

УДК 004.89

РОЛЬ ОТКРЫТОГО КОДА В ФОРМИРОВАНИИ ДОВЕРИЯ К БИБЛИОТЕКАМ МАШИННОГО ОБУЧЕНИЯ

Литвинова Ю.Е., студент гр. 09-211, II курс
Казанский (Приволжский) федеральный университет, г. Казань

В современном цифровом обществе, где алгоритмы машинного обучения принимают всё более значимые решения – от диагностики заболеваний и оценки кредитного риска до управления транспортом и судопроизводства – вопрос доверия к библиотекам машинного обучения приобретает системообразующий характер. Пользователи, бизнес, научное сообщество и государственные регуляторы всё чаще требуют не только высокой точности моделей, но и доказуемой прозрачности, подотчётности, этической устойчивости и воспроизводимости. В этой связи открытый исходный код (open source) становится одним из ключевых механизмов формирования доверия. Он не только позволяет получить доступ к реализации алгоритмов, но и создает условия для коллективной экспертизы, многослойного контроля, независимого аудита и демократизации технологий. Настоящая статья направлена на глубокий анализ роли открытого кода в обеспечении доверенности ML-библиотек, включая технические, социальные, нормативные и организационные аспекты [1].

Прежде всего, открытый код обеспечивает прозрачность алгоритмической логики. В закрытых программных продуктах, где реализация алгоритма недоступна, пользователь не может проверить, как именно система принимает решение, на что она опирается, каким образом обрабатываются данные и какие предвзятости могут быть встроены в код. Открытый код позволяет специалистам в области машинного обучения, математики, права и этики исследовать и понимать внутреннюю структуру библиотеки: от архитектуры нейросети до реализации функций активации, потерь, нормализации, регуляризации и т.д. Такая открытость формирует базу для воспроизводимости научных результатов, что особенно важно в академических и критически регулируемых приложениях.

Не менее важна возможность проведения независимого аудита. В библиотеке с открытым кодом любая организация может привлечь внешнюю команду – будь то университет, консалтинговая фирма или регулятор – для проверки корректности, безопасности и соответствия нормативам. Это особенно актуально в условиях действия таких актов, как AI Act в Европейском

союзе, который требует от разработчиков демонстрации объяснимости и подотчётности алгоритмов. Открытый код позволяет не только выявить уязвимости или предвзятость, но и предложить их исправления, которые затем могут быть приняты сообществом или владельцами библиотеки.

Следующий аспект – это гибкость и адаптируемость. Открытые библиотеки можно доработать под конкретные задачи, будь то интеграция с защищёнными хранилищами, включение механизмов дифференциальной приватности, реализация специфических требований регулятора или встраивание в частную облачную инфраструктуру. Такая возможность особенно важна в организациях, работающих с чувствительными данными, где необходимо соблюдение строгих протоколов безопасности и совместимости. Закрытые библиотеки редко предоставляют такую степень контроля и настройки [2].

Открытый код также способствует коллективной ответственности и повышению качества. Механизмы peer review в open source-среде, поддержка issues, pull request-ов, архитектурных дискуссий и release notes формируют процесс постоянного улучшения и валидации. Чем шире и активнее сообщество вокруг библиотеки, тем выше шансы на быстрое выявление и исправление ошибок, включая неочевидные дефекты, уязвимости и некорректные реализации. Открытые библиотеки, такие как PyTorch, TensorFlow, scikit-learn или Hugging Face Transformers, поддерживаются тысячами разработчиков по всему миру, что делает их надёжными с точки зрения инженерной устойчивости и доверенного развития.

Значимым социальным следствием открытого кода является демократизация доступа к ИИ-технологиям. Разработчики, исследователи и студенты по всему миру получают возможность использовать и модифицировать современные инструменты без барьеров, связанных с лицензированием или коммерческими ограничениями. Это расширяет пул экспертов, вовлечённых в развитие доверенного ИИ, способствует диверсификации взглядов и культурных перспектив, снижает риски монополизации и способствует глобальной прозрачности. В условиях, когда технологии ИИ всё чаще становятся предметом геополитического соперничества, открытость кода также рассматривается как инструмент технологического суверенитета и цифровой независимости.

Открытый код напрямую поддерживает реализацию принципов ответственного ИИ (Responsible AI). Принципы объяснимости, справедливости, надёжности и защищённости, изложенные во многих международных документах, таких как IEEE Ethically Aligned Design, рекомендации OECD по ИИ, принципы AI4People, невозможно реализовать без доступа к технической реализации. Только открытый код делает возможным

внедрение этических тестов, автоматизированной оценки моделей на предмет предвзятости, симметричности или устойчивости к манипуляциям. Это позволяет не только разрабатывать этичные системы, но и строить механизмы этического аудита, в том числе автоматизированного, в рамках MLOps и ML Governance [3].

Существуют и вызовы. Не каждый открытый код по определению безопасен или корректен. Факт публичного размещения не гарантирует качество, поддержку или соответствие требованиям регулятора. Поэтому возникает необходимость развития институтов доверия поверх открытого кода: это и сертифицированные реестры (например, Trusted AI Components), и модели оценки зрелости проекта (по числу коммитов, активности сообщества, наличию тестов, CI/CD, документации), и независимые фонды поддержки (например, Linux Foundation AI, OpenSSF, LF AI & Data). Такие надстроенные институты позволяют отличить действительно надёжные и доверенные библиотеки от экспериментальных или устаревших [4].

Кроме того, встраивание открытого кода в корпоративную ИТ-инфраструктуру требует соблюдения политик лицензирования, анализа юридической совместимости, обеспечения безопасности цепочки поставок (supply chain security). Здесь на помощь приходят инструменты типа SPDX, OSLC, OpenChain, которые обеспечивают контроль происхождения компонентов, юридическую чистоту и формализацию использования open source в производственной среде. Таким образом, открытый код требует не только технической, но и правовой и организационной инфраструктуры, чтобы использовать его как компонент доверенного ИИ.

В заключение, открытый исходный код играет ключевую роль в формировании доверия к библиотекам машинного обучения. Он делает возможной техническую прозрачность, юридическую подотчётность, коллективную экспертизу, оперативное реагирование на ошибки, этическую верификацию и глобальную инклюзивность. В условиях роста регулируемости и общественного контроля над ИИ-системами открытый код превращается из инженерной практики в политико-этический механизм доверия. Поддержка и развитие экосистемы open source в области ИИ должны стать приоритетом для научных сообществ, компаний, государств и международных организаций, стремящихся к построению прозрачного, справедливого и устойчивого цифрового будущего [5].

Список литературы:

1. Raymond, E. S. The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary / E. S. Raymond. – Sebastopol : O'Reilly Media, 1999. – 241 p.

2. Ince, D. C. The Case for Open Computer Programs / D. C. Ince, L. Hatton, J. Graham-Cumming // Nature. – 2012. – Vol. 482, № 7386. – P. 485–488. – DOI 10.1038/nature10836.

3. Jiménez, R. C. Four Simple Recommendations to Encourage Best Practices in Research Software / R. C. Jiménez, M. Kuzak, M. Alhamdoosh [et al.] // F1000Research. – 2017. – Vol. 6. – P. 876. – DOI 10.12688/f1000research.11407.1.

4. Lamprecht, A.-L. Towards FAIR Principles for Research Software / A.-L. Lamprecht, L. Garcia, M. Kuzak [et al.] // Data Science. – 2020. – Vol. 3, № 1. – P. 37–59. – DOI 10.3233/DS-190026.

5. Soergel, D. Rampant Software Errors May Undermine Scientific Results / D. Soergel // F1000Research. – 2015. – Vol. 3. – P. 303. – DOI 10.12688/f1000research.5930.2.