

УДК 004.89

РАЗРАБОТКА ФРЕЙМВОРКА ДЛЯ БЕЗОПАСНОЙ ИНТЕГРАЦИИ МОДЕЛЕЙ В ПРОИЗВОДСТВЕННЫЕ СРЕДЫ

Журавлева Е.С., студент гр. ИУ12-21А, IV курс
Московский государственный технический университет имени Н. Э. Баумана,
г. Москва

Внедрение моделей машинного обучения в производственные системы требует особого внимания к вопросам безопасности, надёжности и управляемости. Современные промышленные и бизнес-процессы часто опираются на автоматизированные решения, где любые сбои или нарушения конфиденциальности данных могут привести к серьёзным финансовым и репутационным потерям. Поэтому создание специализированного фреймворка, предназначенного для безопасной интеграции ML-моделей в рабочие среды, является необходимым условием для успешного масштабирования и эксплуатации искусственного интеллекта в реальных условиях [1].

Главная задача такого фреймворка – обеспечить контроль над всеми этапами взаимодействия модели с производственной инфраструктурой, включая управление доступом, защиту данных, мониторинг работы и обновление. Для этого используется модульный подход, где каждая компонента отвечает за конкретный аспект безопасности и совместимости. Важной частью архитектуры становится изоляция моделей с помощью контейнеризации и применение средств оркестрации для гибкого управления вычислительными ресурсами и масштабирования.

Особое внимание уделяется обеспечению защищённого обмена данными между моделями и внешними системами. Это достигается путём внедрения криптографических протоколов, которые предотвращают несанкционированный доступ и обеспечивают целостность передаваемой информации. Кроме того, реализуются методы управления версиями моделей и конфигураций, что позволяет проводить безопасные обновления без прерывания работы сервисов [2].

В рамках фреймворка также интегрируются инструменты для непрерывного мониторинга качества моделей и выявления аномалий в их работе. Такой мониторинг важен для своевременного обнаружения деградации качества предсказаний и оперативного реагирования, что снижает риски, связанные с неправильными решениями в автоматизированных процессах.

Кроме того, ведётся аудит и журналирование всех операций, что помогает в расследовании инцидентов и повышении прозрачности [3].

Ключевым аспектом разработки является обеспечение совместимости с разнообразными технологиями и стандартами, принятыми в корпоративных и промышленных системах. Фреймворк должен легко интегрироваться с существующими платформами, инструментами DevOps и системами управления данными, поддерживая широкий спектр протоколов и форматов обмена [4].

Также важным элементом становится соответствие требованиям законодательства и внутренним политикам безопасности организаций. Для этого в систему включаются механизмы контроля соблюдения нормативов, управления правами доступа и защиты персональных данных, что позволяет не только снизить юридические риски, но и повысить доверие пользователей и партнеров.

Таким образом, разработка специализированного фреймворка для безопасной интеграции моделей машинного обучения в производственные среды – это комплексная задача, объединяющая технические, организационные и правовые аспекты. Создание таких решений способствует устойчивому и контролируемому развитию искусственного интеллекта в реальных условиях, позволяя извлекать максимальную пользу при минимальных рисках. В дальнейшем важным направлением станет расширение функциональности фреймворков с акцентом на автоматизацию процессов безопасности и адаптацию к новым вызовам цифровой трансформации [5].

Список литературы:

1. Breck, E. The ML Test Score: A Rubric for ML Production Readiness and Technical Debt Reduction / E. Breck, S. Cai, E. Nielsen [et al.] // IEEE International Conference on Big Data. – 2017. – P. 1123–1132. – DOI 10.1109/BigData.2017.8258038.
2. Baylor, D. TFX: A TensorFlow-Based Production-Scale Machine Learning Platform / D. Baylor, E. Breck, H.-T. Cheng [et al.] // Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2017. – P. 1387–1395. – DOI 10.1145/3097983.3098021.
3. Zaharia, M. Accelerating the Machine Learning Lifecycle with MLflow / M. Zaharia, A. Chen, A. Davidson [et al.] // IEEE Data Engineering Bulletin. – 2018. – Vol. 41, № 4. – P. 39–45.
4. Kreuzberger, D. Machine Learning Operations (MLOps): Overview, Definition, and Architecture / D. Kreuzberger, N. Kühl, S. Hirschl // IEEE Access. – 2023. – Vol. 11. – P. 31866–31879. – DOI 10.1109/ACCESS.2023.3262138.

5. Beyer, B. Site Reliability Engineering: How Google Runs Production Systems / B. Beyer, C. Jones, J. Petoff, N. R. Murphy. – Sebastopol : O'Reilly Media, 2016. – 552 p.