УДК 004.89
DOI 10.17513/snt.40823

CC BY 4.0

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ГИБРИДНОЙ ВЕРИФИКАЦИИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ РЕШЕНИЙ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ

[1]Зиновьев В. И. ORCID ID 0009-0008-4384-3768,
[2]Ромашкова О. Н. ORCID ID 0000-0002-1646-8527

[1]Государственное автономное образовательное учреждение высшего образования «Московский городской педагогический университет», Москва, Российская Федерация, e-mail: legrang@yandex.ru;
[2]Федеральное государственное бюджетное образовательное учреждение высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Москва, Российская Федерация

В статье исследована актуальная проблема обеспечения контекстуальной непрерывности и информационной безопасности в децентрализованных организационных системах. В рамках разработки математических моделей и критериев оценки эффективности, качества и надежности организационных систем формализован феномен семантического разрыва, возникающего при транзите цифровых состояний между различными средами доверия. Главная цель работы заключается в совершенствовании процессов управления децентрализованными сетями посредством разработки комплексной математической модели гибридной верификации транзакций. Для достижения поставленной цели предложенная модель декомпозирует общую оценку легитимности на три независимых направления: изоляционный, семантический и синхронизационный базисы. В качестве новой информационной технологии для решения сложных задач управления в организационных системах применена синергия методов машинного обучения, спектрального анализа графов и закона Литтла. Дополнительно реализована инкапсуляция процессов логического вывода в доверенные аппаратные среды исполнения с последующей генерацией криптографических доказательств с нулевым разглашением. Эмпирическая валидация на реальных наборах данных подтверждает высокую точность и отказоустойчивость разработанного мета-предиктора. Предложенная архитектура позволяет динамически адаптироваться к изменяющимся сетевым нагрузкам и эффективно противодействовать атакам на истощение ресурсов. Полученные результаты минимизируют риски оппортунистического поведения агентов и обеспечивают надежную интеллектуальную поддержку принятия стратегических и оперативных управленческих решений в современных распределенных организационных структурах.

Ключевые слова: гибридная верификация, семантический разрыв, закон Литтла, топологическая энтропия, вектор Фидлера, распределенные реестры, нулевое разглашение

MATHEMATICAL MODELING OF HYBRID VERIFICATION FOR INTELLIGENT DECISION SUPPORT IN ORGANIZATIONAL SYSTEMS

[1]Zinovev V. I. ORCID ID 0009-0008-4384-3768,
[2] Romashkova O. N. ORCID ID 0000-0002-1646-8527

[1]State Autonomous Educational Institution of Higher Education "Moscow City Pedagogical University", Moscow, Russian Federation, e-mail: legrang@yandex.ru;
[2]Federal State Budgetary Educational Institution of Higher Education "Russian Presidential Academy of National Economy and Public Administration", Moscow, Russian Federation

The article investigates the urgent problem of ensuring contextual continuity and information security in decentralized organizational systems. Within the framework of developing mathematical models and criteria for evaluating the efficiency, quality, and reliability of organizational systems, the phenomenon of the semantic gap arising during the transit of digital states between different trust environments is formalized. The main objective of the study is to improve the management processes of decentralized networks through the development of a comprehensive mathematical model of hybrid transaction verification. To achieve this goal, the proposed model decomposes the overall legitimacy assessment into three independent directions: isolation, semantic, and synchronization bases. As a new information technology for solving complex management tasks in organizational systems, the synergy of machine learning methods, spectral graph analysis, and Little's law is applied. Additionally, the encapsulation of inference processes into trusted hardware execution environments with the subsequent generation of zero-knowledge cryptographic proofs is implemented. Empirical validation on real datasets confirms the high accuracy and fault tolerance of the developed meta-predictor. The proposed architecture allows for dynamic adaptation to changing network loads and effectively counters resource exhaustion attacks. The obtained results minimize the risks of opportunistic behavior of agents and provide reliable intelligent support for making strategic and operational managerial decisions in modern distributed organizational structures.

Keywords: hybrid verification, semantic gap, Little's law, Fiedler vector, topological entropy, distributed ledgers, zero-knowledge

Введение

Эволюция управления смещается к децентрализованным сетям [1], где отсутствие центра доверия провоцирует оппортунизм агентов [2, с. 417]. Текущие подходы к детерминированному консенсусу [3; 4] не учитывают стохастический AML-контекст при конфликте прозрачности и анонимности [5]. В свою очередь, применение методов графового машинного обучения [6] сопряжено с высокой уязвимостью к сетевым L7 DoS-атакам [7]. Данные барьеры диктуют необходимость в разработке методов и алгоритмов решения задач управления в организационных системах, интегрирующих энтропию полезной нагрузки, спектральную связность графа и сетевые задержки в единый контур. Без такого синтеза возникает «семантический разрыв» – утрата нормативного контекста при транзите актива.

Цель исследования – совершенствование процессов управления транзитом цифровых активов в децентрализованных организационных системах (объект исследования) средствами разработки математической модели гибридной интеллектуальной верификации (предмет исследования), обеспечивающей интеллектуальную поддержку принятия управленческих решений в организационных системах на основе синергии машинного обучения, спектрального анализа графов и доказательств с нулевым разглашением.

Материал и методы исследования

Методологический фундамент исследования основывается на системном подходе [8] к анализу децентрализованных структур, требующем предварительного аналитического описания условий возникновения информационных противоречий при передаче состояний активов.

Результаты исследования и их обсуждение

Цифровой актив в системе моделируется как неделимый многомерный кортеж:

$$A = \langle V, R, H \rangle,$$

где V – номинальная ценность актива; R – нормативный базис (матрица юрисдикционных политик и комплаенс-ограничений); H – направленный ациклический граф истории состояний (родословная актива).

При транзите актива из корпоративной среды (ERP) в децентрализованную среду оператор проецирования Π расщепляет базис R на вычисляемые (on-chain) и скрытые (off-chain) правила

$$R_{tgt} = R_{on} \cup R_{off}. \quad (1)$$

Семантический разрыв формализуется как разность множеств исходного базиса и того, что способен верифицировать детерминированный смарт-контракт

$$\Delta_{sem} = R_{src} \setminus \Pi^{-1}(R_{on}). \quad (2)$$

Для демонстрации процесса расщепления нормативного базиса и формирования компенсаторного механизма разработана диаграмма переходов состояний (рис. 1).

Для устранения Δ_{sem} вводится глобальная функция предиктивной верификации $\hat{Y}$, представляющая собой синергетическое объединение трех независимых метрических функций

$$\hat{Y} = w_1 \cdot F_{iso}(x) + w_2 \cdot F_{sem}(H) + w_3 \cdot F_{sync}(t). \quad (3)$$

Условие нормировки адаптивных весовых коэффициентов

$$w_1 + w_2 + w_3 = 1. \quad (4)$$

Синтез предлагаемой модели предполагает последовательную декомпозицию процесса верификации на функциональные уровни, отвечающие за изоляцию аномалий, семантический анализ транзакционных связей и временную синхронизацию потоков.

Изоляционный базис (F_{iso}). Функция выявляет инъекции и аномальные паттерны в полезной нагрузке текущего запроса x. Сначала вычисляется информационная энтропия Шеннона

$$H_{payload} = -\sum_{i=1}^{n} p_i \cdot \log_2(p_i). \quad (5)$$

Для интеллектуальной классификации применяется алгоритм Изолирующего леса (Isolation Forest). Оценка аномальности $s(x,n)$ вычисляется на основе длины пути $E(h(x))$ в дереве изоляции и средней длины неудачного поиска $c(n)$

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}. \quad (6)$$

Базис F_{iso} агрегирует эти метрики с помощью градиентного бустинга (XGBoost) [9], возвращая нормированную вероятность чистоты payload-составляющей.

Семантический графовый базис (F_{sem}) [10]. Для выявления циклических схем обфускации (например, пулов легализации) анализируется подграф истории H. Вычисляется нормированная матрица Лапласа

$$L_{graph} = I - D^{-1/2} A_{matrix} D^{-1/2}, \quad (7)$$

где D – диагональная матрица степеней, A_{matrix} – матрица смежности.

Рис. 1. Автомат состояний транзита актива
Примечание: составлен авторами по результатам данного исследования

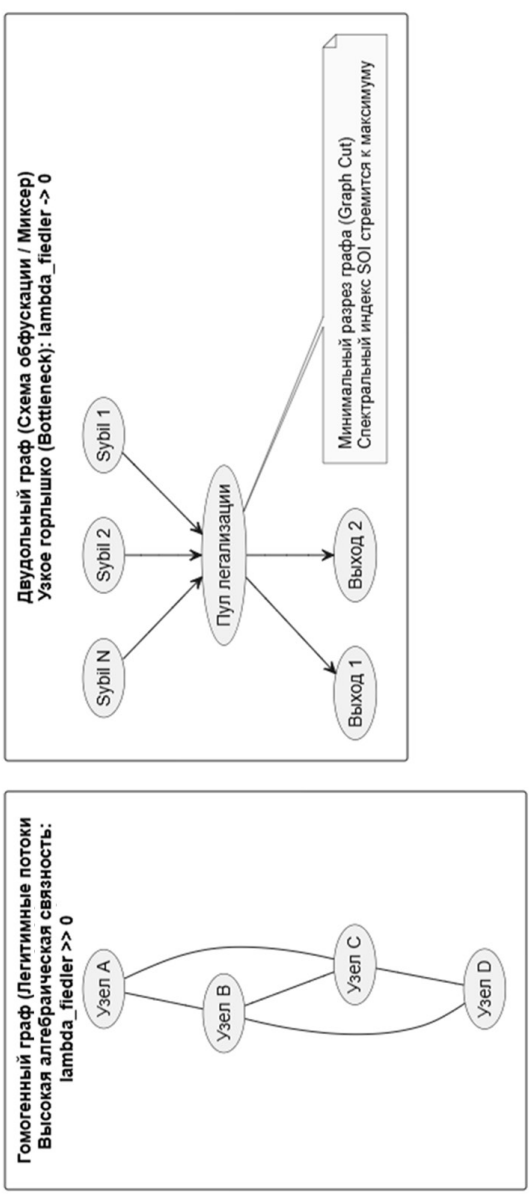

Рис. 2. Топологическая абстракция выявления схем обфускации
Примечание: составлен авторами по результатам данного исследования

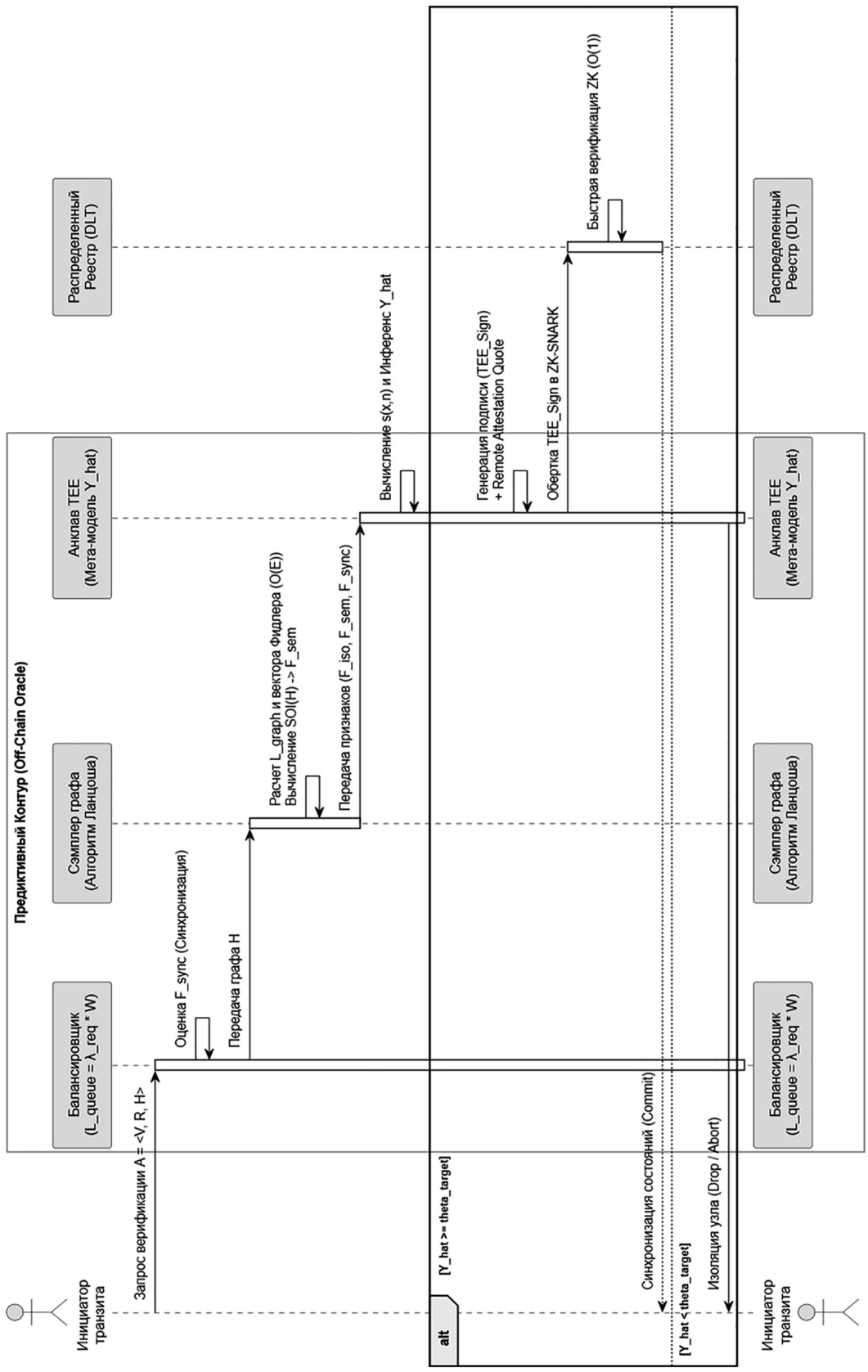

Рис. 3. Архитектура гибридной верификации
Примечание: составлен авторами по результатам данного исследования

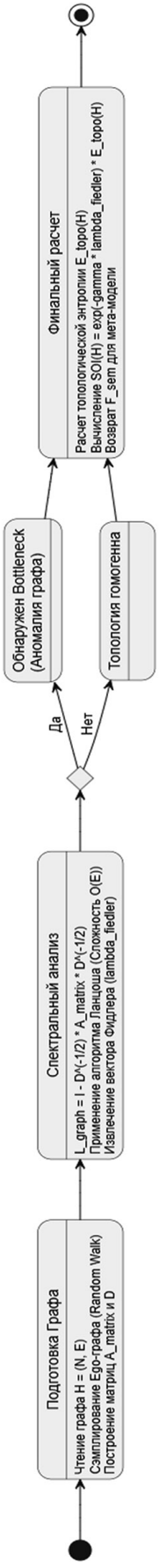

Рис. 4. Алгоритм спектральной верификации
Примечание: составлен авторами по результатам данного исследования

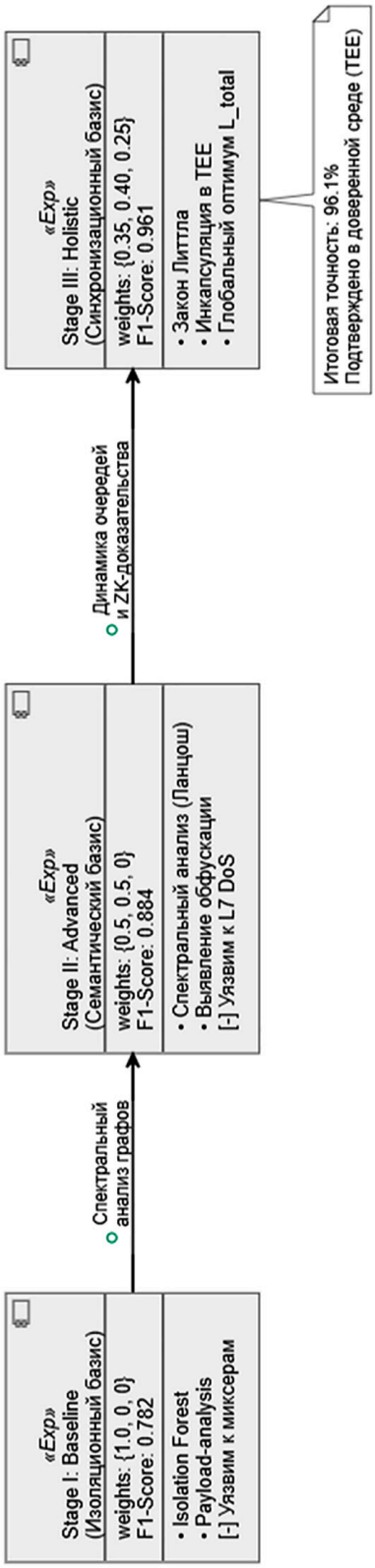

Рис. 5. Абляционный анализ компонентов метапредикта
Примечание: составлен авторами по результатам данного исследования

Для преодоления кубической вычислительной сложности прямого спектрального разложения применяется метод случайных блужданий с возвратом (RWR) для сэмплинга графа. Второе собственное значение (вектор Фидлера $\lambda_{fiedler}$) вычисляется алгоритмом Ланцоша за асимптотическое время $O(E)$, где E – число ребер. Наличие узкого горлышка (признак преднамеренной обфускации) выражается как $\lambda_{fiedler} \to 0$. Концептуальная абстракция представлена на рис. 2.

Топологическая энтропия графа $E_{topo}(H)$ вычисляется по распределению степеней узлов $P(k)$

$$E_{topo}(H) = -\sum_{k} P(k) \log_2 P(k). \quad (8)$$

Спектральный индекс обфускации (SOI), служащий главным предиктором для F_{sem}, равен

$$SOI(H) = \exp\left(-\gamma \cdot \lambda_{fiedler}\right) \cdot E_{topo}(H). \quad (9)$$

Синхронизационный сетевой базис (F_{sync}). Для защиты от асинхронных атак на истощение ресурсов (L7 DoS), генерируемых ботнетами, оценивается состояние распределенной очереди. Согласно закону Литтла из теории массового обслуживания [11]

$$L_{queue} = \lambda_{red} \cdot W,$$

где L_{queue} – математическое ожидание длины очереди, λ_{red} – интенсивность входящих M2M-запросов, W – среднее время задержки обработки. Если L_{queue} экспоненциально растет при легитимном F_{sem},, система диагностирует Sybil-атаку, и F_{sync} стремится к нулю.

Детерминизация итогового решения для смарт-контракта осуществляется по динамическому порогу θ_{target}:

если $\hat{Y} \geq \theta_{target} \Rightarrow \sigma_{oracle} = 1$,

если $\hat{Y} < \theta_{target} \Rightarrow \sigma_{oracle} = 0$.

Практическая апробация разработанных теоретических положений позволила синтезировать целевую архитектуру системы, обеспечивающую интеллектуальную поддержку процессов верификации и криптографическую защиту транзита состояний [12].

Интеграция тяжелых ML-вычислений в распределенный реестр требует применения доказательств с нулевым разглашением (ZK-SNARK) [13; 14]. Однако генерация SNARK для случайного леса или расчета графов аппаратно неэффективна (ZKML-барьер). В качестве синергетического решения предложено инкапсулировать вычисление $\hat{Y}$ в Доверенные среды исполнения (TEE, например, Intel SGX) [15]. Анклав генерирует легковесную подпись и криптографическую квоту удаленной аттестации (Remote Attestation Quote), которые обертываются в ZK-SNARK за константное время $O(1)$ (рис. 3).

Спектральный анализ подграфа детализирован на алгоритмической схеме (рис. 4).

Экспериментальные исследования и абляционный анализ. Обучение ансамбля моделей (XGBoost + Graph Neural Networks) осуществлялось через минимизацию взвешенной асимметричной функции потерь L_{async}

$$L_{async} = -\left[\alpha \cdot y \log\left(\hat{Y}\right) + \beta \cdot (1-y) \log\left(1-\hat{Y}\right)\right]. \quad (10)$$

Для обеспечения глобальной сходимости в условиях мультимодальных данных введена совокупная функция потерь L_{total}

$$L_{total} = \alpha L_{async} + \beta L_{sem} + \gamma L_{sync}. \quad (11)$$

Валидация проведена на графе Elliptic Data Set (N = 203769, E = 234355) методом темпорально-стратифицированного сэмплинга. Для оценки $\hat{Y}$ инжектированы возмущения трех типов: искажения нагрузки (F_{iso}), подграфы обфускации (F_{sem}) и сетевые задержки (F_{sync}). Дисбаланс классов (88/12 %) соответствует энтропии реальных M2M-систем. Синергия компонентов $\hat{Y}$ обоснована абляционным анализом (Ablation Study) с поочередным отключением базисов (рис. 5).

Изолированное ML-профилирование (F_{iso}) не выявляет топологические аномалии. Внедрение F_{sem} повысило F1-Score до 0,884, но не обеспечило сепарацию легитимных пиков нагрузки и атак. Интеграция закона Литтла (F_{sync}) позволила ансамблю адаптироваться к физике сети, достигнув F1 = 0,961 при инференсе 18 мс.

Для обеспечения гибкости организационной системы в условиях волатильности сетевого трафика и изменения паттернов поведения агентов, в разработанной модели реализован механизм динамической адаптации порога принятия решений θ_{target}.

В предложенной гибридной модели порог детерминизации θ_{target} не является статической константой, а вычисляется как функция от скользящего окна исторической топологической энтропии $\overline{E_{topo}}$ и текущей нагрузки на мемпул (mempool) распределенного реестра. При экспоненциальном росте очереди входящих запросов (L_{queue}), модель автоматически повышает требования к спектральной чистоте анализируемого подграфа ($SOI(H)$). Это позволяет системе формировать превентивный защитный барьер, снижая вероятность успешного проведения атак Сивиллы (Sybil attack)

или использования сложных схем обфускации через пулы легализации.

С точки зрения управления организационными системами данный подход означает качественный переход от реактивной модели комплаенс-контроля к проактивной. Система получает возможность автоматически балансировать между пропускной способностью транзакций (TPS) и требуемым уровнем безопасности. В периоды стабильного функционирования сети требования к верификации оптимизируются, что обеспечивает высокую скорость обработки данных. При выявлении паттернов скоординированного оппортунистического поведения агентов система переходит в режим повышенной изоляции, блокируя сомнительные транзиты цифровых активов еще на этапе off-chain предикта.

Внедрение предложенной модели гибридной верификации в контур управления децентрализованными организационными системами позволяет существенно нивелировать транзакционные издержки, связанные с ручным аудитом и комплаенс-контролем. Интеллектуальная поддержка принятия решений, основанная на агрегации метрик из трех независимых базисов, минимизирует влияние человеческого фактора и предотвращает эскалацию конфликтов интересов между независимыми агентами сети. Практическая значимость разработанного подхода подтверждается не только высокой точностью обнаружения аномалий, но и способностью системы к динамической самоадаптации при изменении топологии сети. Это формирует замкнутый цикл управления рисками, что является критически важным условием для обеспечения надежности, прозрачности и отказоустойчивости современных распределенных организационных структур в условиях неопределенности.

Заключение

В ходе исследования решена научная задача по разработке теоретических основ управления в организационных системах применительно к децентрализованным сетям. Выполненная разработка математической модели и критериев эффективности гибридной верификации на базе алгоритма Ланцоша и ZK-SNARK представляет собой новую информационную технологию для решения задач управления, исключающую семантический разрыв без потери производительности. Результаты исследования служат фундаментом для разработки методов и алгоритмов интеллектуальной поддержки принятия управленческих решений в организационных системах, позволяя минимизировать риски в реальном времени.

Список литературы

1. Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, Fei-Yue Wang Decentralized Autonomous Organizations: Concept, Model, and Applications // IEEE Transactions on Computational Social Systems. 2019. Vol. 6. Is. 5. P. 870–878. DOI: 10.1109/TCSS.2019.2938190.

2. Новиков Д. А. Теория управления организационными системами. 4-е изд., испр. и дополн. М.: Ленанд, 2022. 500 с. ISBN 978-5-9710-9459-3.

3. Schär F. Decentralized Finance: On Blockchain – and Smart Contract-Based Financial Markets // Federal Reserve Bank of St. Louis Review. 2021. Vol. 103. Is. 2. P. 153–174. DOI: 10.20955/r.103.153-74.

4. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform // Ethereum White Paper. 2014. 36 p. [Электронный ресурс]. URL: https://ethereum.org/en/whitepaper/ (дата обращения: 09.04.2026).

5. Nassif A. B., Talib M. A., Nasir Q., Dakalbab F. M. Machine Learning for Anomaly Detection: A Systematic Review // IEEE Access. 2021. Vol. 9. P. 78658–78700. DOI: 10.1109/ACCESS.2021.3083060.

6. Zhang Z., Cui P., Zhu W. Deep Learning on Graphs: A Survey // IEEE Transactions on Knowledge and Data Engineering. 2022. Vol. 34. Is. 1. P. 249–270. DOI: 10.1109/TKDE.2020.2981333.

7. Saad M., Spaulding J., Njilla L., Kamhoua C., Shetty S., Nyang D., Mohaisen A. Exploring the Attack Surface of Blockchain: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. 2020. Vol. 22. Is. 3. P. 1977–2008. DOI: 10.1109/COMST.2020.2975999.

8. Каптерев А. И., Ромашкова О. Н., Чискидов С. В., Ермакова Т. Н. Современное состояние и перспективы моделирования цифровых профессиональных пространств в бизнесе и образовании // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2023. Т. 20. № 4. С. 358–372. URL: https://www.elibrary.ru/item.asp?id=63430246 (дата обращения: 09.04.2026). EDN: BSBPRL.

9. Liu F. T., Ting K. M., Zhou Z. Isolation Forest // 2008 Eighth IEEE International Conference on Data Mining. 2008. P. 413–422. DOI: 10.1109/ICDM.2008.17.

10. Wu Z., Pan S., Chen F. A., et al. Comprehensive Survey on Graph Neural Networks // IEEE Transactions on Neural Networks and Learning Systems. 2021. Vol. 32. Is. 1. P. 4–24. DOI: 10.1109/TNNLS.2020.2978386.

11. Little J. D. C. OR FORUM – Little's Law as Viewed on Its 50th Anniversary // Operations Research. 2011. Vol. 59. Is. 3. P. 536–549. DOI: 10.1287/opre.1110.0940.

12. Zhang R., Xue R., Liu L. Security and Privacy on Blockchain // ACM Computing Surveys. 2019. Vol. 52. Is. 3. P. 1–34. DOI: 10.1145/3316481.

13. Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge // Advances in Cryptology – CRYPTO 2013. 2013. P. 90–108. DOI: 10.1007/978-3-642-40084-1_6.

14. Xiaoqiang Sun, F. Richard Yu, Peng Zhang et al. A Survey on Zero-Knowledge Proof in Blockchain // IEEE Network. 2021. Vol. 35. Is. 4. P. 198–205. DOI: 10.1109/MNET.011.2000473.

15. Cheng R. et al. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts // 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. P. 185–200. DOI: 10.1109/EuroSP.2019.00023.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.

Финансирование: Авторы заявляют об отсутствии внешнего финансирования.

Financing: The research was performed without external funding.