

УДК 004.89

ИСПОЛЬЗОВАНИЕ КОНТЕЙНЕРИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ ДОВЕРИЯ К ML-ИНСТРУМЕНТАМ

Третьякова М.Д., студент гр. ИУ12-41М, II курс
МГТУ им. Н. Э. Баумана, г. Москва

В современном ландшафте разработки и эксплуатации систем машинного обучения (ML) контейнеризация становится ключевой технологией, существенно влияющей на надёжность, воспроизводимость и безопасность ML-инструментов. Рост сложности моделей, разнообразие окружений и необходимость быстрой масштабируемости создают вызовы, которые традиционные методы развертывания и управления программным обеспечением не всегда способны эффективно решать. Использование контейнеризации – технологии, позволяющей упаковывать приложения и все их зависимости в единый, переносимый и изолированный от других процессов контейнер – становится важнейшим инструментом для повышения доверия к ML-инструментам на всех этапах их жизненного цикла. В данной статье рассматриваются основные преимущества, архитектурные особенности и практические аспекты применения контейнеризации в области машинного обучения с акцентом на обеспечение безопасности и доверия [1].

Одним из ключевых преимуществ контейнеризации является обеспечение изоляции среды исполнения. ML-модели и связанные с ними компоненты, включая библиотеки, зависимости и конфигурации, упаковываются в контейнеры, что позволяет избежать конфликтов между различными версиями программного обеспечения и гарантировать идентичность окружения при развертывании в разных средах – от локальных рабочих станций до облачных платформ и кластеров. Такая воспроизводимость критически важна для доверия, так как позволяет точно повторять эксперименты, анализировать результаты и обеспечивать согласованность между разработкой, тестированием и продуктивной эксплуатацией.

Кроме того, контейнеризация значительно упрощает управление безопасностью ML-инструментов. Изоляция контейнеров снижает риски, связанные с нежелательным воздействием одной компоненты на другую, а также ограничивает возможные векторы атак, уменьшая поверхность атаки. Современные оркестрационные системы, такие как Kubernetes, предоставляют возможности для настройки политик безопасности, контроля доступа, сетевой сегментации и мониторинга, что позволяет реализовать многоуровневую

защиту на уровне инфраструктуры. Это особенно важно при работе с конфиденциальными данными и чувствительными моделями, где даже незначительные утечки или модификации могут иметь серьёзные последствия [2].

Контейнеризация также способствует упрощению процессов обновления и масштабирования ML-инструментов. Контейнеры можно быстро развёртывать, обновлять и масштабировать без необходимости глубокой модификации основной инфраструктуры. Это повышает гибкость и оперативность реагирования на изменения требований или выявленные уязвимости, что в свою очередь повышает доверие пользователей и операторов к системе. Автоматизация развёртывания с помощью CI/CD-пайплайнов дополнительно снижает вероятность ошибок и обеспечивает согласованность версий компонентов.

Важным аспектом является возможность интеграции контейнеров с инструментами мониторинга и логирования, которые обеспечивают прозрачность работы ML-инструментов и позволяют в реальном времени отслеживать их производительность, устойчивость и безопасность. Наличие подробных логов и метрик способствует быстрому обнаружению аномалий, инцидентов и отклонений от ожидаемого поведения, что является основой для построения доверенных и управляемых систем [3].

Однако использование контейнеризации в ML-средах требует учёта некоторых специфических особенностей и вызовов. Например, контейнеры должны поддерживать эффективное использование ресурсов, включая GPU и специализированные аппаратные ускорители, что важно для производительности моделей глубокого обучения. Также необходимо правильно управлять хранением и обменом данными между контейнерами, чтобы избежать утечек и обеспечить согласованность данных в распределённых вычислительных системах [4].

Кроме технических аспектов, контейнеризация способствует улучшению процессов совместной работы между командами разработки, тестирования и эксплуатации. Благодаря стандартизированным и изолированным средам специалисты могут работать с единым набором инструментов и конфигураций, что снижает риски недопонимания и ошибок, а также ускоряет внедрение новых моделей и функциональности.

В итоге, применение контейнеризации в машинном обучении является важным фактором повышения доверия к ML-инструментам, обеспечивая воспроизводимость, безопасность, управляемость и масштабируемость. Это позволяет создавать более надёжные и предсказуемые системы искусственного интеллекта, готовые к использованию в критически важных и регулируемых сферах. Перспективы развития данной области связаны с интеграцией

контейнерных технологий с другими решениями по безопасности, автоматизации и управлению жизненным циклом моделей, что будет способствовать формированию комплексной и доверенной инфраструктуры для машинного обучения будущего [5].

Список литературы:

1. Felter, W. An Updated Performance Comparison of Virtual Machines and Linux Containers / W. Felter, A. Ferreira, R. Rajamony, J. Rubio // IEEE International Symposium on Performance Analysis of Systems and Software. – 2015. – P. 171–172. – DOI 10.1109/ISPASS.2015.7095802.
2. Pahl, C. Containerization and the PaaS Cloud / C. Pahl // IEEE Cloud Computing. – 2015. – Vol. 2, № 3. – P. 24–31. – DOI 10.1109/MCC.2015.51.
3. Burns, B. Borg, Omega, and Kubernetes / B. Burns, B. Grant, D. Oppenheimer [et al.] // Communications of the ACM. – 2016. – Vol. 59, № 5. – P. 50–57. – DOI 10.1145/2890784.
4. Open Container Initiative. Runtime Specification [Электронный ресурс]. – URL: <https://github.com/opencontainers/runtime-spec> (дата обращения: 09.06.2025).
5. Kubernetes Documentation. Production-Grade Container Orchestration [Электронный ресурс]. – URL: <https://kubernetes.io/docs/> (дата обращения: 09.06.2025).