УДК 004.9

МНОГОУРОВНЕВЫЕ СИСТЕМЫ КАЧЕСТВЕННЫХ ДАННЫХ НА ОСНОВЕ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ И РЕШЕНИЯ

Лопатин И.Н., аспирант, Российский институт стандартизации

В современную цифровую эпоху качество данных является критическим фактором для эффективности систем кибербезопасности, антифрод-механизмов и моделей искусственного интеллекта (ИИ). Внедрение кроссплатформенных систем качества данных с многоуровневым мониторингом, включая статистический анализ, базовый контроль качества данных, расширенное обнаружение аномалий, проверки полноты и генерацию синтетических данных, обеспечивает всесторонний контроль данных. Низкое качество данных может привести к серьезным последствиям, включая пропущенные угрозы, финансовые потери, репутационные риски и этические проблемы. Комплексный подход к управлению качеством данных, включающий разработку стратегии, технологические решения, стандартизацию, мониторинг и обучение персонала, основанный на современных стандартах и лучших практиках, значительно повышает надежность и эффективность систем. Инвестирование в качество данных становится стратегически важным для организаций на фоне растущих объемов данных и усложняющихся угроз.

Ключевые слова: качество данных, кибербезопасность, антифрод-системы, большие языковые модели, атакующие нейросети, искусственный интеллект, многоуровневый мониторинг, кроссплатформенные системы.

ВВЕДЕНИЕ

В современном цифровом мире данные стали одним из ключевых стратегических ресурсов организаций. Они служат основой для принятия обоснованных решений, прогнозирования тенденций, разработки инновационных продуктов и обеспечения безопасности информационных систем. Однако эффективность использования данных напрямую зависит от их качества [1, 2]. Низкое качество данных может привести к ошибочным выводам, снижению эффективности систем, финансовым потерям и репутационным рискам [3].

Особое значение качество данных приобретает в областях кибербезопасности, антифрод-систем[1] и обучения моделей искусственного интеллекта (ИИ). В этих сферах данные используются для обнаружения и предотвращения угроз, анализа поведения пользователей и принятия автоматизированных решений. Ошибки и неточности в данных могут привести к пропуску реальных угроз, увеличению количества ложных срабатываний, снижению доверия к аналитическим моделям и принятию неверных решений.

Проблемы качества данных в кибербезопасности, антифрод-системах и при обучении моделей ИИ (далее – AI-модели, от англ. Artificial Intelligence) особенно актуальны по нескольким причинам:

1. **Разнообразие и сложность источников данных.** Данные поступают из множества разнородных источников с различными форматами, структурами и протоколами передачи. Среди них сетевые журналы, данные приложений, логи[2], средства защиты, социальные сети и др. Интеграция таких данных сложна и повышает риск появления ошибок и несоответствий.
2. **Объем и скорость данных (Big Data).** Большие объемы данных, поступающие с высокой скоростью, затрудняют своевременную проверку и валидацию информации в режиме real time. По данным IBM [4] (Нгуен), ежедневно создается 2,5 квинтиллиона байт данных.
3. **Отсутствие стандартизации.** Различия в форматах данных, протоколах и методах сбора затрудняют их обработку и анализ. Стандарты, такие как STIX/TAXII, не всегда широко внедрены.
4. **Низкое качество обучающих данных для AI-моделей.** Использование данных с низким качеством для обучения моделей искусственного интеллекта приводит

[1] Антифрод-системы (от англ. anti-fraud – борьба с мошенничеством) – программные комплексы для предотвращения мошеннических транзакций.

[2] Лог – это специальный текстовый файл. В него в автоматическом режиме осуществляется запись важной информации о работе программы, сервера или системы.

к снижению точности языковых моделей LLM (L – Large) и SLM (Small language model), применяемых, например, в кибербезопасности как инструменты по автоматизированному взлому инфраструктур.

5. **Этические и нормативные требования**. Рост регуляций в области защиты данных (GDPR[3], CCPA) требует обеспечения высокого качества данных для соблюдения прав пользователей и обеспечения прозрачности процессов.

НЕОБХОДИМОСТЬ КРОССПЛАТФОРМЕННЫХ СИСТЕМ КАЧЕСТВА ДАННЫХ

Для обеспечения высоких требований по качеству данных необходимо внедрение кроссплатформенных систем качества данных, которые содержат несколько уровней мониторинга качества данных (см. рис. 1).

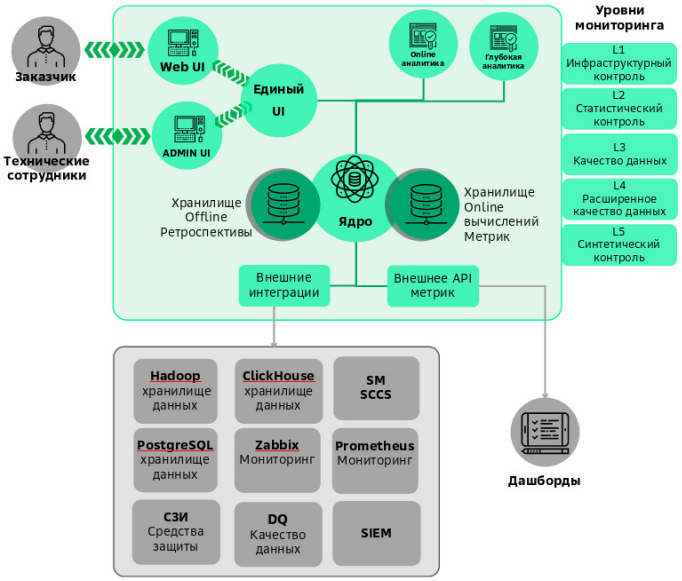

Рис. 1. Архитектура кроссплатформенной системы качества данных

На рис. 1 представлена общая архитектура предлагаемой системы. Она включает пять уровней мониторинга, каждый из которых выполняет специфические функции по обеспечению качества данных:

1. ***Уровень статистического анализа данных.*** Осуществляет анализ статистических характеристик данных, таких как распределение, средние значения, дисперсия.

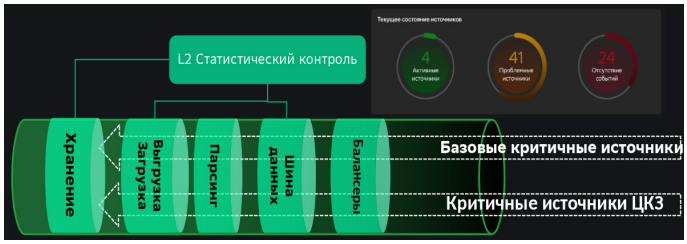

Рис. 2. Блок-схема уровня статистического анализа данных

2. ***Уровень базового качества данных.*** Контролирует наличие и корректность обязательных полей, обеспечивает соответствие данных установленным форматам и типам.

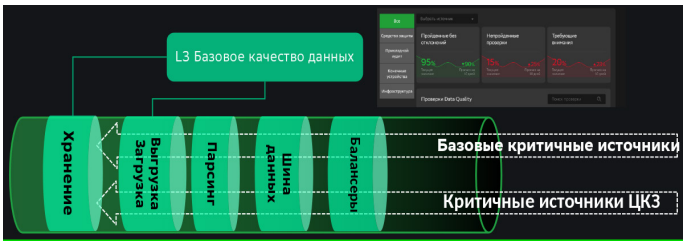

Рис. 3. Блок-схема уровня базового качества данных

3. ***Уровень расширенного качества данных.*** Включает обнаружение аномалий и сопоставление данных между разными источниками для выявления несоответствий и ошибок.

Рис. 4. Блок-схема уровня расширенного качества данных

4. ***Уровень контроля полноты.*** Проверяет, что все необходимые данные были получены и что нет пропущенных записей или недостающих наборов данных.

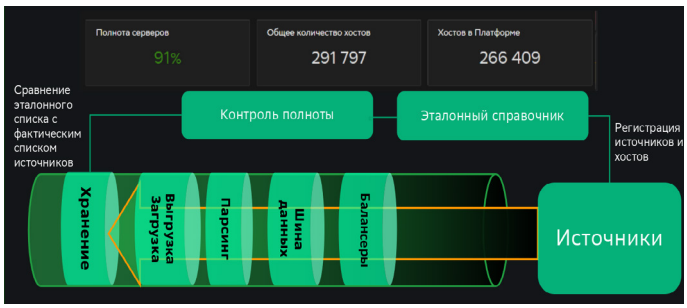

Рис. 5. Блок-схема уровня контроля полноты

3 Регламент (ЕС) 2016/679 Европейского парламента… о защите физических лиц в отношении обработки персональных данных. URL: http://data.europa.eu/eli/reg/2016/679/oj (дата обращения: 23.12.2024).

5. ***Уровень синтетического контроля.*** Использует генерацию синтетических данных для проверки корректности работы систем при различных сценариях и оценки качества на уровне бизнес-логики.

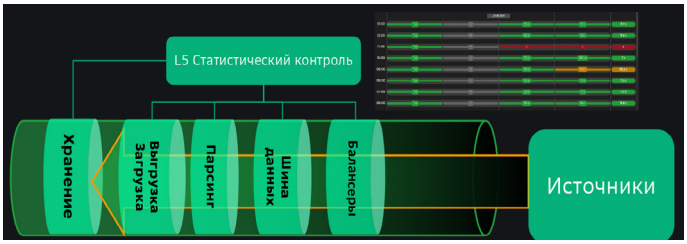

Рис. 6. Блок-схема уровня синтетического контроля

Последствия низкого качества данных:

- пропуск реальных угроз. По данным Cisco[4], около 44% компаний сталкиваются с пропуском киберугроз из-за недостаточного качества данных;
- снижение эффективности антифрод-систем; финансовые институты теряют миллиарды долларов ежегодно из-за мошенничества, которое не было обнаружено из-за низкого качества данных [6];
- низкий уровень доверия к AI-моделям: согласно исследованию [7] компании испытывают трудности с доверием к AI-моделям из-за проблем с качеством данных и непрозрачности алгоритмов;
- этические риски и предвзятость: AI-модели могут усиливать социальные стереотипы и предвзятости, если обучены на некорректных данных [8].

ПРАКТИЧЕСКИЕ КЕЙСЫ

Кейс 1: Финансовый сектор и антифрод-системы

По данным Центробанка, в 2023 году у клиентов банков было похищено 15,8 млрд рублей, что на 30% выше, чем результаты за 2022 год. Банками за первые три месяца 2023 года было отражено 2,7 млн атак кибермошенников на счета клиентов, что позволило не допустить хищения более 700 млрд рублей. При этом Банк России в первом квартале 2023 года инициировал блокировку почти 97 тыс. мошеннических номеров телефонов, а также направил информацию об около 7 тыс. интернет-ресурсов в Генеральную прокуратуру[5]. Отсутствие своевременного обнаружения аномальных транзакций и недостаточная валидация данных привели к значительным финансовым потерям и репутационным рискам. После инцидента банк внедрил многоуровневую систему качества данных, что позволило значительно улучшить безопасность транзакций и снизить риск мошенничества.

Кейс 2: Кибербезопасность – обнаружение массовой эксфильтрации данных через HTTP/HTTPS

Причиной утечки стала уязвимость в веб-приложении, а недостаточное качество данных в логах не позволило своевременно обнаружить эксфильтрацию[6]. Логи не содержали необходимых полей для выявления аномальной активности, таких как объем переданных данных и детализированные записи доступа. После инцидента компания инвестировала в улучшение систем мониторинга и качества данных, включая внедрение многоуровневого контроля[7].

[4] Отчеты Cisco по кибербезопасности. URL: https://www.cisco.com/c/en_uk/products/security/security-reports.html#~latest-reports (дата обращения: 22.12.2024).

[5] Потери банков от киберпреступности. [Сайт: www.tadviser.ru] (дата обращения: 24.12.2024).

[6] Эксфильтрация данных – это несанкционированная передача данных с компьютера с помощью вредоносного программного обеспечения или злоумышленником.

[7] The Guardian. (2018). Equifax data breach caused by 'entirely preventable' mistakes, says House report. URL: https://www.theguardian.com/technology/2018/dec/10/equifax-data-breach-entirely-preventable-house-report (дата обращения: 25.12.2024).

Таблица 1

Примеры правил корреляции в кибербезопасности и соответствующие правила обеспечения качества данных

№	НАЗВАНИЕ ПРАВИЛА КОРРЕЛЯЦИИ	ИСПОЛЬЗУЕМЫЕ ОБЯЗАТЕЛЬНЫЕ ПОЛЯ ИСТОЧНИКА	ПРАВИЛО КАЧЕСТВА ДАННЫХ
1	**Обнаружение использования скомпрометированных учетных записей**	UserID, SourceIP, DestinationIP, LoginTime, AuthenticationMethod, EventID	Проверка корректности UserID, соответствия IP-адресов геолокации пользователя, валидация метода аутентификации
2	**Выявление атак на облачные сервисы с использованием привилегированных API-ключей**	APIKeyID, ServiceAction, SourceIP, UserAgent, Timestamp	Выявление атак на облачные сервисы с использованием привилегированных API-ключей
3	**Детектирование бесфайловых атак через командную строку**	UserID, ProcessID, CommandLine, ParentProcessID, ExecutionTime	Анализ командной строки на подозрительные команды, проверка цепочки процессов, точность временных меток
4	**Обнаружение атак на контейнерные среды (Docker, Kubernetes)**	ContainerID, ImageName, CommandExecuted, SourceIP, Timestamp	Верификация легитимности образов, анализ выполняемых команд, проверка IP-адресов

Таблица 2

Примеры правил антифрод-систем и соответствующие правила качества данных

№	НАЗВАНИЕ ПРАВИЛА АНТИФРОД-СИСТЕМЫ	ИСПОЛЬЗУЕМЫЕ ОБЯЗАТЕЛЬНЫЕ ПОЛЯ ИСТОЧНИКА	ПРАВИЛО КАЧЕСТВА ДАННЫХ
1	**Выявление мошенничества через социальные мессенджеры**	CustomerID, CommunicationPlatform, MessageContent, Timestamp	Анализ содержания сообщений, проверка платформы, точность временных меток
2	**Контроль операций с поддельными мобильными приложениями**	CustomerID, AppID, DeviceID, TransactionAmount, GeoLocation, Timestamp	Верификация подлинности AppID, соответствие DeviceID, проверка геолокации
3	**Обнаружение мошенничества с использованием QR-кодов**	CustomerID, QRCodeData, TransactionAmount, MerchantID, Timestamp	Проверка QR-кода на вредоносность, верификация MerchantID
4	**Анализ операций в криптоактивах через DeFi-платформы**	CustomerID, WalletAddress, TransactionAmount, DeFiPlatformID, CryptocurrencyType, Timestamp	Проверка легитимности DeFi-платформы, анализ аномалий транзакций

Таблица 3

Примеры проблем с AI-моделями, обученными на данных низкого качества

№	ОБЛАСТЬ ПРИМЕНЕНИЯ	ПРОБЛЕМА ИЗ-ЗА НИЗКОГО КАЧЕСТВА ДАННЫХ	ПОСЛЕДСТВИЯ
1	**Обработка естественного языка (LLM)**	Обучение на предвзятых или неточных данных	Распространение дезинформации, усиление стереотипов
2	**Генеративные модели для визуального контента**	Низкое разнообразие обучающих изображений, наличие артефактов	Плохое качество контента, нарушение авторских прав
3	**AI в кибербезопасности для предсказания уязвимостей**	Неполные базы уязвимостей, отсутствие актуальных данных	Неспособность предотвратить новые атаки, повышенный риск выбора ложных планов атак в SLM моделях
4	**Распознавание эмоций в системах обслуживания клиентов**	Ограниченное культурное и этническое разнообразие данных	Неверная интерпретация эмоций, снижение качества обслуживания

ПРИМЕРЫ ВЛИЯНИЯ НИЗКОГО КАЧЕСТВА ДАННЫХ НАПРАВЛЕНИЯ И СПОСОБЫ РЕШЕНИЯ

Для повышения качества данных и эффективности систем кибербезопасности, антифрод-систем и AI-моделей необходимо внедрить комплексный подход:

1. Стратегия управления качеством данных (Data Governance):

- Назначение ответственных. Внедрить роли Chief Data Officer (CDO), Data Steward и Data Custodian [9].
- Политики и стандарты. Разработать и внедрить политики по управлению данными, основываясь на стандартах ISO 8000[8], ISO/IEC 27001[9]

2. Внедрение кроссплатформенных систем качества данных:

- Уровень статистического анализа данных. Использовать методы статистического контроля для выявления аномалий и отклонений в данных.
- Уровень базового качества данных. Контролировать наличие и корректность обязательных полей. Автоматические проверки гарантируют, что все необходимые поля заполнены и соответствуют требуемым форматам.
- Уровень расширенного качества данных. Осуществлять анализ аномалий и сопоставление данных между различными источниками.
- Уровень контроля полноты. Обеспечивать полноту данных, проверяя, что все необходимые записи и наборы данных присутствуют и доступны для обработки.
- Уровень синтетического контроля. Генерировать синтетические данные для тестирования и верификации бизнес-сценариев и выявления влияния данных на них.

3. Технологические решения:

[8] ISO 8000–61:2016 Качество данных. Часть 61: Управление качеством данных: эталонная модель процесса.

[9] SO/IEC 27001:2022 Системы управления информационной безопасностью – практическое руководство для малых и средних предприятий.

- DataOps и MLOps. Применять подходы DataOps и MLOps для управления данными и моделями [10].
- Инструменты валидации и очистки. Использовать ETL-процессы с встроенной валидацией [1].
- Машинное обучение для контроля качества данных. Применять алгоритмы ML для обнаружения аномалий [11].

4. Стандартизация и интеграция:

- Использование стандартов. Внедрять стандарты обмена данными (STIX/TAXII, ISO 20022[10]).
- Интеграция данных. Использовать DataLake и DataVault подходы [12].

5. Мониторинг и аудит:

- Метрики качества данных. Определить и отслеживать ключевые показатели.
- Аудиты и контроль. Проводить регулярные аудиты по стандартам [1, 2].

6. Обучение и культура данных:

- Повышение квалификации. Организовать обучение сотрудников.
- Этические комитеты. Создать группы по этике данных и ИИ [8].

7. Улучшение AI-моделей:

- Справедливость и прозрачность. Использовать методы Explainable AI [12].
- Качество данных. Применять методы очистки и нормализации.

8. Соответствие нормативным требованиям:

- GDPR, CCPA. Обеспечить соответствие регулятивным требованиям.
- Отраслевые стандарты. Внедрять специфичные стандарты (PCI DSS)[11].

9. Передовые технологии:

- Блокчейн. Использовать для обеспечения целостности данных [13].
- ИИ для качества данных. Автоматизировать управление качеством данных [2, 11].

ЗАКЛЮЧЕНИЕ

Качество данных является критическим фактором для эффективности систем кибербезопасности, антифрод-систем и ИИ. Внедрение кроссплатформенных систем качества данных с многоуровневым мониторингом и использованием визуализации процессов позволяет обеспечить всесторонний контроль и повышение надежности данных. Комплексный подход, основанный на стандартах, технологиях и лучших практиках, повышает надежность и эффективность систем. Инвестиции в качество данных становятся стратегически важными для организаций на фоне растущих объемов данных и усложняющихся угроз.

[10] ГОСТ Р ИСО 20022-1–2013 Финансовые услуги. Универсальная схема сообщений финансовой индустрии. Часть 1. Метамодель.

[11] PCI DSS (с англ. Payment Card Industry Data Security Standard – стандарт безопасности индустрии платежных карт).

Список использованных источников и литературы/ References

1. Бурый А.С., Погодин И.М. Оценка качества больших данных. Часть 1. Основные понятия и метрики // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 3(78). С. 49–58. / Buryi A.S., Pogodin I.M. Assessment the Quality of Big Data. Part 1. Basic concepts and metrics. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 3 (78): 49–58. (In Russ.).
2. Бурый А.С., Погодин И.М. Оценка качества больших данных. Часть 2. Модели данных // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 4(79). С. 24–32. / Buryi A.S., Pogodin I.M. Assessment the Quality of Big Data. Part 2. Data Models. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 4 (79): 24–32. (In Russ.).
3. Бирюков А.Н. Качество данных как услуга // Прикладная информатика. 2020. Т. 15, № 4(88). С. 120–132. /Biryukov A.N. Data quality as a service. Applied Informatics. 2020; 15(4): 120–132. (In Russ.).
4. Nguyen T.L. A framework for five big v's of big data and organizational culture in firms. In 2018 IEEE international conference on big data (big data). 2018, pp. 5411–5413.
5. Бурый А.С., Цаплина О.С. Генеративный искусственный интеллект цифрового университета // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 5(80). С. 85–91. / Buryi A.S., Tsaplina O.S. Generative Artificial Intelligence of a Digital University. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 5(80): 85–91. (In Russ.).
6. Redman T.C. Data driven: profiting from your most important business asset. Brighton, MA: Harvard Business Press; 2008, 273 p.
7. Ransbotham S., Kiron D., Gerbert P., Reeves M. Reshaping Business With Artificial Intelligence // MIT Sloan Management Review. 2017; 59(1).
8. Zou J., Schiebinger L. AI can be sexist and racist – it's time to make it fair // Nature, 2018; 559(7714): 324–326.
9. English L.P. Information quality applied: best practices for improving business information, processes and systems. John Wiley & Sons, 2009.

10. Breck E., et al. The ML test score: A rubric for ML production readiness and technical debt reduction // IEEE International Conference on Big Data. 2017. P. 1123–1132.
11. Sculley D., et al. Hidden Technical Debt in Machine Learning Systems //Advances in Neural Information Processing Systems. 2015. T. 28. C. 1–9.
12. Doshi-Velez F., Kim B. Towards a rigorous science of interpretable machine learning //arXiv preprint arXiv:1702.08608. 2017.
13. Kshetri N. Can blockchain strengthen the Internet of Things? // IT Professional. 2017. Vol. 19, no. 4, pp. 68–72.

MULTILEVEL SYSTEMS OF QUALITATIVE DATA BASED ON ARTIFICIAL INTELLIGENCE MODELS: PROBLEMS AND SOLUTIONS

Lopatin I.N., PhD student, Russian Standardization Institute

In the modern digital age, data quality is a critical factor for the effectiveness of cybersecurity systems, anti-fraud mechanisms, and artificial intelligence (AI) models. The implementation of cross-platform data quality systems with multi-level monitoring, including statistical analysis, basic data quality control, advanced anomaly detection, completeness checks, and synthetic data generation, ensures comprehensive data control. Poor data quality can lead to serious consequences, including missed threats, financial losses, reputational risks, and ethical concerns. An integrated approach to data quality management, including strategy development, technological solutions, standardization, monitoring and staff training, based on modern standards and best practices, significantly improves the reliability and efficiency of systems. Investing in data quality is becoming strategically important for organizations amid growing amounts of data and increasingly complex threats.

Keywords: data quality, cybersecurity, anti-fraud systems, large language models, attacking neural networks, artificial intelligence, multilevel monitoring, cross-platform systems.