, тогда целевую функцию представим как:

$$\min_U \sum_{m=1}^{M} [\mathrm{I}(R(d_m) \leq \mathrm{U}) \cdot R(d_m) + \mathrm{I}(R(d_m) > U) \cdot (1 - \alpha_m)], \quad (4)$$

где M – общее число транзакций/решений за интервал времени Δt; $\alpha_m \in \{0,1\}$ – индикатор включения человеческого контроля для m-й транзакции (0 – решение принято автоматически агентом ИИ, 1 – решение подтверждено человеком).

Существующие ограничения:

1. Ограничение по времени оператора (бюджет внимания):

$$\sum_{m=1}^{M} \mathrm{I}(R(d_m) > U) \cdot \tau_m \leq T_{\text{тр}}. \quad (5)$$

2. Требование к автономии среды (пропускная способность):

$$\frac{1}{M} \sum_{m=1}^{M} \mathrm{I}(R(d_m) > U) \cdot \tau_m \leq T_{\text{тр}}. \quad (6)$$

3. Граничные условия: $U \in [0,1]$

$$\sum_{m=1}^{M} \mathrm{I}(R(d_m) \leq U) \geq \gamma_{min}. \quad (7)$$

где $\mathrm{I}(\cdot)$ – индикаторная функция (равна 1, если условие верно, и 0 в противном случае);

$\alpha_m \in [0,1]$ – эффективность верификации транзакции оператором (вероятность обнаружения ошибки человеком; при идеальном контроле $\alpha_m = 1$, тогда риск в HITL-контуре обнуляется);

τ_m – время, необходимое оператору для анализа и верификации транзакции (d_m), причем при ограничении на ресурс человеческого контроля (время оператора, когнитивная нагрузка), существует общий временной бюджет контроля – $T_{max,}$ что $\sum_{m=1}^{M} \alpha_m \cdot \tau_m \leq T_{max}$.

$T_{\text{тр}}$ – доступный временной ресурс оператора (или пула операторов) за интервал Δt.

γ_{min} – минимально допустимый коэффициент автономности системы (доля транзакций, обрабатываемых без участия человека).

На основе динамического вектора доверия $T_i(t)$ вида (2) найдем интегральный уровень доверия к агенту a_i:

$$T_i(t) = w_1 v_i(t) - w_2 h_i(t), (w_1 + w_2 = 1), \quad (8)$$

где w_1, w_2 — весовые коэффициенты значимости метрик доверия $(w_1 + w_2 = 1)$.

При условии, что риск является обратной функцией от вектора доверия T_a и прямой функцией от «ценности» (или критичности) $C(d_k)$ самой транзакции, перепишем выражение (3) для риска, как:

$$R(d_k) = f(C(d_k), T_i(t)) = C(d_k) \cdot (1 - w_1 v_i - w_2 h_i).$$

3. АРХИТЕКТУРА АГЕНТНОГО МОДЕЛИРОВАНИЯ С КОНТУРОМ ВЕРИФИКАЦИИ

Предлагаемая архитектура декомпозирует процесс взаимодействия агентов ИИ и децентрализованной инфраструктуры на четыре связанных уровня. Функциональная структура взаимодействия основных блоков модели представлена на рис. 1 и включает:

1. Агентный уровень – среда агентов ИИ (на базе фреймворков автономии), отправляющая анализируемые по заданному правилу транзакции с целью их занесения впоследствии в БД.

2. Уровень динамической фильтрации: выполняет роль «интеллектуального шлюза», на основе истории из смарт-контрактов вычисляет T_i на основе выражения (2) и функцию риска $R(d_k)$ по (3), решает оптимизационную задачу и динамически сдвигает порог $U^*(t)$ в зависимости от текущей длины очереди к оператору.

3. Уровень логического контроля фактически контролирует поступающий поток транзакций в соответствии с выражениями (4)–(7). При этом агенты ИИ передают не только сами данные d_k, но и метаданные логического вывода (формируют метрику верифицируемости ($v_i(t)$).

4. Уровень прямой регистрации (при высоком показателе доверия): валидированные данные фиксируются децентрализованными протоколами.

5. Уровень человеческого контроля (оркестратор HITL): инструмент приоритизации задач для операторов (наиболее рискованные транзакции с высокой ценой ошибки идут первыми).

6. Модуль адаптации обеспечивает управление порогами (сдвиг порога U).Если время ожидания превышает критическое, генерируется команда для адаптивного снижения нагрузки. Смарт-контракт автоматически обновляет историческую безошибочность h_i для каждого агента по результатам проверок, для возможности ее использования на следующем шаге времени $(t+1)$.

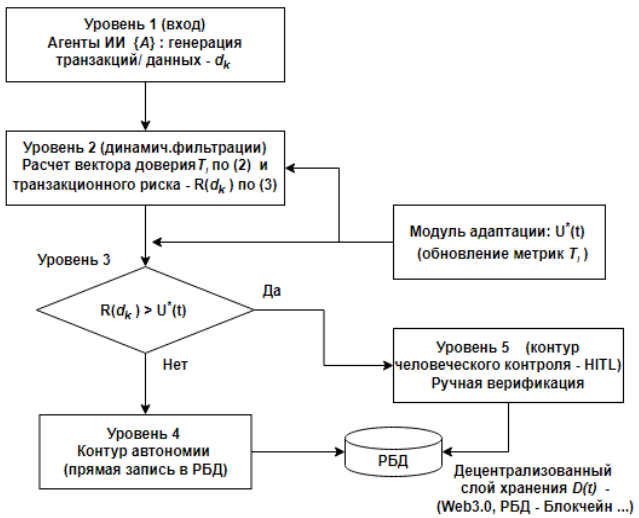


Рис. 1. Функциональная структура агентного моделирования с контуром верификации

Сравнительный анализ с существующими парадигмами агентных систем

Для обоснования предложенного подхода проведено сравнение с тремя доминирующими индустриальными парадигмами: многоагентные системы (МАС) (классические МАС без Web3), LLM-Agent Frameworks (современные среды на основе интеграции больших языковых моделей (LLM) и агентов ИИ) и интеграции с агентными сетями вида DAO/Web3 Agent Networks. По выбранным критериям сравнения предлагаемый подход демонстрирует существенные преимущества, что отражено в табл. 1.

4. ВЫЧИСЛИТЕЛЬНЫЙ ЭКСПЕРИМЕНТ

Цель эксперимента: проверить, как изменение порога человеческого контроля U влияет на совокупный пропущенный риск (риск ошибок, для случая попадания в РБД без проверки) и когнитивную нагрузку на человека (число транзакций, отправленных на ручную проверку).

Выполним моделирование информационного процесса для потока из $M = 1000$ транзакций, генерируемых тремя типами агентов (надежный, нестабильный, вредоносный).

В табл. 2 представлены результаты моделирования осуществления динамического контроля. Величина порога изменяется на интервале $U = [10,70]$ с шагом 10. Анализ результатов эксперимента показывает:

1. Эффект дефицита ресурса (Пороги 10–30): При слишком низком пороге U система пытается отправить на проверку *слишком много* транзакций. Бюджет времени оператора ($T_{max} = 200$) быстро исчерпывается на ранних этапах. В результате критические и высокорисковые транзакции, пришедшие позже, проходят в РБД (блокчейн) без контроля, что удерживает пропущенный риск на высоком уровне.

Таблица 1

Анализ предлагаемого подхода с существующими агентными системами

Критерий сравнения	Классические МАС (JADE, Agent0)	LLM-Agent Frameworks	Web3 Agent Networks	Предлагаемая Web 3.0 архитектура динамического контроля
Парадигма доверия	Закрытая доверенная среда (интранет) в коллективном принятии решений [11]	Отсутствует на уровне протокола	Экономические стимулы	Математическая фильтрация риска на основе верифицируемости в контексте зависимости (2)
Управление ресурсом оператора (HITL)	Статический вызов прерывания (HITL отсутствует либо жестко зашит)	Интерактивный ввод пользователя в консоли (блокирует поток, не масштабируется)	Голосование в DAO (рост временных затрат)	Динамическая оптимизация порога $U^*(t)$ под бюджет времени оператора
Реакция на динамику потока данных	Не адаптируется к перегрузкам	Падение по таймауту API/контекста	Рост стоимости, деградация пропускной способности	Адаптивный сдвиг порога автономности для сохранения пропускной способности системы
Контроль достоверности РБД	Не применимо (используются централизованные СУБД)	Отсутствует встроенный консенсус работы с БД	Консенсус на уровне валидаторов сети (дорого и долго)	Двухуровневый экспресс-контроль

Таблица 2

Результаты моделирования динамического контроля

Порог U	Проверок человеком	Задействовано времени оператора	Совокупный пропущенный риск
10	153	199,9	13901,44
20	156	199,89	12483,91
30	142	177,32	11862,3
40	42	53,09	15268,43
50	9	11,46	16741,13
60	2	3,16	17125,32
70	0	0	17249,84

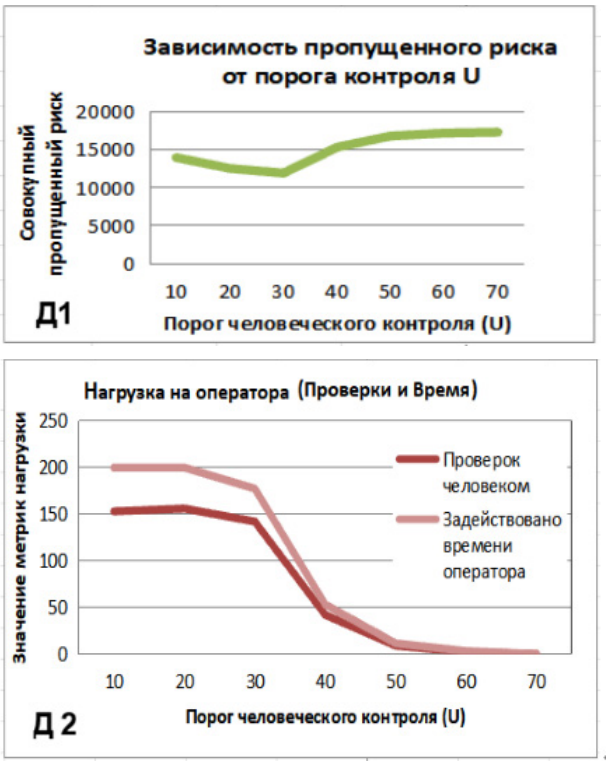


Рис. 2. Кривая риска – диаграмма Д1; нагрузка оператора – диаграмма Д2

2. Точка экстремума (Порог 30): Обнаружен оптимальный порог контроля $U = 30$, при котором достигается минимум совокупного пропущенного риска (12401.89). Время оператора расходуется максимально эффективно – только на действительно опасные аномалии.

3. Деградация контроля (Пороги 50–70): При завышенном пороге оператор почти не привлекается к процессу, автономия агентов ИИ максимальна, но совокупный риск возрастает почти в два раза.

На рис. 2 представлены две диаграммы: Д1 – зависимость совокупного пропущенного риска от порога U, на которой наглядно демонстрируется U-образный вид функции и экстремум (точка оптимума), когда время оператора расходуется максимально эффективно; Д2 – нагрузка на оператора (количество транзакций и затраченное время в зависимости от порога U, показывающая точку насыщения когнитивного ресурса человека ($T_{max} = 200$).

Таким образом, применение агентов ИИ для ведения блокчейн-баз данных в экосистеме Web 3.0 позволяет автоматизировать управление узлами, оптимизировать консенсус и повысить безопасность распределенных систем (РБД). Совмещение децентрализованного хранения данных и автономного интеллекта решает ключевые проблемы современных блокчейнов: масштабируемость и уязвимости в смарт-контрактах.

ЗАКЛЮЧЕНИЕ

Представленная модель позволяет автоматизировать информационный процесс фильтрации данных: система сама определяет, какие транзакции блокчейна от ИИ-агентов требуют «человеческого когнитивного ресурса», а какие могут быть записаны автоматически на основе высокого уровня метрик v_i, h_i.

Фундаментальная идея Web 3.0 заключается в том, что он может реализовать бессерверный Интернет, то есть Интернет, в котором пользователи генерируют контент, принадлежащий самим пользователям.

Основная сложность концепции – проблема доверия. Агент ИИ сам по себе является «черным ящиком». Чтобы сеть оставалась децентрализованной, действия самого агента должны проверяться криптографическими методами, подтверждающими, что агент выполнил инструкции честно и без манипуляций со стороны создателя модели.

Доказана применимость разработанной математической модели фильтрации для оптимизации информационного обмена. Метод позволяет аналитически вычислить порог U для минимизации рисков Web3-среды в условиях жестких ограничений на пропускную способность человеческого фактора.

Список литературы

1. Намиот Д.Е., Куприяновский В.П. Архитектурные модели Web3 // International Journal of Open Information Technologies. 2024. Т. 12, № 2. С. 84–95. – EDN CDXZIS.
2. Бурый А.С., Костылева К.В. Экспертное обоснование вариантов построения интеллектуальных систем на основе интеграции веб-технологий // Правовая информатика. 2024. № 4. С. 4–12. – https://doi.org/10.24412/1994-1404-2024-4-4-12. – EDN HAMFEZ.
3. Wan, S., Lin, H., et al. Web3: The Next Internet Revolution // IEEE Internet of Things Journal. 2024. Т.11, № 21. С. 34811–34825.
4. Клименко А.Б. Методологические основы распределения периферийных вычислительных ресурсов в автоматизированных информационно-управляющих системах // Информационно-экономические аспекты стандартизации и технического регулирования. 2026. № 3 (90). С. 33–42.
5. Alghamedy, F.H., El-Haggar, N., et al. Unlocking a Promising Future: integrating Blockchain Technology and FL-IoT in the journey to 6G // IEEE Access. 2024. № 12. С. 115411–115447.
6. Karim, M.M., Van, D.H., Khan S., Qu Q., Kholodov Y. AI Agents Meet Blockchain: A Survey on Secure and Scalable Collaboration for Multi-Agents // Future Internet. 2025. № 17(2). С. 57. – https://doi.org/10.3390/fi17020057
7. ГОСТ Р 59276–2020 Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. – М.: Стандартинформ, 2021. – 11 с.
8. Бурый А.С., Цаплина О.С. Агентные модели принятия решений на основе генеративного искусственного интеллекта // Правовая информатика. 2025. № 1. С. 101–109. – https://doi.org/24412/1994-1404-2025-1-101-109. – EDN VGEKRZ.
9. Айсин Т.Р., Шамардина Т.В. Детекция галлюцинаций на основе внутренних состояний больших языковых моделей Электронные библиотеки. 2025. Т. 28, № 6. С. 1282–1305. – https://doi.org/10.26907/1562-5419-2025-28-6-1282-1305. – EDN UHHGKI.
10. Бурый А.С., Цаплина О.С. Генеративный искусственный интеллект цифрового университета // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 5(80). С. 85–91.
11. Новиков Д.А. Модели динамики психических и поведенческих компонент деятельности в коллективном принятии решений // Управление большими системами: сборник трудов. 2020. № 85. С. 206–237. – https://doi.org/10.25728/ubs.2020.85.9. – EDN FHKBEH.

References

1. Namiot, D.E., Kupriyanovskij, V.P. Arhitekturnye modeli Web3. International Journal of Open Information Technologies, 2024, vol. 12, n. 2, pp. 84–95. (In Russ.).
2. Buryi, A.S., Kostyleva, K.V. Expert justification of options for building intelligent systems based on the integration of web technologies. Legal Informatics, 2024, no. 4, pp. 4–12. (In Russ.).
3. Wan, S., Lin, H., et al. Web3: The Next Internet Revolution. IEEE Internet of Things Journal, 2024, vol. 11, no. 21, pp. 34811–34825.
4. Klimenko, A.B. Methodological Basics of Edge Computing Resources Allocation in Automated Information and Control Systems. Information and economic aspects of standardization and technical regulation, 2026, no. 3(90), pp. 33–42. (In Russ.).
5. Alghamedy, F.H., El-Haggar, N., et al. Unlocking a Promising Future: integrating Blockchain Technology and FL-IoT in the journey to 6G. IEEE Access, 2024, no. 12, pp. 115411–115447.
6. Karim, M.M., Van, D.H., Khan S., Qu Q., Kholodov Y. AI Agents Meet Blockchain: A Survey on Secure and Scalable Collaboration for Multi-Agents. Future Internet, 2025. 17(2), 57. https://doi.org/10.3390/fi17020057
7. GOST R 59276–2020 Sistemy` iskusstvennogo intellekta. Sposoby` obespecheniya doveriya. Obshhie polozheniya. Moscow: Standartinform Publ., 2021. 11 p. (In Russ.).
8. Buryi, A.S., Tsaplina, O.S. Agentny`e modeli prinyatiya reshenij na osnove generativnogo iskusstvennogo intellekta // Pravovaya informatika, 2025, no. 1, pp. 101–109. (In Russ.).
9. Aisin, T.R., Shamardina, T.V. Hallucination detection based on the internal states of large language models // Electronic libraries, 2025, vol. 28, no. 6, pp. 1282–1305. (In Russ.).
10. Buryi, A.S., Tsaplina, O.S. Generativny`j iskusstvenny`j intellekt cifrovogo universiteta // Informacionno-e`konomicheskie aspekty` standartizacii i texnicheskogo regulirovaniya, 2024. № 5(80). С. 85–91. (In Russ.).
11. Novikov, D.A. Dynamics models of mental and behavioral components of activity in collective decision-making. Upravlenie bol'simi sistemami, 2020, no. 85, pp. 206–237. (In Russ.).