MWS × DevOps Conf 2026

Результаты опроса о DevOps-практиках от MWS Cloud Platform и DevOpsConf 2026

M W S × DevOps Conf 2026

Срез DevOps-практик

Опрос проводился:
с 13 марта по 3 апреля

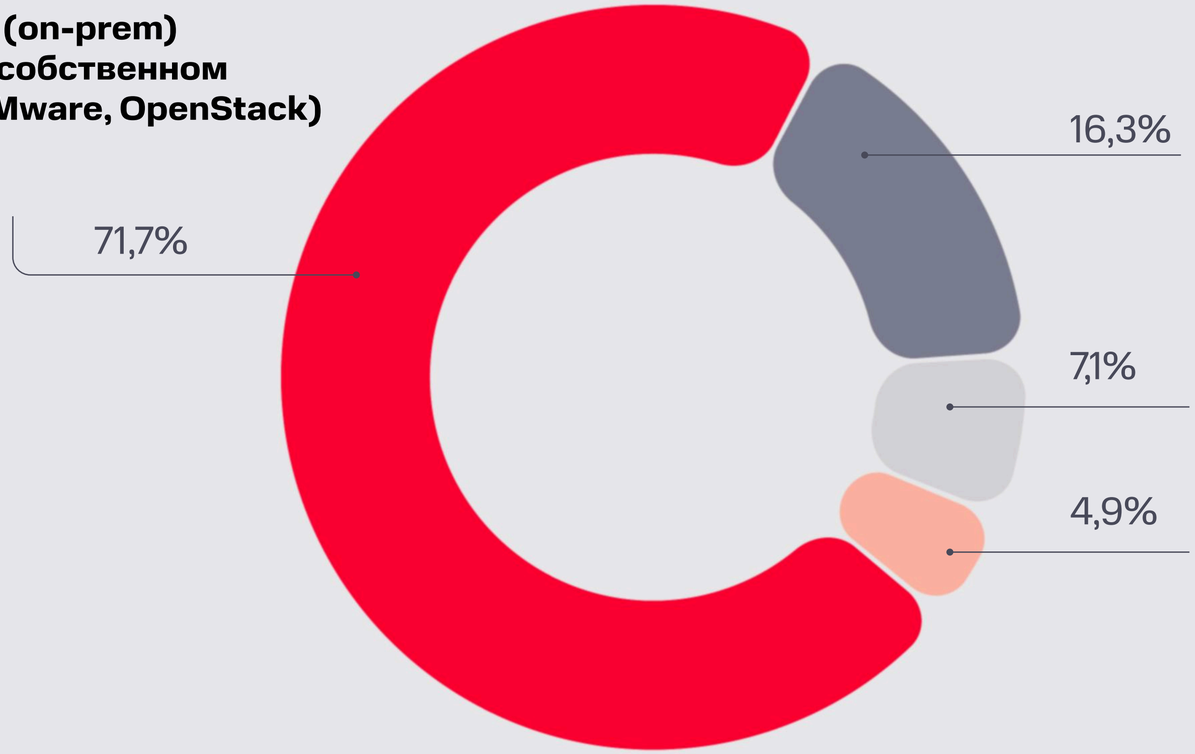
Участники:
DevOps-инженеры, SRE, Platform Engineers, архитекторы платформенных решений, TechLead, TeamLead

Направления:
DevOps • K8S • AI • Security • IDP • инцидент-менеджмент

M W S × DevOps Conf 2026

Kubernetes

Как развёрнуты ваши основные Kubernetes-кластеры?



Своя инфраструктура (on-prem) на арендованном или собственном железе (Bare-Metal, VMware, OpenStack)

В публичных облаках с использованием managed-сервисов облачных провайдеров (MWS Cloud, Yandex Cloud, VK Cloud, Cloud.ru)

Не используются Kubernetes-кластеры

В публичных облаках self-managed Kubernetes (самостоятельное управление Kubernetes-инфраструктурой)

Как развёрнуты ваши production-окружения?

Несколько зон доступности (дата-центров),географически распределённых у разных провайдеров (решение проблем с latency и/или data residency)

31%

30,4%

Несколько зон доступности (дата-центров) у одного провайдера

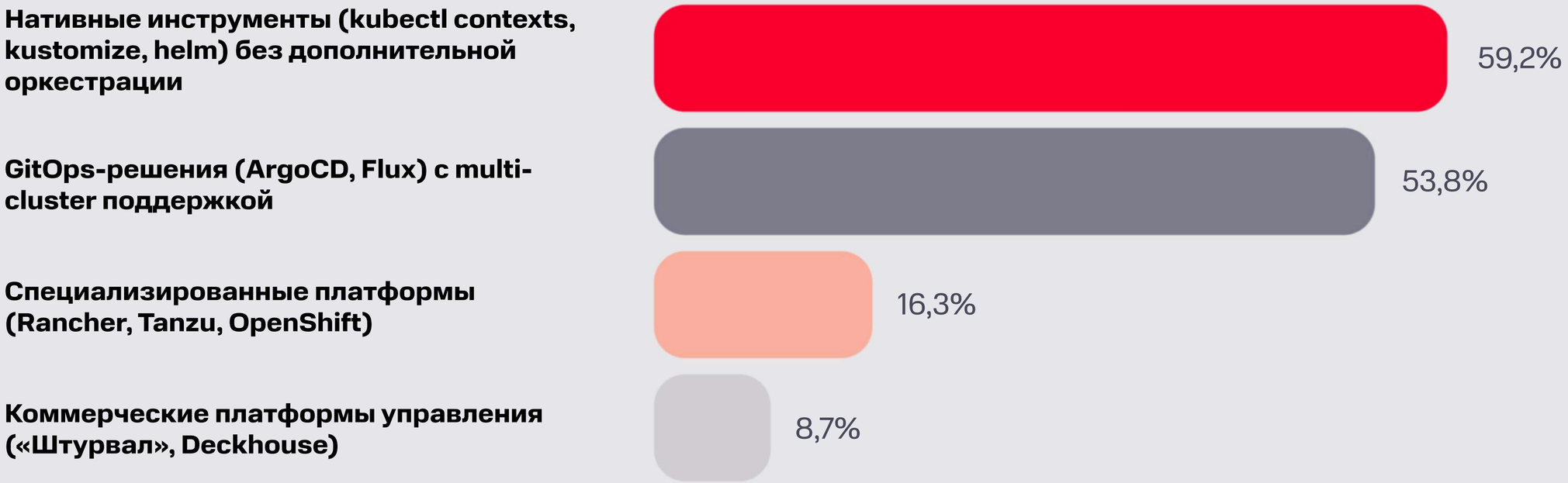
19%

19,6%

Несколько зон доступности (дата-центров) у разных провайдеров

Одна зона доступности (дата-центр)

Какие инструменты вы используете для управления несколькими Kubernetes-кластерами?



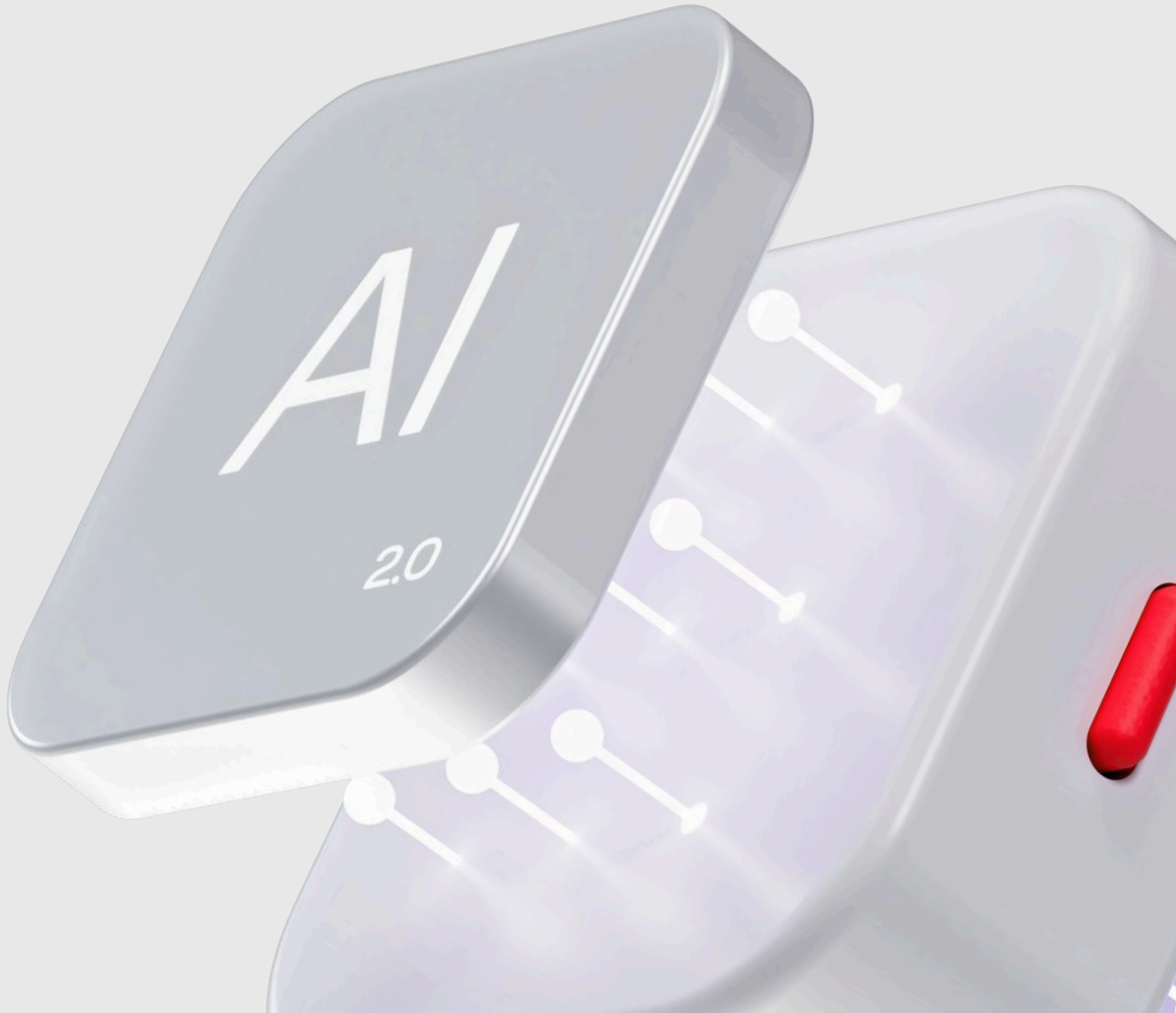
Комментарий эксперта MWS Cloud Platform

> Российский рынок Kubernetes заметно повзрослел. Компании одна за другой переходят на него, что характерно, выбирают «ванильные» сборки. Причина простая: не хочется привязываться к конкретному вендору. Если потребуется переехать с одной инфраструктуры на другую, это делается быстро, без лишних проблем.
>
> В облачной среде большинство уже строит инфраструктуру сразу на двух-трёх провайдерах, понижая тем самым риски. Но многие команды до сих пор живут на on-premise инсталляциях, но тренд идёт на спад, и главная причина здесь — TCO собственной инфраструктуры неумолимо растёт.

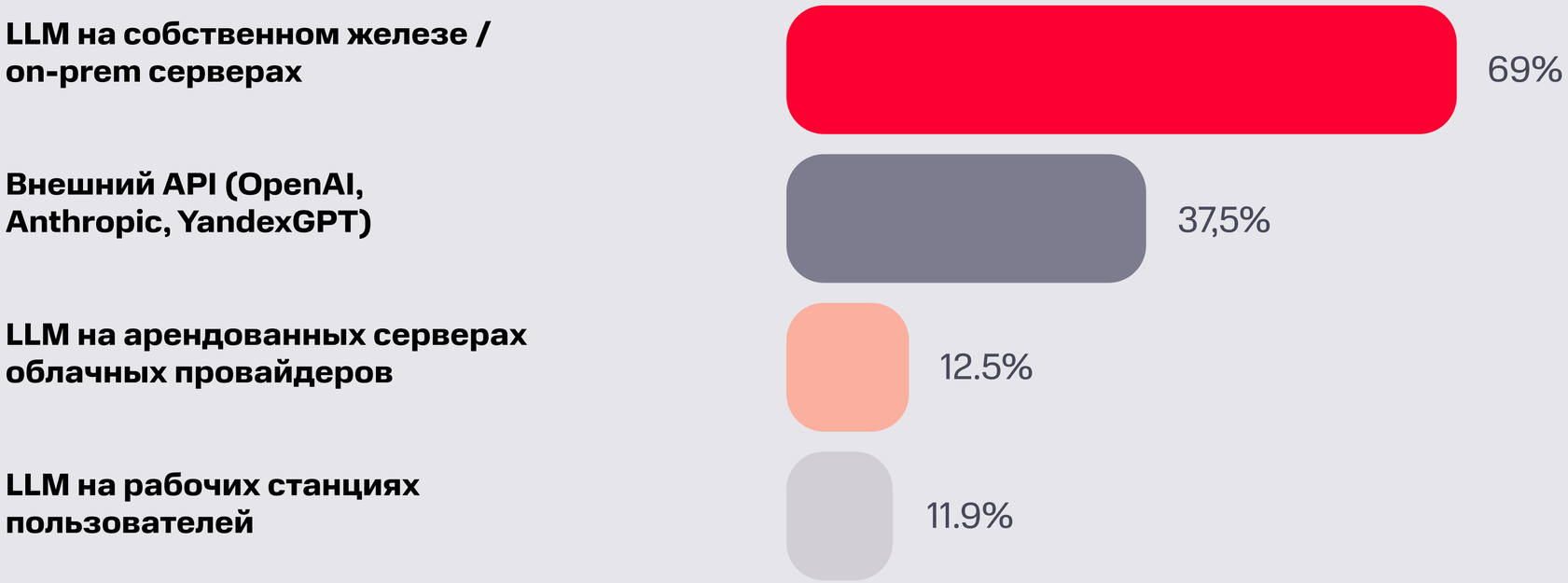
Андрей Дикий
CTO Container Ecosystem, MWS Cloud Platform

M W S × DevOps Conf 2026

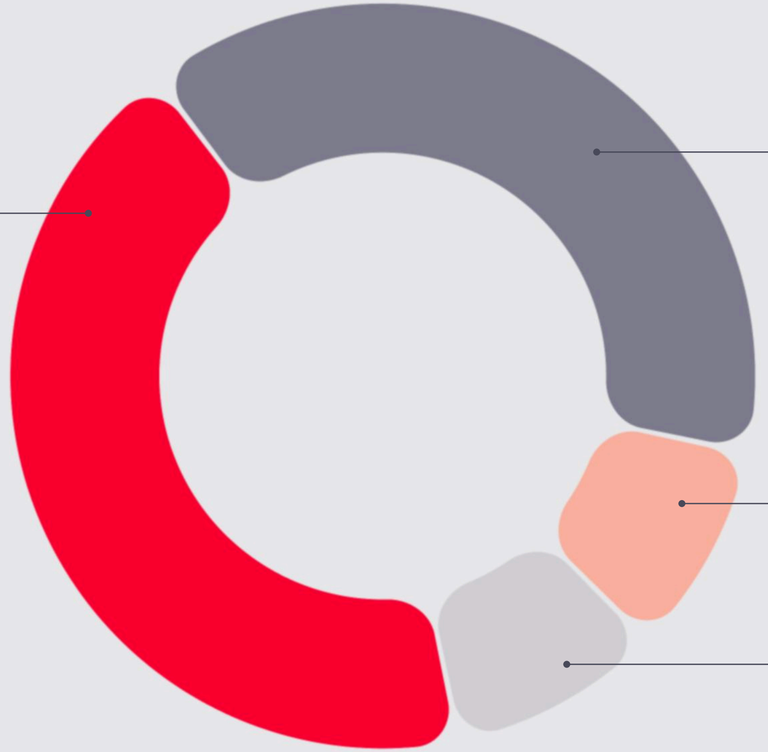
AI



Как ваш проект или компания в настоящее время использует языковые модели (LLM)?



Как вы подключаете свои LLM к внутренним базам знаний и данным?



42,9%

Не используем, модель работает только со своими встроенными знаниями

38,6%

Собрали свой RAG-пайплайн с помощью open-source фреймворков (LangChain, LlamaIndex) и self-hosted векторной базы (Qdrant, Chroma)

9,2%

Используем готовые RAG-решения из конструкторов чат-ботов или AI-платформ

9,2%

Используем управляемый векторный сервис (например, от Yandex, Google) и сами управляем связкой с LLM

Как вы интегрируете свои LLM с существующими системами и инструментами?

Изучаем или планируем внедрять в ближайшее время интеграции LLM с существующими системами и инструментами

35,9%

23,4%

Нет необходимости интегрировать наши LLM с существующими системами и инструментами

19,6%

Интеграция LLM с другими системами осуществляется вне AI-контура (стандартные API и кастомные интеграции)

21,2%

Уже используем MCP (Model Context Protocol) или его аналоги в наших проектах

Комментарий эксперта MWS Cloud Platform

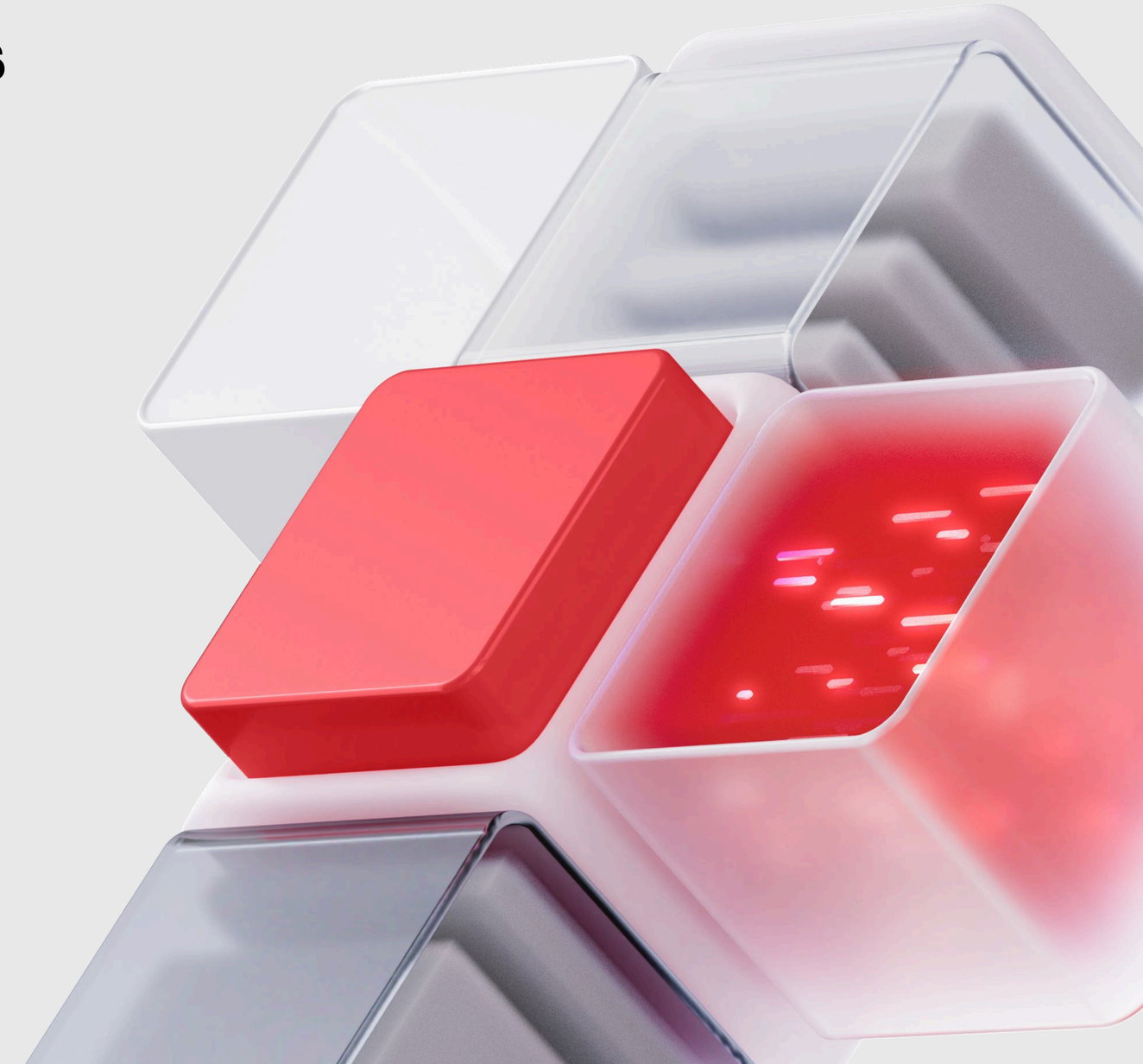
> Рынок внедрения LLM переходит от экспериментов к практическому применению: многие компании ещё оценивают сценарии, но около половины уже начали внедрение. При этом подходы остаются фрагментированными — от использования API до собственных RAG-пайплайнов и глубокой интеграции через MCP.
>
> Хотя сейчас есть уклон в сторону on-prem, стратегически рынок движется в облако. Поддержка SOTA-моделей требует значительных ресурсов и экспертизы, доступных немногим, поэтому облачные и API-решения становятся не только быстрым стартом, но и долгосрочной моделью с лучшей масштабируемостью и экономикой.

Никита Казарян

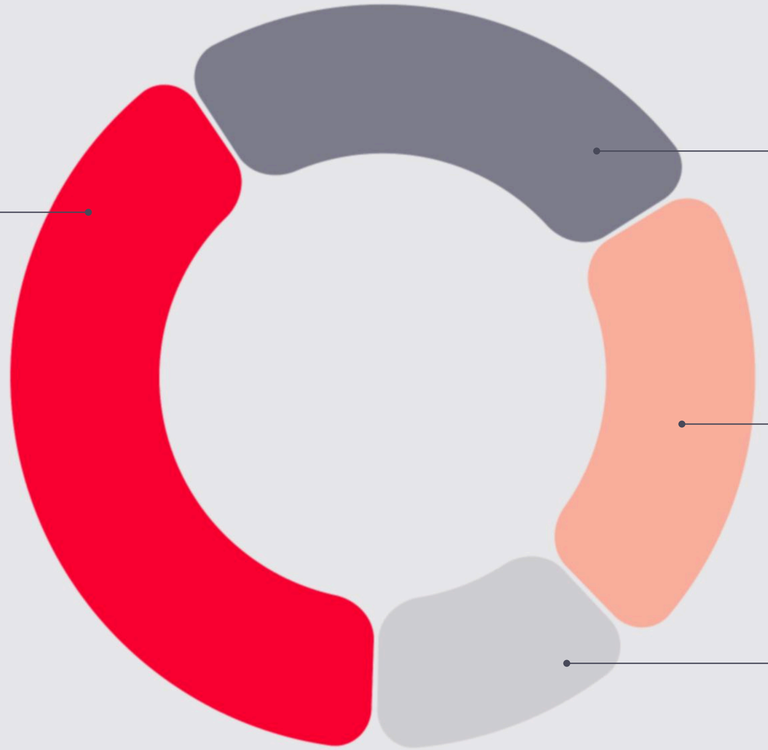
Руководитель направлений AI Platform и Security Platform, MWS

MWS × DevOps Conf 2026

Security



Как у вас организовано управление доступом к продакшену?



40,2%

Централизованная модель через IAM/SSO с маппингом ролей

25,5%

Ролевые модели стандартизированы по типам команд (dev, ops, qa и т. д.)

21,7%

Используется принцип least privilege с регулярным аудитом ролей

12,5%

Минимальная базовая настройка, права распределяются вручную

Как реализован аудит действий в продакшене?

49,5%

Аудитные логи централизованно собираются (ELK, Loki, SIEM)

26,6%

Есть автоматические алерты на подозрительные действия, и проводится регулярный аудит прав и действий

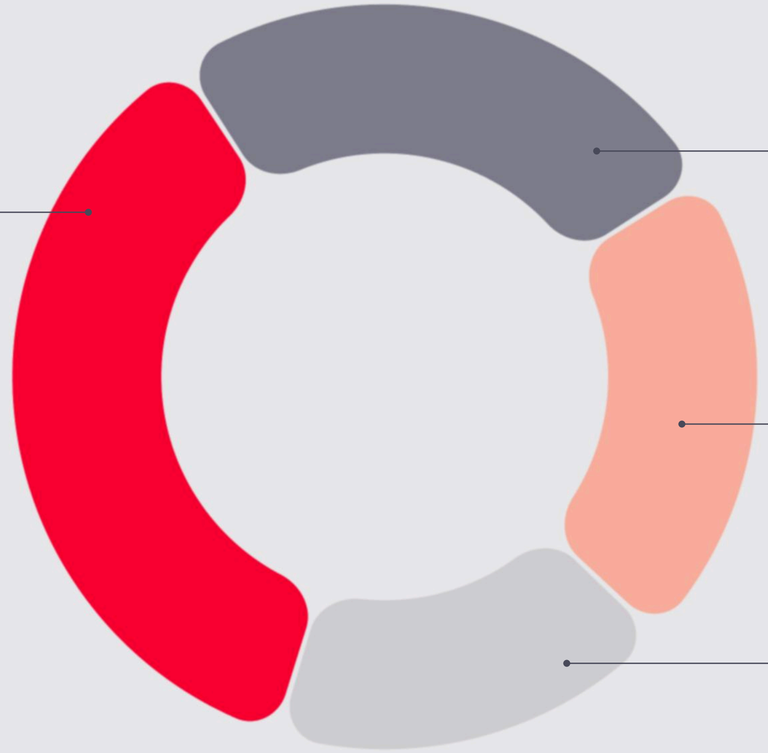
12,5%

Есть аудитные логи «на местах» (требуется сбор логов по сервисам при расследовании инцидентов)

11,4%

Не знаю или нет аудитных логов о действиях, совершаемых с продакшеном

Используете ли вы шифрование данных (практика encryption at rest или данные в s3/database)?



37%

Используем шифрование только для секретных ресурсов (опционально используется внешний KMS)

23,4%

Шифруем разные типы ресурсов (опционально используется внешний KMS)

20,7%

Не знаю, есть ли у нас шифрование данных

19%

Осознанно не используем шифрование данных (ради скорости либо есть другой контур защиты)

Комментарий эксперта MWS Cloud Platform

> Результаты показывают, что базовые практики безопасности в продакшене уже широко внедрены, но зрелость сильно варьируется.
>
> С одной стороны, почти половина компаний централизует доступ через IAM/SSO и собирает аудитные логи в единую систему — это хороший признак движения к управляемой и наблюдаемой безопасности. Также заметна доля команд, применяющих least privilege и автоматические алерты, что говорит о переходе от формального контроля к практическому снижению рисков.
>
> С другой стороны, остаётся значимый «разрыв зрелости»: часть команд по-прежнему управляет доступами вручную, аудит либо фрагментирован, либо отсутствует как процесс, около 20% не уверены, используется ли шифрование данных вообще.
>
> Особенно показательно, что шифрование часто применяется точечно (только для секретов), а не как стандарт по умолчанию. Это указывает на реактивный, а не системный подход к защите данных.
>
> Главный вывод: индустрия в целом прошла этап «есть хоть какая-то безопасность» и движется к более зрелым практикам, но всё ещё не хватает стандартизации и подхода secure by default.

Георгий Фатеев
Ведущий разработчик, MWS

M W S × DevOps Conf 2026

IDP

Есть ли в вашей компании команда IDP (Internal Development Platform) для решения инфраструктурных задач?

47,3%

Есть команда IDP и общая инфраструктура для развёртывания

21,7%

Каждая команда самостоятельно решает вопросы со своей инфраструктурой

20,1%

Есть общие требования в компании, и каждая команда строит свою инфраструктуру в соответствии с ними

10,9%

Есть виртуальная команда IDP (группа энтузиастов из разных команд) и общая инфраструктура для развёртывания

Как вы относитесь к необходимости иметь IDP (Internal Development Platform) в вашей компании для сборки и развёртывания в продакшене?

48,9%

Есть подобная IDP и оцениваю её положительно (удобная автоматизация рутины)

26,1%

Не знаю или считаю — нет никакой необходимости в IDP

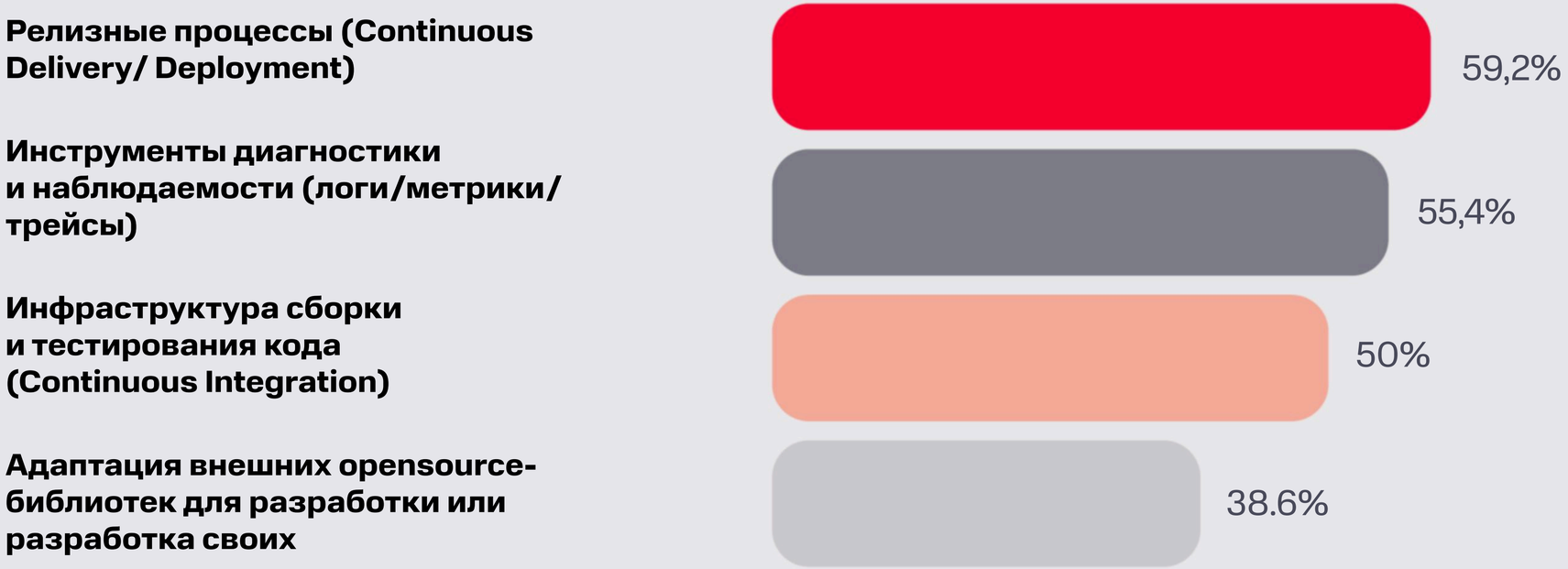
19,6%

Есть подобная IDP и оцениваю её нейтрально (не мешает и не помогает)

5,4%

Есть подобная IDP и оцениваю её отрицательно (бюрократия, лишние действия, плохой UX)

Какие проблемы решает или должна решать IDP (Internal Development Platform) в вашей компании?



Комментарий эксперта MWS Cloud Platform

Почти половина (47,3%) опрошенных работает в компаниях с общей инфраструктурой и командой IDP (Internal Development Platform). Это показывает высокий уровень зрелости инженерной культуры в компаниях. Многие (48,9%) очень позитивно оценивают вклад IDP в свою работу, то есть идёт активная работа с внутренними пользователями и не только «кнут» используется для внедрения внутренних платформ.

Закономерно IDP используется для релизных процессов, диагностики/наблюдаемости и сборки/тестирования. Это «низко висящие фрукты», и это проще всего продать бизнесу. Но это мешает воспринимать команду IDP как продуктовую полного цикла. Многие считают это инфраструктурой поддержки кода. Предположу, что история с адаптацией внешних библиотек и написания своих будет активно развиваться, по мере роста зрелости IDP-платформ.

Сергей Киселев

Руководитель направления Development Platform, MWS Cloud Platform

MWS × DevOps Conf 2026

Управление инцидентами

Как вы приносите опасные изменения (миграции) на продакшен?

Как устроен процесс разбора прошедших инцидентов в вашей компании?

45,7%

Разбираем инциденты узким кругом экспертов на встречах (приватный Live Site Review)

28,3%

Есть процесс разбора инцидентов назначенными экспертами (без разбора на всех)

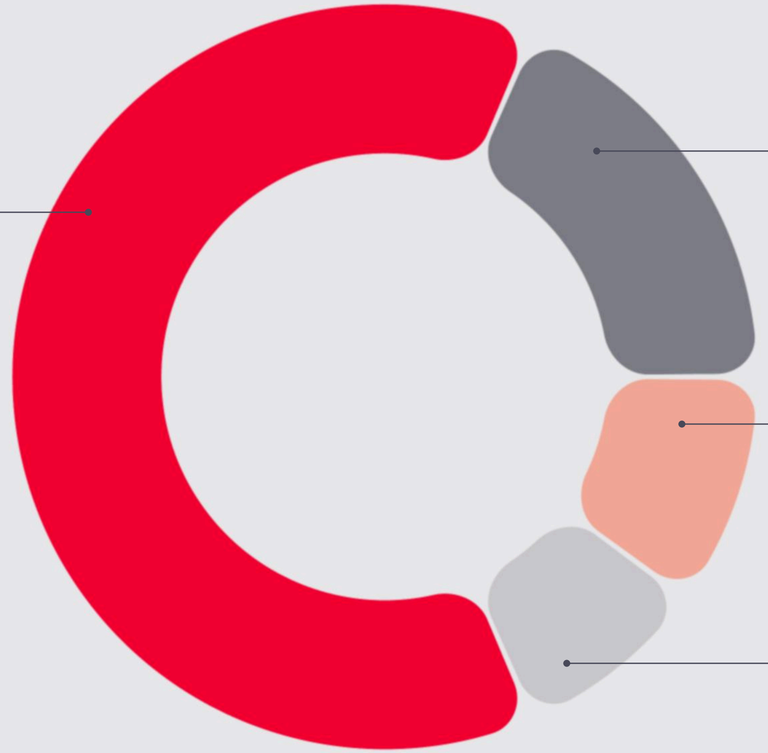
20,7%

Разбираем инциденты внутри компании на открытых встречах (Live Site Review)

5,4%

Не проводим или не видим смысла в разборе прошедших инцидентов

Публикуете ли вы отчёты об инцидентах?



61,4%

Отчёты об инцидентах доступны только для внутреннего использования

18,5%

Предоставляем отчёты об инцидентах некоторым пользователям либо регуляторам по запросу

11,4%

Не пишем отчёты об инцидентах

8,7%

Публикуем публичные отчёты об инцидентах для наших пользователей

Комментарий эксперта MWS Cloud Platform

> Российские команды выстроили сильную защиту на входе в продакшен: тестирование на стенде стало нормой, планы отката пишутся заранее. Но интересно, что при этом feature flags используются заметно реже — а ведь именно они дают контроль после деплоя, когда стенд уже бессилен. Это говорит о том, что мышление всё ещё больше про «не пустить плохое», а не про «быстро откатить плохое в проде».
>
> Разбор инцидентов узким кругом экспертов — самый популярный формат, и в этом есть логика: на встрече те, кто глубоко в контексте сервиса, без лишнего шума. Вопрос не в том, сколько людей на разборе, а в том, что происходит дальше — доходят ли выводы до смежных команд. Если доходят, узкий формат работает отлично. Если нет, знание замыкается в бункере.

Алексей Мыльцев

Руководитель направления Storage SRE, MWS Cloud Platform

MWS × DevOps Conf 2026

Спасибо всем участникам опроса

Ваши ответы формируют картину DevOps-практик на рынке и помогают развивать профессиональное сообщество