monq

ОТЧЕТ К ИССЛЕДОВАНИЮ

Использование Open Source решений системного и инфраструктурного уровня в российских организациях

Подготовлено аналитическим центром ООО «Монк Диджитал Лаб»

Ответственный за отчет:

управляющий партнер ООО «Монк Диджитал Лаб»

Ганюшкин Николай Александрович

19.08.2025

monq.ru

Оглавление

Введение и цели исследования 1

Методология и выборка 2

Использование Open Source в инфраструктуре 4

Практики внедрения, обновлений и модификации Open Source 9

Анализ рисков и инцидентов при использовании Open Source 11

Экономические аспекты и преимущества Open Source (TCO-анализ) 16

Барьеры и ограничения перехода на отечественные альтернативы 18

Прогноз на 3 года и стратегические сценарии 21

Прогноз доли Open Source через 3 года 23

Комментарии и оценки ИТ-лидеров: взгляд на Open Source от экспертов рынка 24

Выводы 27

Практические рекомендации 28

Список источников и приложения 29

Приложение А. Анкета опроса ИТ-директоров 30

Приложение В. Словарь терминов и методологические комментарии 31

Введение и цели исследования

Открытое программное обеспечение (Open Source Software, OSS) стало неотъемлемой частью современного ИТ-ландшафта. После ухода с российского рынка ряда западных вендоров бизнес и государственные структуры обратили особое внимание на Open Source как на способ сохранить доступ к современным технологиям и снизить зависимость от импорта. Уже к 2024 году порядка 80–83% российских компаний используют или планируют использовать открытые программные решения[1]. Для крупного бизнеса этот показатель еще выше – по оценкам, около 90% предприятий уровня **enterprise** применяют Open Source в своей ИТ-инфраструктуре[2].
Еще в 2021 году исследование Accenture и «Сколково» прогнозировало, что к 2026 году свыше 90% российских компаний будут использовать открытое ПО[3], и эти ожидания близки к реальности.

80–83%
доля OSS в 2024 году

>90%
прогноз на 2026 год

Основные цели исследования

- Оценить текущее проникновение и использование Open Source по различным слоям ИТ-инфраструктуры (операционные системы, СУБД, виртуализация, контейнеризация, DevOps-инструменты, мониторинг, резервное копирование и др.)
- Изучить практики внедрения, сопровождения, обновления и модификации Open Source-продуктов в организациях
- Выявить ключевые риски, связанные с использованием открытого кода, а также реальные инциденты, с которыми столкнулись компании
- Проанализировать экономические аспекты: выгоды от Open Source, совокупная стоимость владения (TCO) и сравнение с проприетарными решениями
- Изучить барьеры и ограничения на пути перехода от Open Source к отечественным проприетарным аналогам в контексте программы импортозамещения
- Представить прогноз на ближайшие три года относительно доли Open Source в ИТ-инфраструктуре и рассмотреть возможные сценарии (например, ужесточение регуляторики или, наоборот, развитие экосистемы открытого кода)
- Привести комментарии и оценки ИТ-лидеров и экспертов отрасли относительно долгосрочного использования Open Source и необходимых компетенций
- В приложении представить пресс-релиз с ключевыми результатами исследования, предназначенный для широкого круга СМИ

Данное исследование посвящено тому, **как именно** российские организации используют Open Source в области инфраструктурного и системного ПО (за исключением области ИБ), с какими практиками и трудностями они сталкиваются, и какую роль открытое ПО играет в их стратегиях.

Исследование носит прикладной характер и рассчитано на деловую ИТ-аудиторию. Аналитический стиль изложения поддерживается фактическими данными опроса и внешними источниками, ссылки на которые приведены по тексту.
Отчет структурирован по перечисленным разделам и предоставляет целостную картину текущего состояния и перспектив использования OSS в российских организациях.

Методология и выборка

Основой отчета стал опрос ИТ-директоров и руководителей ИТ-подразделений российских организаций, проведенный в августе 2025 года. Анкета включала как количественные, так и качественные вопросы, охватывающие использование Open Source на разных уровнях ИТ-стека, практики и проблемы эксплуатации, а также взгляды на будущее открытого ПО. Дополнительно были собраны экспертные комментарии от лидеров отрасли для качественного анализа

Выборка

В опросе приняли участие 138 организаций различного масштаба и отраслевой принадлежности. География охватывает Россию, преимущественно ЦФО.
Структура выборки по размеру компаний: около **50%** респондентов представляют крупный бизнес (более 5000 сотрудников), **30%** – средние компании (1000–5000 сотрудников) и **20%** – организации с численностью до 1000 человек.

Такое распределение обеспечивает репрезентативность ответов крупных предприятий, на долю которых приходится основная часть ИТ-инфраструктуры страны.

По отраслям респонденты распределились следующим образом:
~23% приходится на промышленность, добывающий сектор и энергетику; **17%** – на финансовый сектор и финтех;
14% – на ритейл и e-commerce; **~12%** – на государственный сектор; оставшиеся **~33%** – другие отрасли (телеком, ИТ, услуги и др.)

Таким образом, охвачен широкий спектр экономических секторов – от госорганов и предприятий ТЭК до ИТ-компаний и онлайн-бизнеса. Это позволяет увидеть отраслевую специфику в использовании Open Source.

Осведомленность респондентов

Примечательно, что подавляющее большинство опрошенных ИТ-директоров (≈95%) хорошо осведомлены о том, какие программные решения (как проприетарные, так и Open Source) используются в их организации. Лишь единицы (менее 5%) признались, что имеют поверхностное представление. Таким образом, данные опроса можно считать надежными – ответы дают лица, глубоко погруженные в свою ИТ-архитектуру. Этот факт коррелирует с отраслевыми обзорами, согласно которым более 80% российских компаний уже используют решения с открытым исходным кодом в своих инфраструктурах[4]. Иначе говоря, тема Open Source находится в фокусе внимания отечественных ИТ-руководителей.

Определения и границы исследования

Под Open Source в опросе подразумеваются программные продукты с открытым исходным кодом, распространяемые по лицензиям, соответствующим критериям Open Source Initiative (MIT, GPL, Apache 2.0, BSD и др.), а также их форки и решения на их основе. В контексте импортозамещения упоминаются также «отечественные продукты», под которыми понимается коммерческое ПО российских разработчиков, включая продукты из реестра Минцифры РФ (некоторые из них основаны на OSS). Вопросы опроса фокусировались на инфраструктурном программном обеспечении (Infrastructure Software) – системах, платформенных решениях, инструментах для разработки и администрирования.
Бизнес-приложения (ERP, CRM и т.п.) прямо не рассматривались, хотя в комментариях респонденты могли упоминать и их.

Ограничения

Результаты опроса отражают мнение ИТ-директоров и могут не полностью учитывать точку зрения рядовых разработчиков или инженеров эксплуатации. Кроме того, опрос проводился среди организаций, уже имеющих опыт использования OSS, поэтому в выборке почти отсутствуют компании, полностью избегающие Open Source (что само по себе показатель тенденции). Анкетирование проводилось в условиях 2025 года – крайне динамичного периода для ИТ-отрасли РФ, и восприятие рисков/стратегий могло меняться по ходу развития событий (санкции, новые требования регуляторов и т.д.). Тем не менее, совокупность количественных данных и экспертных мнений дает целостное представление о роли Open Source на текущий момент.

Обработка данных

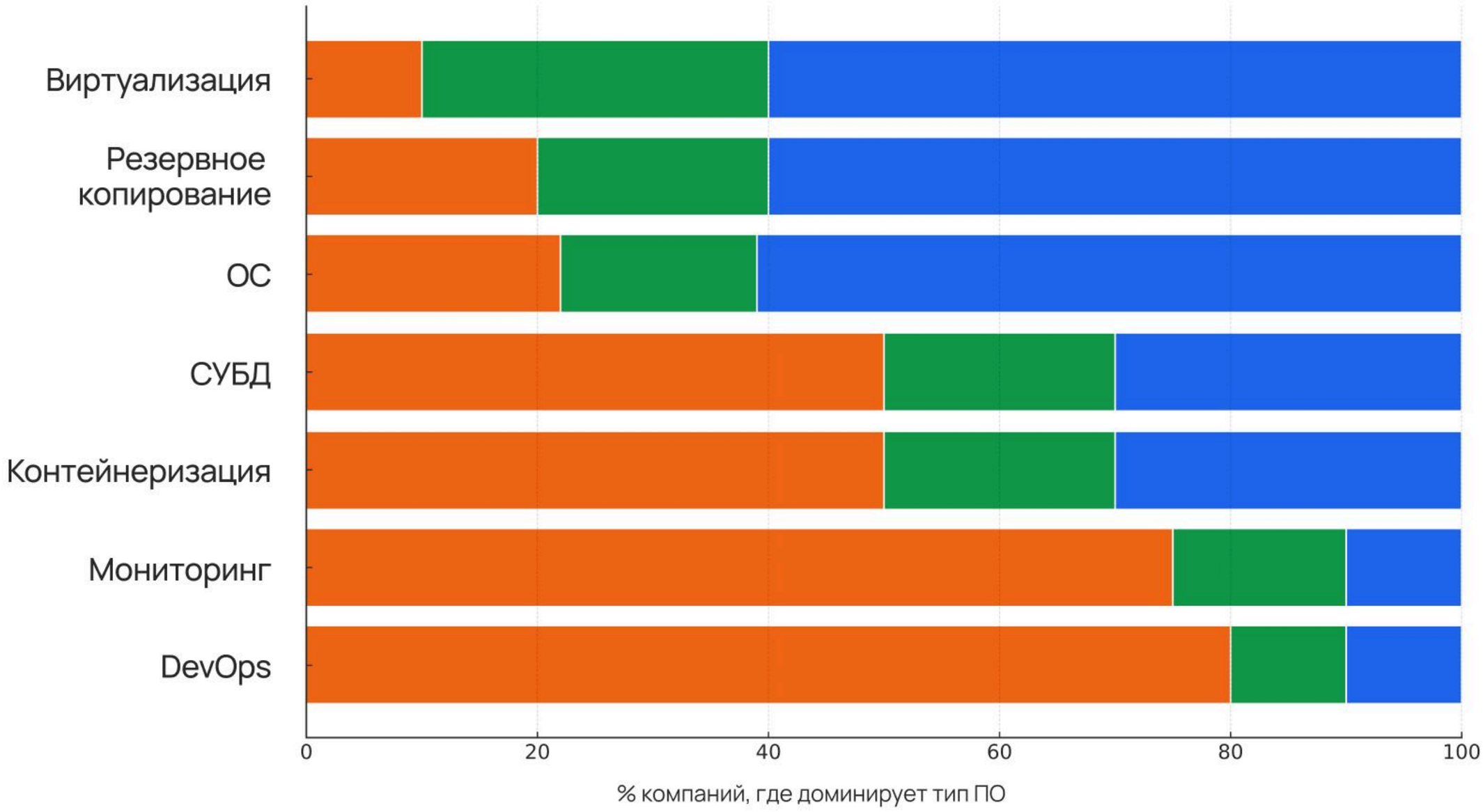
Количественные ответы агрегированы и представлены в виде процентов от числа респондентов, зачастую с разбивкой по сегментам. Качественные комментарии классифицированы по темам. Для проверки и дополнения результатов привлечены внешние аналитические отчеты (например, исследование ГК В1 2024 года[1][2] и др.), ссылки на которые приведены в тексте.
Такой подход обеспечивает верификацию выводов и позволяет соотнести их с общерыночными трендами.

Далее в отчете представлены результаты исследования, структурированные по ключевым темам. →

Использование Open Source в инфраструктуре (по слоям)

Опрос показал, что Open Source проник во все уровни ИТ-инфраструктуры российских организаций, хотя степень этого проникновения различается в зависимости от категории систем. Ниже приводится анализ использования OSS в основных слоях инфраструктуры – от операционных систем до инструментов DevOps – с указанием долей компаний, для которых соответствующие решения преобладают.

Срез по инфраструктуре



Далее подробно про каждый слой. →

Операционные системы (ОС)

Серверные ОС. Около половины опрошенных указали, что продолжают использовать западные проприетарные серверные ОС (прежде всего Microsoft Windows Server) на большинстве систем. Тем не менее, значительная доля уже переориентировалась на открытые и отечественные платформы. У 22% респондентов преобладают открытые ОС семейства Linux (например, Ubuntu Server, Debian, CentOS/AlmaLinux). Еще ~17% используют преимущественно отечественные операционные системы из реестра Минцифры – такие как Astra Linux, РЕД ОС, Rosa и др. Остальные (~10%) затруднились выделить доминирующую платформу или имеют паритет.

Разброс по отраслям значителен. В госсекторе наблюдается наиболее высокая доля отечественных ОС: большинство государственных организаций в выборке уже перешли на сертифицированные национальные дистрибутивы Linux в рамках импортозамещения.

Для сравнения, в промышленности и добывающем секторе пока доминируют устаревшие западные системы – Windows Server, а также *nix-системы, развернутые еще до 2022 года. Переход на альтернативы там идет медленнее из-за консерватизма и критичности промышленных приложений. ИТ/телеком компании и крупные онлайн-сервисы, напротив, чаще других используют серверные Linux-дистрибутивы (чистый Open Source) в качестве базовой ОС для своих сервисов – для них это исторически стандарт де-факто.

Настольные ОС Примечание: Настольные ОС не были основным предметом опроса, информация дана по комментариям участников
Рабочие станции пользователей в большинстве компаний остаются на Windows 10/11. Однако на уровне инфраструктуры (серверы, СХД, сетевое оборудование) роль Linux-ОС чрезвычайно велика. В контексте импортозамещения многие организации рассматривают перевод части рабочих мест на отечественные ОС (Astra Linux, РЕД ОС и др.), но отмечают проблемы совместимости офисного ПО и обучения персонала.

СУБД (системы управления базами данных)

Среди систем управления базами данных проникновение OSS еще выше, чем в случае ОС. Около половины (≈50%) участников опроса отметили преобладание открытых СУБД – прежде всего PostgreSQL, а также MySQL/MariaDB – в своих организациях. Проприетарные СУБД западных вендоров (Oracle Database, Microsoft SQL Server, IBM Db2) все еще занимают существенную долю, но их доминирование снизилось: ~30% респондентов все еще в значительной мере зависят от таких коммерческих СУБД, поддерживая старые установки или постепенно мигрируя. Оставшиеся ~20% используют в основном российские СУБД из реестра (часто форки PostgreSQL с поддержкой – например, Postgres Pro, «Ред База Данных» и др.).

Отраслевые различия. В банковском и финансовом секторе отмечается активная миграция с Oracle на PostgreSQL – многие банки уже перевели ряд систем на открытые СУБД, часто при участии отечественных компаний-партнеров (Postgres Pro и др.) для поддержки. Ритейл и e-commerce также массово внедряют PostgreSQL для новых проектов, ценя его гибкость и отсутствие лицензий. Промышленные предприятия более консервативны: там нередко еще эксплуатируются устаревшие версии Oracle или MS SQL, однако новые проекты запускаются преимущественно на PostgreSQL. В госсекторе заметна ориентация на отечественные СУБД из реестра – в рамках требований импортозамещения выбираются поддерживаемые локальными вендорами продукты (нередко также основанные на PostgreSQL).

В целом, СУБД – одна из категорий, где Open Source стал мейнстримом в российских компаниях.
Это подтверждается и внешними данными: по исследованию ГК В1, 53% компаний используют OSS именно для управления базами данных[5]. PostgreSQL фактически превратился в стандарт для новых систем, благодаря сообществу и накопленному опыту эксплуатации в масштабах enterprise.

Виртуализация

Платформы виртуализации – область, где инерция существующих инсталляций сильна. Более 60% опрошенных все еще в большей степени полагаются на западные коммерческие платформы виртуализации (в первую очередь VMware vSphere, а также Microsoft Hyper-V). Эти решения были массово внедрены в 2010-х годах, и их замена сопряжена с высокими затратами и рисками, поэтому компании продолжают эксплуатировать уже приобретённые лицензии. Особенно характерна такая ситуация для промышленности и финансового сектора, где виртуализированная инфраструктура строилась вокруг VMware и за эти годы сильно обросла экосистемой.

Тем не менее, с 2022–2023 гг. начался переход и на альтернативы. Около 10% организаций указали, что у них уже преобладают Open Source средства виртуализации – такие как KVM (в составе дистрибутивов Linux), Xen, а также комплексные open-source решения вроде Proxmox VE или oVirt. Еще около 30% используют российские системы виртуализации, в том числе из реестра Минцифры (пример – платформа zVirt от компании Orion Soft). Крупные госкорпорации и отдельные телеком-операторы в 2023 г. приступили к опытным проектам по внедрению национальной виртуализации, стремясь к независимости от VMware. В коммерческом же секторе пока преобладает прагматичный подход «не трогай, пока работает» – ресурсы существующих VMware-кластеров будут вырабатываться до конца, параллельно изучаются пути миграции.

Важный аспект: контейнеризация (см. ниже) в ряде случаев позволяет обойтись без расширения традиционной виртуализации. Некоторые компании, особенно ИТ-сектор, фокусируются на контейнерах вместо запуска множества ВМ, что косвенно снижает зависимость от VMware.

Контейнеризация и оркестрация

Технологии контейнеризации – одна из областей, где Open Source доминирует практически повсеместно. Около половины респондентов (≈50%) сообщили, что активно используют контейнерные платформы на базе OSS: Docker для контейнеризации и Kubernetes для оркестрации – напрямую или в составе готовых дистрибутивов. В ИТ-компаниях, у крупных онлайн-сервисов, в ритейле и банках контейнерные кластеры стали стандартом при развертывании приложений. Небольшая доля компаний из этих 50%, менее 15% используют коммерческие продукты на базе OSS, например, ряд банков внедряет Red Hat OpenShift (на базе Kubernetes) для унификации CI/CD и управления микросервисами.

Еще ~30% опрошенных указали, что у них «пока остаются западные решения» или вообще не используется контейнеризация. Вероятно, в этих организациях практика контейнеров еще не развита (что типично для более консервативных отраслей) либо используются проприетарные оркестраторы от ушедших вендоров (например, старые версии VMware Tanzu и пр.). Оставшиеся ~20% респондентов отметили отечественные решения из реестра – это могут быть компании, перешедшие на российские форки Docker/K8s или использующие локальные репозитории и сборки (например, «Контейнерная платформа» от Сбертех и др.).

Общая картина:
контейнеризация – в большей степени охвачена Open Source решениями.

Даже консервативные предприятия, столкнувшись с отсутствием коммерческих альтернатив, вынужденно обратились к открытым технологиям. Фактически, экосистема контейнеров и Kubernetes глобально развивается открытым сообществом, и российские пользователи остаются в этом русле. Отдельные компании упоминают проблемы (см. раздел про риски), связанные с зависимостью от иностранных репозиториев (Docker Hub, Google Container Registry), однако решение видят во внедрении локальных зеркал, а не в отказе от привычных технологий.

Системы резервного копирования

Системы бэкапа и резервного копирования – наименее охваченная Open Source область из рассмотренных. Здесь до недавнего времени доминировали проприетарные продукты (Veeam, Veritas, CommVault и др.), и даже после их ухода переход на альтернативы происходит медленно. Около 50–60% компаний продолжают полагаться на западные системы резервного копирования, зачастую эксплуатируя ранее приобретенные лицензии или старые версии (в случае Veeam – несмотря на прекращение официальной поддержки в РФ).

Около 20% респондентов сумели внедрить Open Source инструменты бэкапа – среди упоминавшихся: Bacula/Bareos, Amanda, UrBackup, RESTic и др. Еще примерно столько же (~20–30%) перешли на отечественные продукты для резервного копирования, представленные в реестре (например, решения Рубэкап, «Кибер Бэкап», а также модули резервирования в составе отечественных ОС и платформ).

Отрасли: в госсекторе и структурах с высокими требованиями ИБ заметен активный переход на российские системы бэкапа – это мотивировано и поддержкой, и соответствием нормативам. Коммерческий сектор более инертен: многие продолжают использовать legacy-системы бэкапирования до исчерпания их ресурса, параллельно тестируя Open Source (часто для второстепенных задач). В целом, резервное копирование остается узким местом: OSS-решений тут меньше, а их функциональность/удобство уступает привычным корпоративным продуктам, поэтому доля Open Source ниже, чем в других слоях инфраструктуры.

Мониторинг и наблюдаемость (observability)

Системы мониторинга — наоборот, область, наиболее полно охваченная Open Source. Более 75% респондентов указали, что у них преобладают открытые инструменты мониторинга. На практике это, как правило, сочетание таких решений как Zabbix (классический инфраструктурный мониторинг), Prometheus/Grafana (метрики и визуализация), системы логирования на базе стеков ELK или Graylog, и др. За последние 5–7 лет эти OSS-инструменты стали стандартом и вытеснили проприетарные аналоги (IBM Tivoli, Microsoft SCOM и т.п.). Хотя респонденты часто отмечают, что это временная мера, открытое ПО сильно уступает по функционалу и возможностям коммерческим западным решениям.

Около 15% компаний используют преимущественно российские решения для мониторинга, часто основанные на Open Source, но коммерчески поддерживаемые. В реестре ПО присутствуют, например, продукты Monq, Gmonit, WiSLA, Пульт, Smart Monitor и др. – их выбирают организации, требующие официальной техподдержки и сертификаций. Оставшиеся ~10% все еще используют старые западные системы, не переведенные на OSS. Но эта доля, по оценкам самих участников, будет снижаться естественным путем: западные продукты не обновляются, и со временем все переходят на открытые или отечественные системы наблюдаемости.

Таким образом, мониторинг – одна из самых «open source-зависимых» областей.

В случае появления дополнительных санкционных барьеров или регуляторных ограничений мониторинг может попасть под угрозу, что приведет к увеличению числа аварий. Этот тренд подтверждается и в других исследованиях: мониторинг и базы данных были первыми направлениями, где компании массово заменили иностранное ПО на открытый или отечественный софт [7].

Инструменты DevOps (CI/CD, IaC, и др.)

Экосистема DevOps-инструментов исторически строилась вокруг Open Source решений, что нашло отражение и в ответах. Около 80% участников сообщили, что в области CI/CD и управлении конфигурациями у них преобладают открытые решения. Самые распространенные: Jenkins (CI-сервер), GitLab CE (репозиторий кода и пайплайны), Nexus/Artifactory OSS (репозитории артефактов), Ansible/Terraform (автоматизация инфраструктуры как кода), Kubernetes (оркестрация, как отмечалось) и др. Многие компании используют комбинированный OSS-стек для полноценных DevOps-процессов – от сборки до мониторинга.

Около 5–10% внедрили отечественные инструменты DevOps. В основном это разработки на базе все того же OSS, но адаптированные под требования клиентов: например, коммерческие форки GitLab (GitLab EE Russian Edition), отечественные аналоги Jenkins (есть решения под эгидой Ростеха) или использование TeamCity с локальной поддержкой. Часть компаний относит к «отечественным» также средства, включенные в отечественные платформы (как часть продуктов Астра, Базальт и др.).

Еще порядка 10% остаются на проприетарных решениях – чаще всего упоминалось продолжение использования Atlassian Bamboo, Microsoft TFS/Azure DevOps Server и подобных систем, которые уже не поддерживаются официально, но продолжают работать внутри контуров компаний. Такие ответы встречались у некоторых предприятий, которые инвестировали значительные средства в эти инструменты ранее.

Напротив, сферы мониторинга, DevOps и контейнеризации оказались наиболее «импортозамещенными» за счет Open Source, поскольку там исторически сильны позиции открытого ПО. Однако возникает нюанс: эти же сферы (контейнеры, CI/CD, мониторинг) наиболее зависимы от глобального OSS-сообщества, т.е. от иностранных репозиториев и обновлений. Эта двоякость проявляется в дальнейшем анализе рисков (раздел 5).

Обобщение по инфраструктуре

Анализ по категориям показывает, что наибольшая зависимость от западного коммерческого ПО сохраняется на уровне базовых платформ – операционных систем, систем виртуализации, резервного копирования.

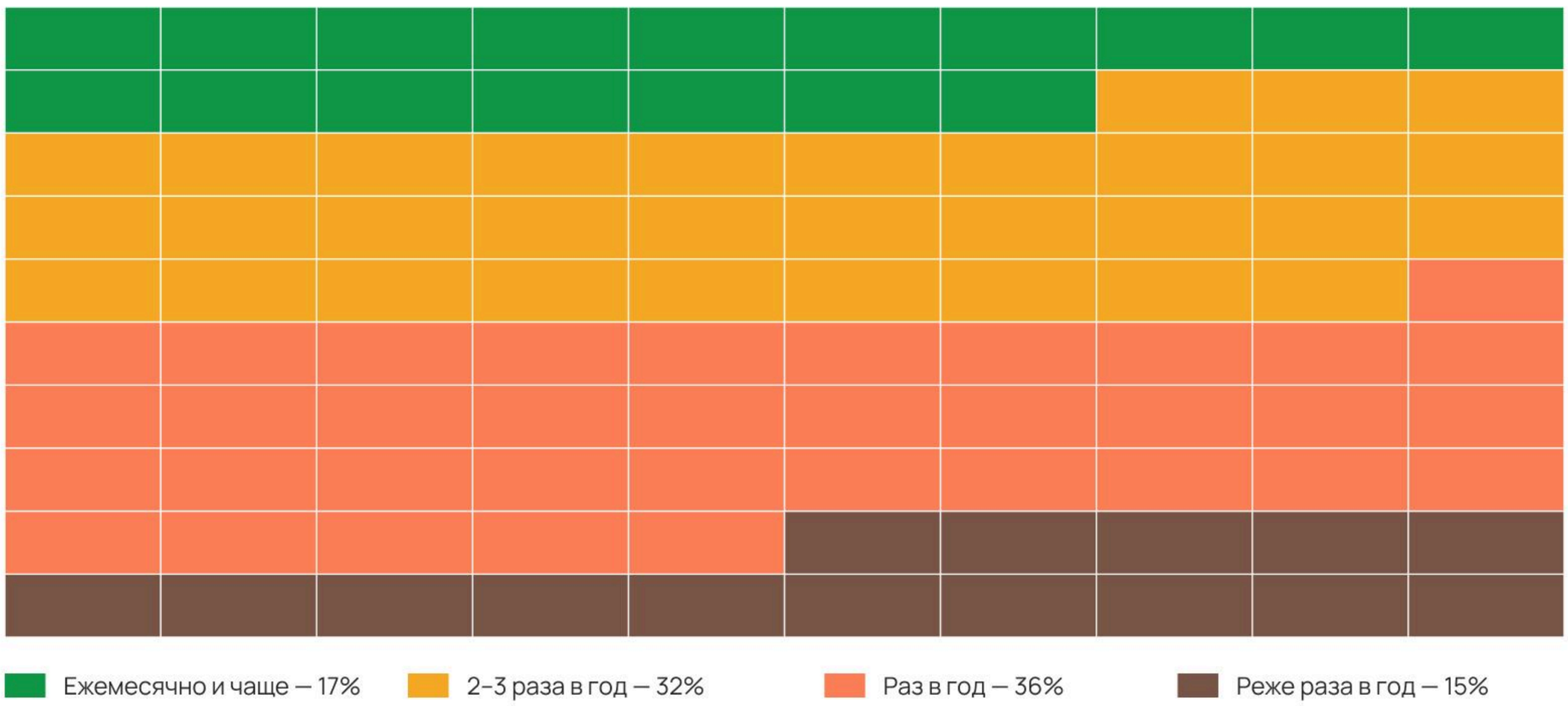
Полученные результаты коррелируют с данными других исследований. Например, по данным группы В1, 77% российских организаций уже используют российское программное обеспечение с открытым исходным кодом, в первую очередь для организации ИТ-инфраструктуры (56% случаев) и управления базами данных (53%)[8]. В крупных компаниях OSS начинает проникать даже в прикладные бизнес-приложения, однако на уровне ОС и платформ замена идет медленнее[5][2].

Практики внедрения, обновлений и модификации Open Source

Помимо факта использования OSS, важно понять как компании его используют: насколько часто обновляют версии, вносят ли изменения в открытый код, имеют ли внутренние форки. Опрос выявил значительные различия в подходах.

Частота обновлений версий

Лишь ≈17% участников практикуют очень частое обновление Open Source-продуктов – вплоть до режима непрерывного обновления, то есть устанавливают новые версии по мере их выхода (не реже раза в месяц). Как правило, это характерно для ИТ-компаний и ведущих онлайн-сервисов, где приняты Agile-методологии и есть выделенные команды для поддержания стека. Еще ~32% обновляются несколько раз в год (условно 2–3 раза в год выходят на актуальные версии). Около 36% придерживаются более консервативного цикла – обновляют OSS-платформы примерно раз в год, после тщательного тестирования. И оставшиеся ~15% признались, что делают апгрейды реже раза в год, фактически лишь при острой необходимости (принцип «работает – не трогай»).



Такая разбивка ожидаема: крупные корпоративные пользователи (особенно промышленность, госсектор) склонны реже обновлять версии, опасаясь нарушить стабильность рабочих систем. Напротив, компании e-commerce, телеком и ИТ-бизнес чаще внедряют обновления оперативно, получая выгоду от новых функций и закрытия уязвимостей.

Отдельно отмечалось, что для критических систем (банковские, промышленные) обновления OSS часто задерживаются, пока сообщество не «обкатает» релиз – организации предпочитают не быть первопроходцами на новых версиях.

Использование «как есть» vs модификации кода

Большинство респондентов – около **65%** – используют Open Source-продукты без существенных доработок, ограничиваясь штатными возможностями и настройкой через конфигурации и плагины. Это означает полагаться на официальные релизы сообществ, получая обновления «из коробки».

В то же время приблизительно **35%** компаний сообщили, что им приходится вносить изменения в исходный код OSS или поддерживать собственные форки проектов под свои нужды. Склонность к самостоятельным доработкам выше у организаций с сильными инженерными командами – например, крупные банки, телеком-операторы, ИТ-компании. Такие компании создают внутренние форки (например, модифицируют PostgreSQL или ELK под высоконагруженные сценарии, дописывают модули безопасности для Linux-дистрибутивов и т.п.) и в некоторых случаях контрибьютят (отправляют изменения обратно сообществу). Малый и средний бизнес, а также большинство госструктур, напротив, стараются использовать OSS «как есть» и опираться на стандартную поддержку сообщества или внешних подрядчиков.

Тем не менее, доля тех, кто модифицирует и дорабатывает Open Source, довольно значительна – более трети. Это свидетельствует о формировании в России собственной экспертизы по ряду ключевых проектов и о желании адаптировать открытое ПО под местные требования (например, интеграция с отечественными ГОСТ-алгоритмами шифрования, локализация на русский язык и др.). В комментариях ИТ-директора отмечали, что наличие исходников дает им уверенность: «если понадобится, сами допишем необходимый функционал».

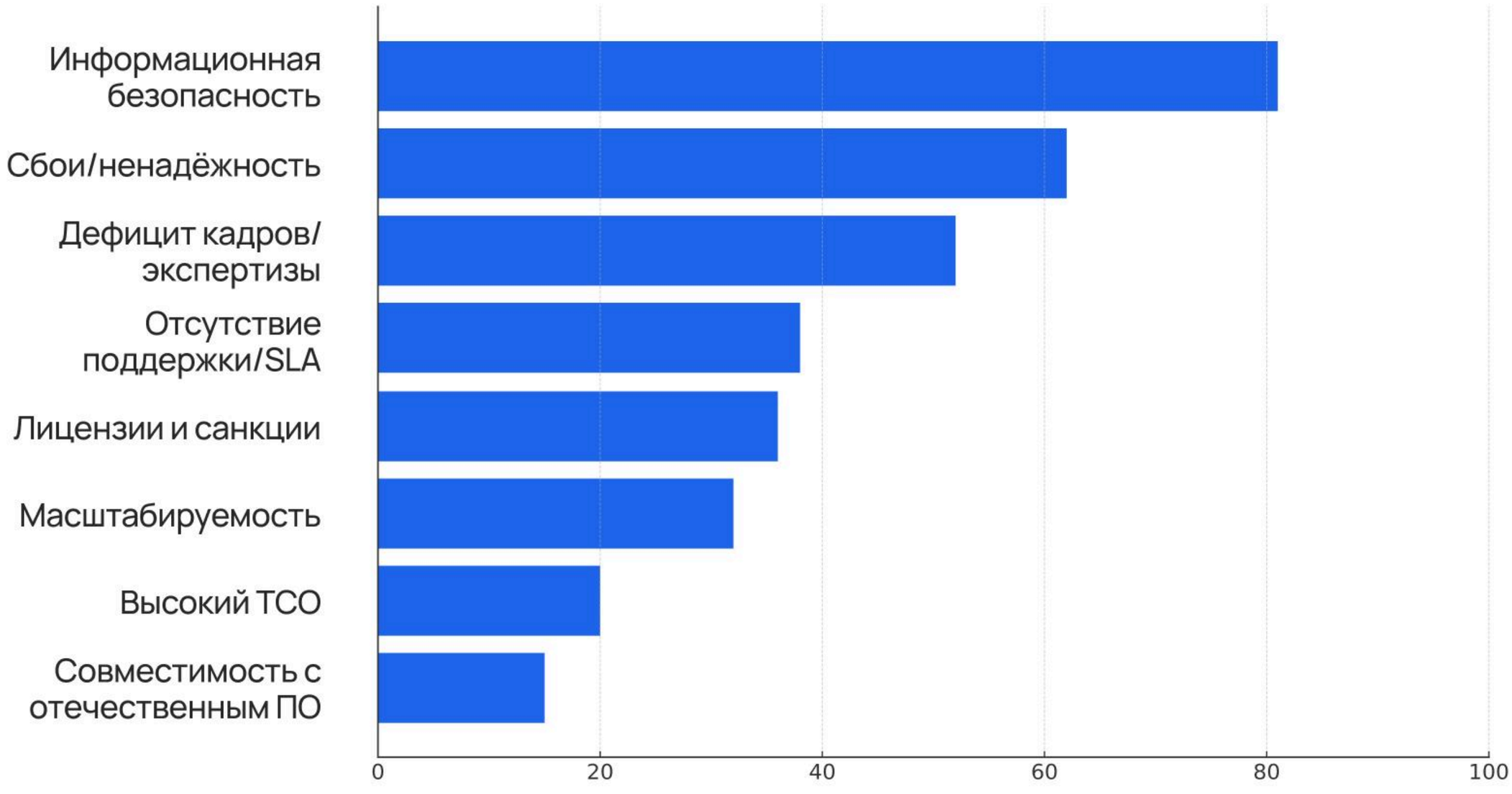
Практики внедрения OSS

Около **58%** респондентов ответили, что перед внедрением Open Source проводят расчет полной стоимости владения (TCO) и сравнение с альтернативами, включая затраты на поддержку, обучение, инфраструктуру и т.д. (см. раздел 6). В крупных компаниях этот показатель выше (до 70%), в малом бизнесе – лишь ~30% системно оценивают TCO, многие действуют интуитивно или исходя только из экономии на лицензиях. То есть примерно в половине случаев выбор OSS оформляется экономическим обоснованием. Те, кто TCO не считает, руководствуются в основном стратегическими или техническими причинами (требования регуляторов, наличие исходников, давление времени).

При внедрении новых OSS-решений практически все компании тестируют их в пилотном контуре, прежде чем переводить на них критичные нагрузки. Среди рекомендаций, которые давали опытные участники, часто упоминались: постепенный переход (поэтапная миграция модулей или филиалов, а не «в омут с головой»), тщательное обучение персонала и наличие плана отката. Эти меры помогают снизить риски при развертывании открытого ПО.

Анализ рисков и инцидентов при использовании Open Source

Несмотря на значительные преимущества OSS, ИТ-руководители осознают и риски, связанные с открытым кодом. В опросе респондентов просили указать ключевые риски использования Open Source. Распределение ответов очертило следующий профиль рисков (каждый участник мог выбрать несколько):



Информационная безопасность

Этот риск вышел на первое место: 81% опрошенных включили безопасность в топ-3 проблем OSS. Опасения связаны с наличием уязвимостей в открытом коде, потенциальных «закладок», а также с зависимостью от зарубежных обновлений и отсутствием гарантированной поддержки. Особенно сильно на ИБ акцентировали внимание представители финансового сектора и госорганов – для них безопасность и соответствие регулятивным требованиям критичны. Отмечалось, что переход на OSS повышает импортонезависимость, но порождает новые вопросы ИБ: нужно научиться самим аудировать код и быстро закрывать уязвимости. Интересно, что среди целей перехода на Open Source безопасность тоже фигурировала у ~52% респондентов (как способ устранить риски закладок в проприетарном ПО) [10], то есть существует двойственность: OSS дают больше контроля, но требуют больше компетенций в ИБ.

Сбои, баги и надежность

На второй позиции – 62% респондентов отметили риск отказов и недостаточной надежности Open Source-систем. Здесь речь о стабильно высокой нагрузке и критичных для бизнеса системах: банки и ритейл упоминали опасения, что базы данных или ОС на OSS могут дать сбой, приводящий к простоям. Хотя многие открытые продукты очень зрелые, всё же ожидания такие, что проверенные проприетарные решения надежнее (связано и с наличием SLA). Отчасти этот страх подпитывают инциденты, которые действительно случались (см. ниже). Для снижения риска компании выстраивают резервирование, кластеры, но психологически риск отказа OSS-систем считается существенным. Многие ИТ-директора понимают, что ожидать идеальной работы от бесплатного ПО невозможно, и баги и сбои – это справедливая цена выбора бесплатного продукта.

Дефицит кадров и экспертизы

Такую проблему включили 52% участников. Многим организациям не хватает специалистов, способных квалифицированно внедрять и поддерживать Open Source, особенно если речь о тонкой настройке или доработке кода. Этот риск чаще подчеркивали промышленность и региональный бизнес, где сложно привлечь опытных DevOps-инженеров или администраторов OSS-систем. В госсекторе тоже отмечают, что дефицит квалифицированных кадров затрудняет переход на открытое ПО: требуется переобучение, смена менталитета ИТ-персонала. Эксперты советуют заранее готовить команды и вкладываться в образование, иначе Open Source может стать «невостребованным» из-за нехватки знаний.

Отсутствие официальной поддержки и SLA

Этот пункт упомянули 38% респондентов. Для банков и крупных предприятий отсутствие гарантированной поддержки вендора является серьезным препятствием: если Open Source-продукт выходит из строя, некому предъявить претензии, всю ответственность несет внутренняя команда. Государственные заказчики, привыкшие к контрактам с техподдержкой, также обеспокоены переходом на модель community поддержки. В комментариях звучало: «в случае критического инцидента виноватым окажется менеджер, выбравший Open Source, потому что нет поставщика, на которого можно переложить ответственность». Часть компаний решает это через контракты со сторонними интеграторами на поддержку OSS, но такие услуги – относительно новая практика и не распространенная.

Лицензионные, правовые и санкционные ограничения

В сумме 36% респондентов включили в топ рисков юридические аспекты. Сюда входят: возможное изменение лицензий самих OSS-проектов (например, переход на лицензии типа SSPL, ужесточающие условия использования), риск санкций против платформ (блокировка GitHub, Docker Hub и др.), а также неясность статуса некоторых открытых лицензий в российской юрисдикции. Финансовый сектор и телеком особенно обеспокоены перспективой, что любимый проект сменит лицензию или что доступ к репозиториям окажется под запретом по внешнеполитическим причинам. Этот риск стимулирует обсуждения о создании локальных зеркал и хранилищ кода (см. стратегические меры в разделе 8).

Трудности масштабирования

Около 32% опрошенных указали, что Open Source-решения могут хуже масштабироваться под рост нагрузки или бизнеса. В частности, e-commerce и телеком обращают внимание: выдержит ли OSS-СУБД резкий рост транзакций? Справится ли система мониторинга с миллионами метрик? У крупных промышленных предприятий есть сомнения, что отдельные открытые проекты «доросли» до уровня Enterprise. Однако объективно многие OSS-продукты доказали свою масштабируемость (Kafka, Kubernetes, Hadoop и др.), поэтому в рейтинге рисков это не самый массовый пункт, но присутствует и его учитывают при архитектурном планировании. Некоторые ИТ-директора, особенно из крупного ритейла и банков отмечали, что опенсорс-решения никогда не смогут заменить высоконагруженный Enterprise решения.

Высокая совокупная стоимость владения (TCO)

Хотя одним из драйверов OSS называется экономия, 20% респондентов видят риск в том, что суммарные затраты на Open Source не ниже, чем на проприетарное ПО, а иногда и выше. ИТ-директора отмечают: расходы на доработку, поддержку своими силами, обучение персонала, интеграцию могут нивелировать выигрыш от отсутствия лицензий[11]. Такой ответ встречался у представителей как промышленности, так и ИТ-бизнеса, хорошо понимающих стоимость жизненного цикла ПО. Тем не менее, большинство участников (62%) считают TCO скорее преимуществом OSS (см. раздел 6), поэтому риск высокого TCO не вошел в топ-5. Но для некоторых компаний неоправданный рост внутренних затрат на поддержание OSS – реальная проблема.

Совместимость с отечественным ПО

Лишь 15% отметили этот риск в области инфраструктурного ПО, то есть он оказался на последнем месте. Суть его: некоторые респонденты (преимущественно госструктуры) обеспокоены, что отдельные OSS-продукты трудно интегрировать с отечественными системами или они не проходят необходимые сертификации. Примеры: интеграция Linux-систем с российскими крипто-средствами (ГОСТ SSL/TLS), поддержка национальных шифров, соответствие приказам регуляторов – это точечные вопросы, но не массовая проблема. Более серьезной интеграционной трудностью называют в целом стыковку OSS с унаследованными корпоративными системами (Галактика, 1С и др.), однако это уже общая технологическая сложность, не специфичная для открытого ПО. Интересно, что исследование B1 также показало: интеграция с существующими системами – самый частый вызов при внедрении OSS (39% отметили), наряду с проблемами настройки (30%) и нехваткой функционала (29%)[12][13].

Иные риски

Практически никто из опрошенных не добавил других рисков помимо перечисленных выше. В единичных комментариях упоминалось: недостаток документации на русском языке; сложность аудита открытого кода (для чего нужны эксперты). Но эти моменты коррелируют с уже названными проблемами (дефицит компетенций, поддержка). Таким образом, список рисков достаточно полно охватывает основные опасения.

Общий профиль рисков

Безопасность, надежность и кадры – универсальные волнения во всех отраслях; банки и госорганизации дополнительно акцентируют юридические вопросы и поддержку; коммерческий бизнес (ритейл, производство) фокусируется на надежности и окупаемости; ИТ-компании – на дефиците талантов и возможных лицензионных изменениях.

Несмотря на перечисленные риски, большинство компаний продолжают расширять использование Open Source, параллельно вырабатывая меры по снижению угроз (см. рекомендации в разделе 10).

Инциденты, связанные с OSS

Респондентов также спросили: сталкивались ли они с серьезными инцидентами из-за Open Source. Около **32%** (38 из ~120 ответивших на этот вопрос) указали, что да, были значимые инциденты. Примеры, которые они привели:

Инцидент с Zabbix в крупном ритейле

«Во внутренней сети у нас был развёрнут Zabbix без строгой политики обновлений. В результате в продакшене осталась версия с известной уязвимостью в модуле веб-интерфейса. Через этот вектор злоумышленники получили доступ к серверу мониторинга, а оттуда — в сегмент внутренней сети. В итоге произошла масштабная перегрузка сетевого оборудования и частичная остановка работы кассовых узлов в более чем 200 магазинах. Выяснилось, что регулярный аудит безопасности open source-инструментов у нас не был формализован, и это стало ключевой причиной инцидента.»

Уязвимости в библиотеках и компонентах

Многие упоминали случаи, когда обнаружение критической уязвимости в используемом открытом компоненте требовало внепланового обновления и экстренного патча. В частности, несколько ответов косвенно сослались на известный инцидент Log4Shell в декабре 2021 г. (уязвимость в библиотеке Log4j) – этот случай заставил многие компании срочно обновлять компоненты по безопасности. Подобные ситуации воспринимаются как серьезный риск, но и как часть жизни с OSS: «Да, пришлось срочно обновиться, но вендорского ПО это тоже касается».

Сбои после обновлений

Ряд компаний испытали технические проблемы при обновлении Open Source-продуктов. Например, комментарий: «обновление open source компонента вызвало падение части системы, откатывались назад». Такое случается, если новое версия оказалась несовместима или содержала баг. Без контрактной поддержки устранение проблемы ложится на собственную команду, что усложняет ситуацию. Тем не менее, подобные инциденты респонденты называли неприятными, но преодолимыми.

Санкционные ограничения доступа

Некоторые участники столкнулись с проблемами из-за блокировки зарубежных ресурсов. Самый яркий пример – временная блокировка Docker Hub весной 2022 г. (речь о введенных ограничениях доступа для российских IP). Один из респондентов указал: «ограничение доступа к Docker Hub привело к сбоям в процессах CI». Другие упоминали необходимость срочно настраивать зеркала репозиториев (Maven, PyPI), когда облачные сервисы ввели ограничения. Эти инциденты стимулировали компании заблаговременно создавать локальные копии важных репозиториев.

В целом, из тех ~32% участников, кто заявил о наличии инцидентов, около трети привели подробности — и большинство описанных случаев напрямую касалось проблем безопасности (уязвимости в компонентах) и доступности инфраструктуры OSS (срывы обновлений, недоступность репозиториев). При этом тот факт, что ≈68% организаций не фиксировали серьёзных сбоев, не должен вводить в заблуждение: в отличие от проприетарного ПО с контрактной поддержкой, где вендор несёт репутационные и финансовые риски, открытые проекты зачастую не имеют ответственного центра, который гарантированно закроет уязвимость или предотвратит её появление.

ИТ-директора, утверждавшие, что «критичных сбоев по вине Open Source не было», в ряде случаев опираются на удачное стечение обстоятельств или изолированные сценарии применения, а не на гарантии качества. Вендорское ПО, за которым стоят компании с брендом, репутацией и SLA, вынуждено следить за безопасностью гораздо жёстче — именно потому, что на кону доверие рынка и будущее продукта. В экосистеме же open source ответственность распределена между тысячами добровольцев и интеграторов, что неизбежно создаёт «разрывы» в безопасности и реагировании. Даже зрелые проекты вроде Linux, PostgreSQL или Kubernetes уязвимы к человеческому фактору, задержкам в выпуске патчей и рискам цепочки зависимостей, а отсутствие централизованного контроля делает такие инциденты потенциально более опасными для бизнеса.

Экономические аспекты и преимущества Open Source (TCO-анализ)

Несмотря на перечисленные риски, практически все опрошенные видят значимые выгоды в использовании Open Source. Вопрос об основных преимуществах OSS выявил следующую топ-5 мотиваций (респонденты могли отметить несколько):

Гибкость и возможность кастомизации

Самый популярный ответ – отмечен 66% респондентов. Возможность дополнять и изменять код под свои нужды, отсутствие жесткой привязки к функциональному roadmap'у вендора – одно из главных преимуществ OSS. Особенно это ценится в ритейле/e-commerce и среди ИТ-компаний, где умение быстро доработать продукт под специфические бизнес-требования дает конкурентное преимущество. Многие прямо указали: «гибкость решений, возможность кастомизировать под процессы компании» как ключевой плюс. Внешние данные подтверждают значимость этого фактора – около 39% компаний переходят на Open Source именно ради возможности доработок[10]. OSS предоставляет свободу творчества, тогда как закрытый софт ограничен видением производителя.

Отсутствие привязки к вендору (vendor lock)

На втором месте – 64% респондентов. Для российского бизнеса после 2022 г. критично избежать зависимости от единственного поставщика, особенно иностранного. Open Source дает уверенность, что продукт не исчезнет с рынка неожиданно: даже если оригинальный разработчик прекратит поддержку, исходный код доступен и может быть продолжен сообществом или усилиями самой компании. Это напрямую связано с понятием технологической независимости. Госсектор и финансовые организации особо подчеркнули этот аспект – открытое ПО рассматривается как элемент обеспечения суверенитета ИТ-инфраструктуры. Исследование B1 также показало, что 83% компаний теперь используют или планируют использовать OSS именно в контексте импортозамещения и снижения зависимости от зарубежных вендоров[14][2].

Низкая совокупная стоимость владения (TCO)

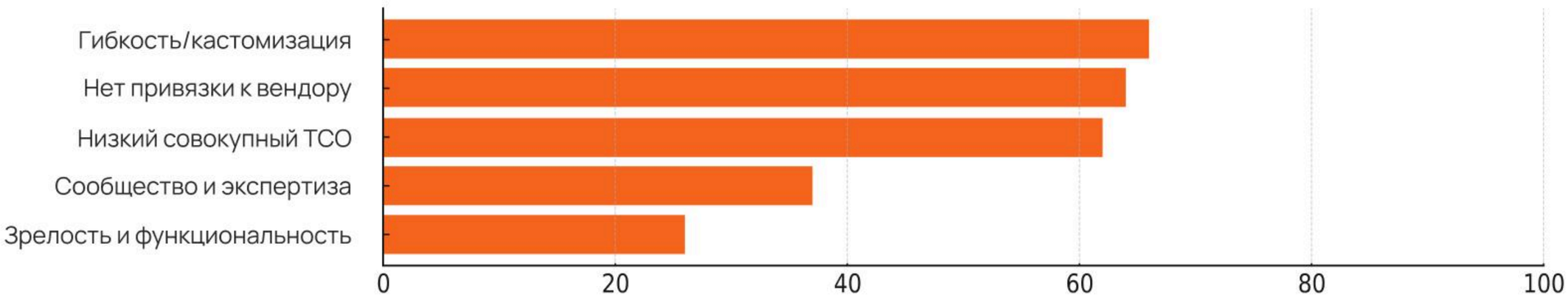
На третьем месте – 62% отметили экономическую выгоду OSS. Хотя, как обсуждалось, некоторые видят риск роста TCO, все же вдвое больше руководителей считают Open Source более выгодным экономически. Отсутствие затрат на лицензии, свобода масштабирования без удорожания, возможность перераспределять бюджет на своих разработчиков вместо оплаты зарубежного ПО – эти факторы особенно ценятся в промышленности и финансовом секторе. Ранее значительная часть их ИТ-бюджетов уходила на лицензии Oracle, Microsoft и др., теперь эти средства можно вкладывать во внутренние проекты. Многие организации называют экономию одной из целей перехода на OSS, и результаты опроса полностью подтверждают эту мотивацию[15]. Отметим, по оценке компании Sirius, использование OSS и его поддержка могут быть на 10–15% дешевле проприетарных решений[16][17], а иногда экономия гораздо выше, если учесть курс валют и рост цен на иностранные продукты.

Широкое сообщество и доступность экспертизы

Этот пункт выбрали 37% респондентов. Большое сообщество пользователей и разработчиков OSS обеспечивает прозрачность кода, быстрое нахождение и исправление ошибок, обилие документации и примеров, а также наличие специалистов на рынке труда. Особенно ценят это ИТ/телеком компании и средний бизнес, у которых может не быть ресурсов на платную поддержку – они полагаются на коммьюнити и открытые знания. Для популярных OSS-систем легко найти ответы на форумах, нанять сотрудника с опытом – зачастую проще, чем искать эксперта по редкому проприетарному ПО. Некоторые упоминали: «прозрачность кода и доверие» – мол, открытый код можно проверить на уязвимости; другие – «легкость найма специалистов, знающих Linux/Postgres и т.д.».

Зрелость и функциональность продуктов

Примерно 26% включили в топ преимуществ то, что современные Open Source-продукты весьма функциональны и зрелы. Действительно, многие OSS-системы развиваются десятилетиями и достигли уровня enterprise-функциональности (Linux, PostgreSQL, Kubernetes, Apache Kafka и др.). Для ряда задач они стали мировым стандартом де-факто. Банки и телеком-компании, выбирая OSS, исходят из того, что продукт проверен глобальным сообществом и имеет сопоставимый (а иногда более широкий) набор функций по сравнению с проприетарными аналогами. Однако в суммарном рейтинге этот пункт занял лишь пятое место – вероятно потому, что не для всех сегментов открытые решения достаточно зрелые.



Другие преимущества

Немногие респонденты (менее 5%) указали что-то вне основных категорий. В отдельных ответах в опции «Другое» упоминались, к примеру: открытость кода как гарантия доверия (возможность независимого аудита безопасности), свобода в выборе инфраструктуры, отсутствие принудительных обновлений. Пара скептически настроенных участников написали, что «не видят особых преимуществ» – такие мнения были исключением, предположительно от компаний, которые вынужденно используют OSS по санкционным причинам, но пока не ощутили плюсов.

Расчет полной стоимости владения (TCO)

Как отмечалось, ~58% компаний в той или иной мере оценивают TCO OSS vs проприетарного ПО при принятии решений[18]. Тем самым они стараются учесть не только экономию на лицензиях, но и все сопутствующие расходы. Для таких оценок зачастую используются внутренние методики, которые включают: стоимость поддержки (внешней или внутренней), требования к инфраструктуре (например, большее число серверов для OSS или наоборот), затраты на обучение сотрудников, потенциальные простои и риски. Примечательный результат опроса: в малом бизнесе лишь ~30% считают TCO перед внедрением OSS – часто там решают «на глаз» или исходя из прямых затрат. В крупных компаниях ~70% обязательно считают экономику, прежде чем утвердить миграцию. То есть зрелость практик управления расходами сильно варьируется по масштабу компаний

В целом, большинство участников считает, что Open Source приносит экономию. Даже если формально TCO иногда сравним с проприетарным ПО (из-за стоимости специалистов), OSS дает более контролируемую структуру затрат: компания платит зарплаты своим инженерам, развивая компетенции, вместо выплаты лицензий внешнему вендору. В условиях, когда бюджеты на ИТ оптимизируются, такой подход воспринимается положительно.

Барьеры и ограничения перехода на отечественные альтернативы

Одной из важных задач исследования было понять, что мешает организациям отказаться от Open Source в пользу отечественного проприетарного ПО, если рассматривать такую альтернативу. Иными словами, почему, несмотря на курс на импортозамещение, бизнес продолжает широко использовать OSS, а не полностью мигрирует на продукты российских разработчиков? Респондентам предложили отметить причины, препятствующие переходу на отечественные аналоги. Абсолютное большинство выбрало сразу несколько факторов. Топ-3 барьеров выглядят следующим образом:

Незрелость отечественных продуктов – 88%

Практически все ИТ-директора согласны, что российское ПО пока недостаточно отлажено и зрелое. Этот ответ давали представители и бизнеса, и госорганизаций. Комментарии: отечественные аналоги западных систем появились совсем недавно, у них меньше функционала, они хуже протестированы в боевых условиях. Даже если заявлен базовый функционал, ему не хватает полировки и стабильности. По сути, «сырость» отечественных решений – главный барьер на пути отказа от OSS в пользу национального софта. В исследовании B1 схожий вывод: при переходе на OSS 67% компаний не смогли полностью достичь целей, часто из-за проблем с подготовкой персонала, интеграцией и ИБ – что отчасти тоже указывает на незрелость окружения и решений[19][20]. Таким образом, пока российские продукты не достигнут сопоставимого уровня надежности, Open Source будет предпочтительным вариантом.

Отсутствие нужного функционала – 82%

Вторым по значимости фактором стало отставание российских продуктов по функциональности. 82% респондентов отметили, что отечественные аналоги зачастую уступают и Open Source, и ушедшим западным решениям по возможностям. Например, системы виртуализации, мониторинга, DevOps-инструменты – ИТ-директора жалуются, что им не хватает привычных функций, интерфейсов, интеграций. Даже при желании перейти, им «нечем заменить без потери возможностей». Особенно это подчеркивали промышленность и ритейл – там много узкоспециализированных ИТ-систем, у которых нет российских аналогов (или они в зачаточном состоянии). В банковской сфере также ряд критичных систем пока не имеют функционально равного отечественного решения, поэтому банки либо остаются на OSS-платформах, либо продолжают эксплуатировать старые иностранные версии, ожидая появления нужного функционала в РФ.

Высокие цены на лицензии отечественного ПО – 74%

Третьим крупным барьером стало ценовое несоответствие: ~74% респондентов считают стоимость российских продуктов неоправданно высокой. Это звучит парадоксально – казалось бы, отечественные решения должны стать доступной альтернативой. Но рынок диктует свое: со снижением конкуренции некоторые вендоры подняли цены, заложили дорогую поддержку. В итоге владение отечественным ПО нередко обходится дороже, чем связка Open Source + свои ресурсы[21]. Такой ответ особенно характерен для среднего бизнеса, которому не по карману лицензии крупных отечественных систем (назывались группы Astra, Naumen, решения «Ростелекома» и др.). Банки и госкорпорации тоже соглашаются: бюджеты не безграничны, а цены продуктов из реестра иногда сопоставимы с прежними ценами мировых лидеров, хотя часто и ниже их. Большинство участников опроса отмечают, что предпочитают OSS во многом именно по экономическим соображениям, и если отечественный софт не дает ощутимой экономии, смысла мигрировать на него нет.

Следующими по значимости барьерами (их тоже отметили многие, хотя и не большинство) стали:

Низкое качество послепродажного сервиса – 50%

Половина респондентов указывает, что поддержка у отечественных вендоров пока хромает. Не хватает компетенции, реагирование на инциденты медленное, команды поддержки маленькие и перегружены. Бизнес опасается, что купив отечественный продукт, он не получит должного уровня сервисного сопровождения. Это особенно важно для банков и крупных предприятий – они привыкли к SLA от IBM, Oracle и т.д., а молодые российские компании не всегда могут обеспечить такой же уровень. В результате доверие к качеству поддержки низкое, и OSS с self-support или поддержкой от сообществ иногда выглядит не хуже.

Трудности внедрения и миграции – 34%

Примерно треть (34%) отмечает, что переход на отечественное ПО трудоемок: требует переобучения персонала, переделки интеграций, изменений бизнес-процессов. Многие уже прошли болезненный опыт замены одного ПО на другое в 2022 году и не хотят снова переживать подобный стресс при переходе с OSS на что-то еще. Органы власти спускают распоряжения «перейти на отечественное», но на практике организации не хотят быть полигоном для обкатки сырых систем. Проще продолжать использовать OSS, которое уже настроено, чем тратить ресурсы на сомнительную миграцию на новый отечественный аналог с неопределенным исходом.

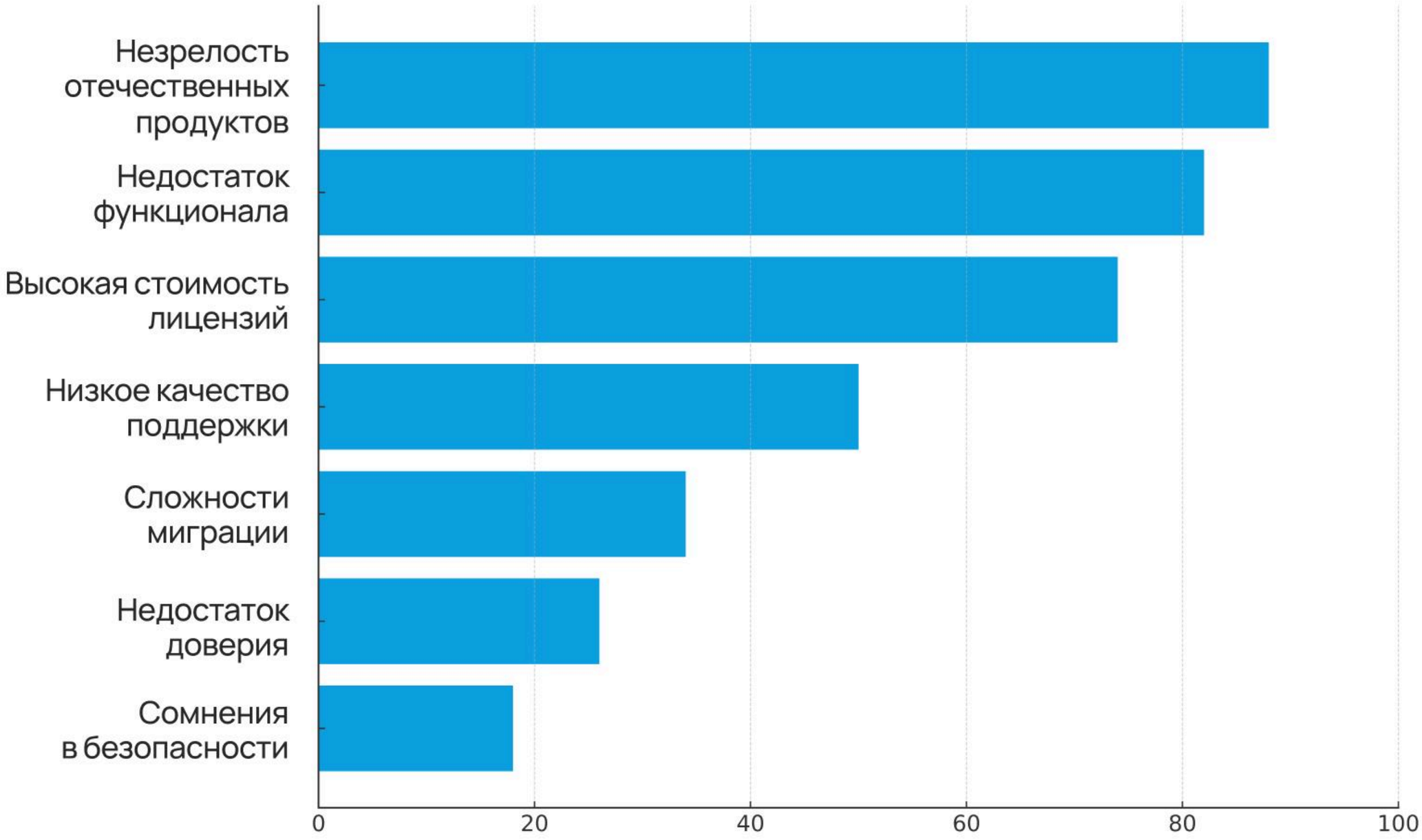
Недостаток доверия к отечественным вендорам – 26%

Четверть респондентов упомянули и фактор доверия. Здесь речь не столько о политическом доверии, сколько об уверенности в стабильности самого вендора. Бизнес опасается, что разработчик российского ПО может закрыться через год, не суметь масштабировать продукт или бросить его. Есть память о случаях, когда отечественные проекты сворачивались, не достигнув зрелости. Этот скепсис более присущ частному сектору. Госсектор, напротив, зачастую доверяет «своим» вендорам по умолчанию, зная, что их поддержит государство. А вот частные компании предпочитают надежность: Open Source с большим международным комьюнити зачастую вызывает больше уверенности, чем продукт небольшой российской фирмы с неопределенными перспективами.

Безопасность отечественных решений – 18%

Почти незначимый в общем количестве, но все же отмеченный 18% пункт: недоверие к защищенности российского ПО. Парадоксально, но даже в условиях импортозамещения некоторые специалисты по ИБ больше доверяют мировому Open Source (проверенному тысячами глаз), чем закрытому коду новых отечественных программ. Кроме того, из-за спешки разработки в 2022–23 годах некоторые отечественные продукты могли выйти сырыми, не прошедшими полноценного аудита безопасности. Этот аспект всплывал у представителей банков, для которых информационная безопасность – краеугольный камень. Хотя в общем списке факторов он оказался на последнем месте, для критичных организаций он играет роль: они опасаются, что новое российское ПО может содержать неизвестные уязвимости, тогда как в популярном OSS многие уязвимости уже выявлены и закрыты.

Итог анализа показывает, что значительная часть барьеров к переходу на отечественные решения основана не столько на личном опыте компаний, сколько на сложившихся в отрасли установках и восприятии. Многие ИТ-директора признавались, что сами не проводили полноценных пилотов российских продуктов, а опирались на мнение коллег, рыночные слухи и публичные кейсы — зачастую единичные и не всегда репрезентативные. Фактически, в ряде случаев OSS выбирают «по инерции», потому что он уже внедрён и считается технологически проверенным, тогда как отечественное ПО воспринимается «по умолчанию» как более слабое, без попытки его объективной оценки



Это указывает на серьёзную проблему маркетинга российских вендоров: при ограниченных ресурсах они не в состоянии проводить агрессивные кампании по продвижению, масштабные пилотные внедрения и PR-программы, которые десятилетиями использовали западные enterprise-вендоры для завоевания доверия клиентов. У западных конкурентов бюджеты на продвижение, развитие партнёрских сетей и работу с лидерами мнений исчислялись сотнями миллионов долларов в год — российские игроки в таких условиях изначально находятся в уязвимом положении.

Чтобы переломить ситуацию, отечественным вендорам нужна не только господдержка, но и активная вовлечённость заказчиков: тестирование продуктов на реальных сценариях, готовность делиться обратной связью, помощь в формировании дорожных карт и публичная поддержка успешных кейсов. Без такой совместной работы «разрыв доверия» между рынком и российским ПО будет сохраняться, а open source — оставаться предпочтительным выбором просто потому, что он уже знаком и принят.

Прогноз на 3 года и стратегические сценарии

Открытое ПО в России сейчас – вынужденная, но во многом успешная мера, и важно понять, останется ли оно столь же значимым через несколько лет. В рамках исследования респонденты дали оценку, какую долю инфраструктурного ПО (в процентном соотношении) будут занимать Open Source-решения через 3 года. Также обсуждались стратегические сценарии – например, как компании поступят в случае ужесточения регулирования OSS.

Open Source: временное решение или долгосрочная стратегия?

Мнения ИТ-директоров разделились относительно того, является ли использование OSS лишь временной мерой (на период, пока не появятся зрелые отечественные аналоги), либо же Open Source останется частью долгосрочной стратегии ИТ-развития компаний.

Большая часть опрошенных – около 60% – склоняется к тому, что Open Source для них скорее временное решение, а не постоянная стратегия. Особенно единодушны в этом представители крупного бизнеса и государственного сектора. В госструктурах открыто говорят, что OSS используется на переходный период, пока не появятся полностью готовые отечественные продукты, после чего планируется вернуться к «своему» ПО. Некоторые банки также стратегически рассчитывают со временем мигрировать на отечественные платформы (например, ждут российских систем резервного копирования, виртуализации, СУБД, мониторинга и т.д., чтобы заменить ими Open Source).

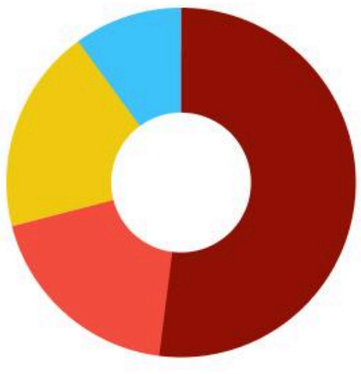
Однако значимая доля – порядка 40% – напротив, не рассматривают Open Source как временную затычку. Эти респонденты (преимущественно представители ИТ-компаний, телеком, e-commerce, а также часть промышленников) заявляют, что намерены продолжать развивать OSS-стек и через 3, и через 5 лет. Они считают открытое ПО частью своей постоянной ИТ-стратегии и не планируют отказываться от него, даже если на рынке стабилизируется предложение отечественных продуктов. В пользу этого говорят успехи OSS, независимость и возможность самим влиять на код. Как отметил один из участников: «Мы строим ИТ на Open Source не потому что больше ничего нет, а потому что это дает нам гибкость. Если появится российский аналог, который превзойдет по качеству – посмотрим, но просто ради галочки переходить не будем».

Таким образом, рынок находится в некотором подвешенном состоянии ожидания: многие готовы при первой возможности перейти на отечественное ПО, если оно догонит по качеству, но пока этого не произошло – выбирают Open Source и закладываются на него как на основу. Можно сказать, что OSS сейчас – это стратегический компромисс, и его роль в будущем зависит от развития российского ПО. Никто из опрошенных не ожидает, что Open Source вытеснит полностью все решения или, наоборот, что через 3–5 лет все поголовно перейдут на закрытое отечественное ПО. Вероятнее всего, нас ждет гибридная модель: сосуществование отечественных разработок и OSS-платформ, где доля того или иного будет зависеть от конкретной области и успехов вендоров.

Временное решение	Долгосрочное решение

Гипотетический запрет иностранного Open Source: влияние и действия

Особый сценарий, который был рассмотрен в опросе, – это гипотетический полный запрет использования иностранного OSS. Подразумевается ситуация, когда регуляторными или санкционными мерами компаниям в РФ запретили бы пользоваться ПО из глобальных репозиториев (GitHub, Docker Hub и т.д.), разрешив только проверенный «отечественный» открытый код. Мы подчеркнем, что это во многом умозрительный сценарий, но его вероятность обсуждается (например, звучали идеи обязать использовать только OSS с проверенным кодом или в крайнем случае – ответные санкции Запада, отключающие доступ к репозиториям).



Результаты: большинство (≈70%) компаний оценивают такой шаг как крайне негативный для своих ИТ-процессов. Конкретнее, **52%** респондентов считают, что запрет на иностранный OSS значительно ударит по их инфраструктуре, приведет к сбоям и усложнению сопровождения. Еще **19%** – оценивают такой сценарий как критичный, ставящий бизнес под угрозу (то есть «почти катастрофа»). Итого 71% воспринимают потерю глобального OSS как существенный или фатальный удар.

Эти компании поясняют: запрет кода из GitHub/Docker Hub приведет к разрыву устоявшихся процессов разработки и обновления. Многие называют влияние «очень серьезным» – придется кардинально перестраивать пайплайны поставки ПО, переводить все на локальные форки. Особенно остро это для коммерческих компаний, глубоко зависящих от мирового OSS (банки, онлайн-сервисы, разработчики ПО). Например, отмечалось, что CI/CD и DevOps-инфраструктура сильно завязана на Ansible, Terraform, GitLab, Jenkins – уход которых без аналогов парализует конвейеры сборки кода[23]. Также назывались средства контейнеризации (Docker, Kubernetes): без них e-commerce и крупному бизнесу будет крайне тяжело быстро выпускать приложения[23].

С другой стороны, около **19%** полагают, что запрет отразится незначительно на их работе, и еще **≈10–11%** (по данным опроса ~18% выборки) заявили, что вообще не почувствуют влияния такого запрета. Кто эти оптимисты? В основном, это представители госорганов и компаний, уже сделавших ставку на локальные репозитории и отечественные форки. Некоторые госИТ-директора утверждают, что у них весь необходимый код уже хранится внутри страны, зависимости зеркалированы, и внешние репозитории им не нужны. Часть индустриальных предприятий с относительно статичной ИТ-средой (где ПО давно не обновлялось) тоже уверены, что заморозка новых зарубежных исходников не повредит их работе. Однако таких ответов меньшинство – повторимся, около 1/5 выборки.

> Итого, ~70% отрасли зависит от глобального OSS, и его внезапная потеря вызвала бы тяжелые последствия[24]. Это важный вывод в контексте госрегулирования: слишком резкие ограничения могут действительно «отключить кислород» значительной части ИТ-ландшафта страны.

План действий на случай запрета OSS респонденты видят достаточно ясно. 76% (три четверти) ответили, что в таком случае будут переходить на локальные форки и зеркала Open Source. Проще говоря – развернут собственные репозитории кода внутри страны, форкнут важные проекты и продолжат их развитие самостоятельно или силами сообщества. Этот шаг назвали практически все представители ИТ-бизнеса, телекома, крупные банки – у многих уже идет работа по созданию внутренних GitHub-зеркал, кэш-прокси для Docker Registry и т.п.[25]. Крупные компании заранее архивируют исходники критически важных библиотек, чтобы иметь копию. Такой курс на технологическую автономность – очевидный выбор для тех, кто не собирается отказываться от OSS даже под давлением. Фактически, они готовы превратить глобальный Open Source в национальный (форкнут и жить в локальном контуре).

14% респондентов выбрали вариант «все из перечисленного», что подразумевает комплекс мер: и локальные форки, и ускоренный переход на отечественные аналоги, и изменение архитектуры систем. Этот вариант чаще отмечали представители госсектора[26]. Вероятно, они понимают, что по распоряжению «сверху» им придется делать все сразу: и форкать, и замещать, и переписывать, не считаясь с издержками. Такой подход характерен для организаций с государственным управлением, где могут одновременно развивать несколько направлений во исполнение указаний.

Интересно, что лишь около 10% (каждый десятый) признались, что не будут предпринимать ничего из перечисленного в случае запрета. Что скрывается за этой позицией? Некоторые уточняли в комментариях: просто перестанут обновлять ПО, заморозят используемые версии и продолжат работать на них «пока можно». Другие, вероятно, пока сами не понимают, что делать, или надеются, что до полного запрета не дойдет. В любом случае, полное бездействие – редкость. Подавляющее большинство имеет хотя бы базовый проактивный план на случай ухудшения ситуации: локализация открытого кода, создание резервных репозиториев – главный ответ российского ИТ-сообщества на угрозу внешней блокировки.

Прогноз доли Open Source через 3 года

Как отмечалось, средний прогноз респондентов относительно доли OSS через 3 года составил ≈45% инфраструктурного ПО. Однако разброс мнений очень велик, что отражает разную стратегию компаний:

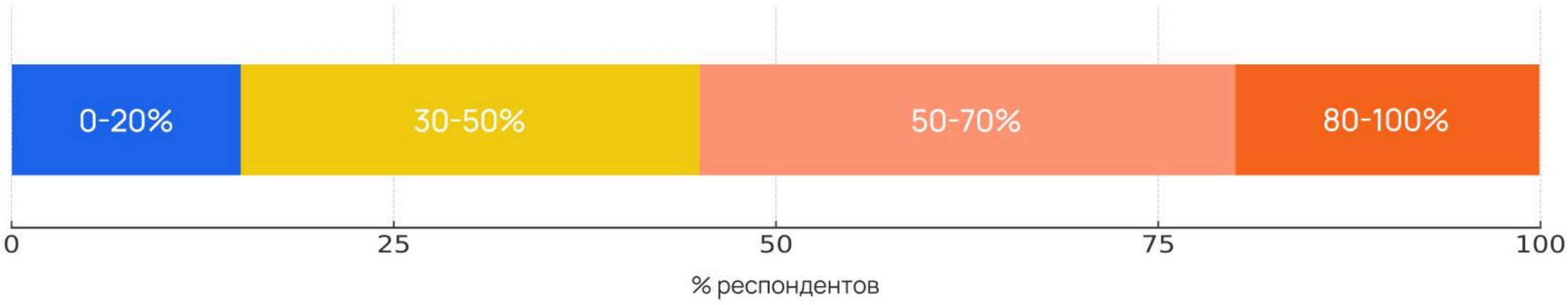
Около 15% (в основном госорганизации) дали крайне низкие прогнозы: 0–20% OSS в инфраструктуре через 3 года. Некоторые ответы из госструктур даже звучали «0%» или «10%», т.е. предполагается почти полное вытеснение Open Source отечественным ПО. Это, по сути, отражает официальную позицию: государственный сектор рассчитывает минимизировать долю иностранного OSS, заменив его национальными платформами (возможно, закрытыми). Эти респонденты, очевидно, относятся к тем 60%, кто считает Open Source временной мерой.

Около 30% прогнозируют умеренный результат: 30–50% OSS. Это самый популярный диапазон – многие верят, что OSS займет существенную, но не доминирующую долю. Часто встречался ответ «50%». Такой подход свойствен финансовому сектору и промышленности – они ожидают, что через несколько лет примерно половина инфраструктуры останется на Open Source, а половина будет на отечественном ПО. Вероятно, предполагается сосуществование: где-то получится внедрить российское ПО (особенно там, где есть зрелые продукты – офисные приложения, ECM, некоторые платформы), а где-то все равно будет OSS (например, базы данных, системы контейнеризации и DevOps-инструменты).

Около 5% самых смелых прогнозов дали 80–100% OSS. Несколько ответов было «80%», и один респондент (представитель ИТ-бизнеса) указал даже «100% open source». Эти мнения отражают уверенность, что почти весь инфраструктурный софт станет открытым. Вероятно, речь о компаниях, которые уже сейчас на 70–80% используют OSS и не видят причин возвращаться к закрытым моделям. Примечательно, что даже энтузиасты редко верят в полные 100% — видимо, понимают, что какая-то доля специфических решений все же останется проприетарной (например, собственные разработки или строго регламентированные системы).

Если усреднить прогнозы и разбить по сегментам, получается ожидаемое распределение: госсектор ждет минимальную долю Open Source (в среднем прогноз всего ~13%, то есть практически свести к нулю OSS в будущем). Промышленные предприятия и силовые организации также довольно сдержанны (~30–35%). Финансовый сектор прогнозирует около 40% (менее половины). А вот ритейл и особенно ИТ/телеком ожидают высокую долю: у ритейлеров средний прогноз ~54%, у технологических компаний – 60% и выше. То есть, чем более технологична и конкурентна отрасль, тем больше верят в OSS.

Для сопоставления: на мировом уровне Open Source уже сегодня занимает значительную долю. По оценкам, объем глобального рынка услуг, связанного с OSS, вырастет с $25,6 млрд в 2022 до $50–54 млрд к 2027 году[29], что подразумевает высокий темп роста (CAGR ~16%). Российские эксперты также дают позитивные прогнозы: ожидается рост отечественного рынка OSS до ~250 млрд руб. в ближайшие годы[30][28] (возможно, к 2030 г.). Наш опрос подтверждает общее мнение сообщества: доля Open Source в ИТ будет расти или как минимум сохраняться на высоком уровне. Никто не предрекает возвращения к статус-кво 2010-х с тотальным господством проприетарного ПО. Скорее всего, мы увидим окончательное формирование двухкомпонентной модели: национальные разработчики закроют критичные ниши, а OSS останется фундаментом для большого числа задач.



Комментарии и оценки IT-лидеров: взгляд на Open Source от экспертов рынка

Для качественного обогащения исследования были собраны комментарии отечественных IT-экспертов и лидеров мнений относительно долгосрочного использования Open Source и необходимых условий успеха. Ниже приведены ключевые тезисы из их оценок (источник – открытые публикации и интервью в СМИ[31][32][33]):

Недооценка затрат и важность поддержки

Дмитрий Фролов, владелец независимого IT-проекта TvoyGit, отмечает, что одним из рисков является недооценка требуемых затрат при внедрении OSS «из коробки». Многие организации, особенно обладающие сильными инженерными командами, предпочитают растить экспертизу внутри, не всегда учитывая стоимость и сроки такой разработки[31]. По мнению эксперта, наличие локального вендора, предлагающего поддержку того же OSS-продукта на всем жизненном цикле, может быть отличной (и даже более дешевой) альтернативой сугубо самостоятельному пути[31]. Это перекликается с позицией представителей бизнеса: если в стране сформируется рынок услуг по поддержке OSS, компании будут рады воспользоваться им, нежели нести скрытые издержки самостоятельно.

Дефицит компетенций и риски «сырых» решений

Сергей Жемжицкий, зам. технического директора Arenadata, не видит в Open Source каких-то принципиально новых, неизвестных рисков – все основные угрозы понятны и решаемы при наличии компетенций[34]. Однако он подчеркивает специфический риск для объектов критической инфраструктуры (ОКИИ): там иногда внедряют технологии, недостаточно обеспеченные локальными компетенциями. В результате в чувствительных областях могут оказаться решения, которые не выдержат испытания временем и могут прекратиться в развитии, если вокруг них нет устойчивого сообщества или поддержки[34]. Пример – организации ОКИИ могут взять модный OSS-продукт, но без экспертизы и участия в сообществе этот продукт может «застрять» в их инфраструктуре без обновлений. Жемжицкий также упоминает свежий кейс с блокировкой Docker Hub для российских IP как сигнал: при использовании неофициальных зеркал есть риск получить вредоносные закладки, так что важно развивать собственные репозитории и компетенции безопасного использования OSS[35]. Главным подходом к работе с такими рисками он называет развитие компетенций и образование – обучение принципам и культуре эффективного и безопасного использования Open Source, начиная с университетов и внутрикорпоративных программ[36].

Ошибки в подходе компаний к Open Source

Надежда Кострюкова, и.о. директора АНО «Открытый код» (инициатива Минцифры РФ), обращает внимание на низкое понимание природы Open Source на рынке. По ее словам, некоторые компании выкладывают свои разработки в открытый доступ, но не планируют их поддерживать – смысла таких действий мало, это не делает продукт успешным OSS[37]. Другие не разбираются в моделях лицензирования и стоящих за проектом силах: пытаются форкнуть проект, который на самом деле open-core, а не полностью open-source (то есть нет сообщества, а открыт только код)[38]. Например, несколько российских компаний сделали форки популярного проекта Dremio, не учтя, что у него закрытая модель разработки – в итоге эти форки невозможно развивать и поддерживать полноценно[38]. Также эксперт критикует декларации некоторых организаций: «теперь используем только open source» после ухода вендоров. Они не осознают реальную стоимость развития таких проектов, которая может измеряться сотнями миллионов рублей в год[39]. Через некоторое время эйфория «мы свободны, все под контролем» сменится разочарованием: нужные фичи не появляются сами собой, баги некому быстро исправить и т.д.[40]. В итоге большинство компаний, которые сейчас делают ставку на «только Open Source», стратегически проиграют, если не создадут механизмов поддержки – они не смогут поддерживать должный темп разработки[40]. Вывод Кострюковой: необходимо восстановить доверие компаний к вендорам, но уже к отечественным. Последние же, в свою очередь, к сожалению, часто пытаются просто заработать быстрых денег в условиях дефицита предложений – это выливается в необоснованный рост цен и появление множества форков OSS, в которые разработчики почти ничего не вкладывают[41]. Потребуется время, чтобы все участники процесса – вендоры и потребители – нашли баланс для успешного развития технологий на базе OSS.

Смена лицензий и покупка OSS-проектов

Владимир Озеров, CEO компании Querify Labs, добавляет еще один риск: когда открытый проект покупается крупной компанией и вектор его развития меняется[33]. Примеры – MySQL (приобретена Oracle) или Nginx (приобретен F5) – показывают, что проект может перестать быть прежним. Впрочем, Озеров отмечает, что если ПО востребовано, то появляются форки: так, на место MySQL пришла MariaDB, на место закрытого ElasticSearch – OpenSearch, на смену CentOS – Rocky Linux[33]. Для большой компании поддерживать свой форк OSS не составляет проблемы, а если ресурсов нет – всегда можно перейти на альтернативный OSS-продукт, благо обычно их несколько. Таким образом, мировой опыт подсказывает: даже смена лицензии или закрытие проекта – решаемая проблема, сообщество часто подхватывает знамя.

Необходимость внутренних компетенций

Практический пример привел **Павел Логинов, руководитель отдела эксплуатации EdgeCenter**: когда Red Hat прекратил поддержку CentOS, компания была вынуждена за короткий срок перевести все сервера на CentOS Stream 8, а затем планирует миграцию на Ubuntu[42]. Это иллюстрирует важность гибкости и готовности быстро адаптироваться к изменениям в OSS-мире. Компании, имеющие сильные команды, могут относительно безболезненно совершать такие переходы – еще один аргумент в пользу инвестиций в внутренние компетенции.

Перспективы OSS-бизнеса

Дмитрий Калаев (ФРИИ) и некоторые венчурные эксперты указывают на сложность монетизации OSS-проектов. Открытая модель зачастую не сулит быстрого заработка, а успех требует сначала завоевать популярность и репутацию в сообществе, и лишь потом строить бизнес[43]. Хотя есть успешные примеры (Nginx, Postgres Pro), в целом инвесторы с осторожностью относятся к стартапам на основе Open Source – бизнес-модель кажется менее очевидной, чем продажа лицензий. Для корпоративных пользователей это означает, что часть OSS-проектов может испытывать недостаток финансирования, что повышает риски (прекращение развития, отсутствие поддержки). Эта мысль созвучна опасениям, отмеченным в разделе 5: у OSS есть «подводные камни» жизненного цикла, поэтому компаниям важно следить за состоянием проектов, которые они используют, и по возможности участвовать в их поддержке (через контрибьюции или спонсорство).

Общая оценка экспертов

Российским организациям предстоит сформировать корпоративные компетенции работы с OSS, чтобы перейти от просто эксплуатации к стратегическому использованию открытых технологий[44]. Открытое ПО – не панацея само по себе; его преимущества раскрываются при условии активного участия компаний в сообществе, наличия плана B (форков, альтернатив) и грамотного управления рисками (обновления, безопасность, лицензии). Многие сложности, с которыми сталкивается OSS, встречаются и у проприетарных решений, но в случае OSS организация сама должна быть более проактивной. Как подчеркнул один из экспертов, «у открытости есть цена» – и эта цена выражается в необходимых инвестициях в людей, процессы и возможно партнерства[45]. Однако, заплатив эту цену, компания получает значительные дивиденды в виде независимости и инновационности.

Комментарии ИТ-лидеров дополняют количественные результаты опроса: Open Source эффективно работает «в долгую» лишь при наличии компетентной команды или надежного партнера. Без этого организация рискует застрять с устаревшей версией или сделать неправильную ставку. Поэтому главный совет от экспертов – развивать культуру работы с Open Source внутри страны: обучение, обмен опытом, открытые совместные проекты. Тогда и риски снизятся, и выгоды OSS будут реализованы в полной мере[36].

Выводы

По итогам исследования картина выглядит зрелой, но трезвой. ПО с открытым исходным кодом стало опорой текущей инфраструктуры — прежде всего в мониторинге, DevOps и контейнерах, где доля открытых решений достигает 70–90%. Однако этот успех — скорее тактический ответ на внешние шоки, чем устойчивая стратегия. В критичных слоях (виртуализация, резервное копирование, серверные ОС) зависимость от унаследованных западных платформ по-прежнему велика, а там, где open source уже доминирует, он приносит с собой повышенный операционный риск и «размытую» ответственность.

Главный вывод

Рынок за два года научился жить на open source, но не закрыл вопрос управляемости и гарантированности результата. Около 60% ИТ-директоров прямо называют open source временной мерой — до появления зрелых отечественных альтернатив; порядка 40% видят в нём долгосрочную стратегию. Это не раскол, а констатация: бизнес ценит гибкость и отсутствие вендорской привязки, но при работе с инфраструктурой он по-прежнему ищет контрактную ответственность, SLA и предсказуемые релизы.

Риск-профиль подтверждает осторожность

32% компаний сталкивались с серьёзными инцидентами — чаще всего с уязвимостями и сбоями после обновлений, а также с недоступностью внешних репозиториев. Характерный пример — инцидент с Zabbix в крупном ритейле: отсутствие формализованных процедур безопасной эксплуатации позволило атакующему пройти через мониторинг в сеть и нарушить работу кассовых узлов. Такие истории не уникальны: в open source нет единого ответственного центра, и даже зрелые проекты уязвимы к задержкам патчей, ошибкам в цепочке зависимостей и человеческому фактору. Для бизнеса это означает простую вещь — без собственных процессов и внешнего SLA открытый стек остаётся зоной повышенного риска.

Экономика тоже неоднозначна. Да, 62% респондентов фиксируют выигрыш по TCO, но каждый пятый — рост совокупной стоимости владения: внутренняя поддержка, доработки, обучение и интеграции «съедают» экономию на лицензиях. Выгода появляется там, где есть дисциплина обновлений, зрелый инжиниринг и грамотное портфолио: open source без процессов — дешевый на входе, дорогой на выходе.

Отдельный пласт — восприятие отечественных продуктов. Цифры суровы: 88% говорят о «сырости», 82% — о нехватке функционала, 74% — о цене. Но качественные комментарии показывают: во многих компаниях такие оценки не подкреплены собственными пилотами. Решение часто принимается «по рынку», а не по стенду с метриками. Это симптом не только продукта, но и коммуникации: у российских вендоров нет достаточных маркетинговых бюджетов и длительных «школ доверия», которыми десятилетиями пользовались глобальные игроки. В результате разрыв доверия подпитывается не столько фактами эксплуатации, сколько дефицитом сопоставимых испытаний.

При этом роль российских вендоров в устойчивости ландшафта — ключевая. Именно они могут закрыть то, чего принципиально не даёт open source: персональную ответственность, SLA, управляемые релизы и гарантированную совместимость. Их стартовые условия объективно сложнее — меньше ресурсов, меньше брендинга, больше скепсиса. Значит, на стороне заказчиков и государства должна появиться институциональная поддержка: от софинансирования пилотов до инфраструктуры автономности (зеркала, реестры проверенных зависимостей, юридически выверенный режим форков).

Практические рекомендации

Для бизнеса

Закладывайте в архитектуру «страховку» против типовых рисков open source: обязательное сканирование зависимостей и управление версиями, канареечные релизы и план отката, локальные зеркала артефактов/образов, каталог одобренных библиотек. Считайте полный TCO до миграции (поддержка, интеграции, обучение, простои). Превратите дискуссию про отечественные продукты из «мнений» в измерения: 3–6-месячные пилоты с KPI (SLO, стоимость инцидента, трудозатраты на обновления) и сопоставимыми стендами. В критичных зонах «прикручивайте» к open source контрактную поддержку российских компаний — чтобы закрыть вопрос ответственности и времени реакции.

Для российских вендоров

Доверие должно стать частью продукта. Публичная дорожная карта, LTS-ветки, регулярные security-адвайзори, предсказуемый релиз-менеджмент. Сервис — дифференциатор: 24×7 поддержка, жёсткие SLA, миграционные утилиты и сервисы, совместимость с популярным открытым стеком и другими отечественными продуктами. Маркетинг — через практику: референс-кейсы с метриками TCO/SLO, бесплатные пилотные пакеты, песочницы, сеть интеграторов. Там, где это возможно, — открывать ядро (open-core) для ускорения доверия, сохраняя коммерческую надстройку.

Для государства и регуляторов.

Сместить акцент с директив «заменить любой ценой» на поддержку безопасного использования open source и рост отечественных продуктов. Нужны национальные зеркала Git- и контейнерных реестров, реестр проверенных зависимостей, типовые SLA и шаблоны контрактов для закупок, софинансирование пилотов у системных заказчиков. Юридически закрепить режим форков и правомерного использования локальных зеркал. Поддержать центры компетенций (вузы/технопарки) и программы подготовки инженеров по эксплуатации открытого стека в промышленных условиях.

Open source сегодня — однозначно полезный инструмент, который спас рынок от технологического провала, одновременно переложив на заказчика бремя безопасности и устойчивости. Отечественные вендоры, даже с меньшими бюджетами, способны вернуть инфраструктуре управляемость и настоящую суверенность — через сервис, лицензионную чистоту, совместимость и ответственность. Следующие 3–5 лет определят баланс: либо open source останется временной «заплатой», либо станет зрелым компонентом гибридной модели, где открытый стек дополняется российскими продуктами с понятной поддержкой и предсказуемой эволюцией. Чтобы случился второй сценарий, бизнесу нужно мерить и пилотировать, вендорам — продвигать и интегрировать, государству — работать над спросом и укреплять инфраструктуру автономности. Тогда привычка уступит месту доверию, а компромисс — стратегии.

Список источников и приложения

Основные источники данных:

- Опрос ИТ-директоров 2025 (Россия) – авторское исследование, результаты которого представлены в данном отчете. Выборка: 138 организаций, метод – анкетирование + интервью.
- Аналитический отчет ГК B1 «Программное обеспечение с открытым кодом: открытые возможности, скрытые сложности» (2024) – результаты опроса 150 экспертов ИТ. Использованы для сравнения проникновения OSS (83% компаний используют или планируют) и проблем внедрения (данные о 77% использующих российское OSS, 67% не достигли целей и др.).
- Статья Дмитрия Кабанова «OSS, который не смог» – почему нельзя так просто взять и использовать Open Source вдолгую (vc.ru, июнь 2024) – аналитический материал с комментариями экспертов. Использован для раздела 9 (мнения ИТ-лидеров: Фролов, Жемжицкий, Кострюкова, Озеров и др.).
- Отраслевой обзор ItWeek.ru «Почему российские компании массово переходят на модель open-source» (2025) – содержит статистику и прогнозы (Accenture: >90% компаний к 2026; данные B1: 83% уже используют; оценка Strategy Partners: рынок OSS в РФ 250 млрд руб к 2030).
- SberPro Медиа: «Открытый доступ: какие задачи решает Open Source и какие риски нужно учесть» (2023) – статья об OSS, данные MarketsandMarkets (мировой рынок OSS-услуг $54 млрд к 2027), цитаты экспертов о плюсах/минусах открытого ПО.
- Материалы Tadviser, CNews, Forbes и др. по теме Open Source в России. В частности, Tadviser (2022) о 80% компаний, использующих LAMP-стек, Forbes (2023) о тенденциях OSS, CNews о росте использования OSS в облаках (80% компаний увеличили использование OSS за год) и т.д. Эти данные использовались косвенно для общего фона и проверки консистентности результатов.
- Отчет Linux Foundation «State of Open Source Security» (2023) – использован опосредованно через цитирование в источниках (для указания на необходимость юридической экспертизы лицензий).

Для удобства читателей при ссылках в тексте отчета указаны цитаты из открытых источников в формате [№ источника]. Полные тексты доступны по прямым ссылкам. В приложении также можно найти методику опроса и анкету

Приложения:

- Приложение А. Анкета опроса ИТ-директоров (2024) – включает список вопросов, используемые определения и шкалы, а также развернутые опции ответов.
- Приложение В. Глоссарий терминов – расшифровка используемых сокращений и названий (OSS, СУБД, CI/CD, Kubernetes, и т.д.), список упомянутых продуктов с указанием их происхождения (Open Source проект, отечественный разработчик, западный вендор).

[1][4][5][7][8][9][10][13][30][45][46][59] Программное обеспечение с открытым кодом: открытые возможности, скрытые сложности https://b1.ru/analytics/b1-open-source-software-survey-2024

[2] [3] [17] [28] Почему российские компании массово переходят на модель open-source https://www.itweek.ru/foss/article/detail.php?ID=232948

[6] [11] [12] [14] [15] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [47] [48] [49] [50] [51] [52] [53] [55] [56] [57] Результаты опроса по использованию Open Source в российских организациях (сырые данные исследования)

[16] [29] [54] Открытый доступ. Какие задачи решает open source и какие риски нужно учесть при его применении I СберПро Медиа https://sber.pro/digital/publication/otkrytyj-dostup-kakie-zadachi-reshaet-open-source-i-kakie-riski-nuzhno-uchest-pri-ego-primenenii

[31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] «OSS, который не смог», или почему использование open source решений вдолгую требует корпоративных компетенций / Хабр https://habr.com/ru/articles/818009

[58] Программное обеспечение с открытым кодом (Open Source) в России https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BE%D0%B4%D0%BE%D0%BC_(Open_Source)_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#:~:text=,Linux%2C%20Apache%2C

Приложение А. Анкета опроса ИТ-директоров

Название исследования: Опрос по использованию Open Source-решений в российских организациях
Цель: Сбор информации об использовании ПО с открытым исходным кодом, оценка рисков, выгод, барьеров и перспектив.
Период проведения: 1–12 августа 2025 года
Метод: обзвон базы контактов по таргетной выборке, отправка ссылки на форму, онлайн-анкетирование через Яндекс.Формы, анонимный сбор данных.

1. Профиль организации
1.1. Численность сотрудников: «До 1 000», «1 000–5 000», «Более 5 000»
1.2. Отрасль: «Финансовый сектор / финтех», «Промышленность / добыча / энергетика», «Ритейл / e-commerce», «Госсектор», «Телеком», «Другое»
1.3. Знаете ли вы, какие решения используются в вашей организации?: «Да», «Нет, имею поверхностное понимание»
2. Стек по уровням инфраструктуры
2.1. Операционные системы: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.2. СУБД: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.3. Виртуализация: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.4. Контейнеризация / оркестрация: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.5. Резервное копирование: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.6. Мониторинг и observability: «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
2.7. Инструменты DevOps (CI/CD, IaC): «Open Source», «Остались пока западные решения», «Из реестра Минцифры»
3. Практика использования Open Source
3.1. Как часто обычно обновляете версии Open Source-продуктов?: «Непрерывно», «2–3 раза в год», «1 раз в год», «Реже 1 раза в год»
3.2. Используете в большинстве случаев Open Source-решения в СПО «как есть» без модификаций?: «Да», «Нет».
4. Риски
4.1. Какие риски вы считаете основными? (выберите до 3): «Информационная безопасность», «Сбои / баги», «Трудности масштабирования», «Отсутствие поддержки», «Лицензионные, регуляторные или санкционные ограничения», «Несовместимость с отечественным ПО», «Дефицит кадров», «Высокая итоговая стоимость владения», «Другое (укажите)»
4.2. Если выбрали «Другое», напишите свой вариант: (свободный ответ)
4.3. Были ли в вашей организации значимые инциденты, связанные с Open Source (сбой, уязвимость, санкционный запрет и прочее)? Выберите один из вариантов: «Да», «Нет»
4.4. Если были, поделитесь причинами и последствиями: (свободный ответ)
5. Экономика и выгоды
5.1. Основные выгоды использования Open Source (выберите до 3): «Низкая стоимость владения», «Зрелость продуктов и богатый функционал», «Гибкость и кастомизация»
5.2. Если выбрали «Другое», напишите свой вариант: (свободный ответ)
5.3. Проводите ли вы расчет TCO при выборе нового решения (Open Source против коммерческих)? Выберите один из вариантов: «Да», «Нет».
6. Отечественные альтернативы
6.1. Что, по вашему мнению, мешает переходу на отечественное ПО? (выберите до 3): «Завышенные цены на лицензии», «Недостаток доверия», «Незрелость продукта», «Отсутствие требуемого функционала», «Слабая защищенность и уязвимость», «Низкое качество постпродажного сервиса», «Трудности внедрения», «Другое (укажите)»
6.2. Если выбрали «Другое», напишите свой вариант: (свободный ответ)
7. Стратегия и прогнозы
7.1. Open Source для вашей компании — временная мера или долгосрочная стратегия? «Временная мера до появления зрелых отечественных альтернатив», «Постоянная стратегия»
7.2. Если иностранный Open Source будет запрещен, что вы предпримете? «Перейдем на локальные форки / зеркала», «Перейдем на отечественное ПО», «Перепишем архитектуру», «Всё перечисленное», «Ничего»
7.3. Какую долю инфраструктурного ПО, по вашему прогнозу, будет занимать Open Source через 3 года? (Укажите %)
8. Дополнительно
8.1. Ваши дополнительные комментарии по теме использования Open Source: (свободный ответ)

Приложение В. Словарь терминов, методологические комментарии

Пояснения к ключевым терминам

ПО с открытым исходным кодом (open source) — Программное обеспечение, распространяемое с лицензиями, позволяющими свободно изучать, изменять и распространять его исходный код. Примеры: Linux, PostgreSQL, Kubernetes. В рамках данного исследования к open source также отнесены коммерческие дистрибутивы, построенные на открытом коде, если ядро решения и ключевая функциональность доступны по открытой лицензии.
Отечественное ПО — ПО, включённое в Единый реестр российских программ для ЭВМ и баз данных (Минцифры РФ). Критерии включения: разработка на территории РФ, владение исключительными правами российским юридическим или физическим лицом, соответствие ряду технических и правовых условий.
Западное ПО — Программные продукты иностранных компаний, преимущественно из США, ЕС, Великобритании, Канады, Австралии, Японии и других стран с действующими санкционными режимами в отношении РФ.
Гибридные решения — Продукты, сочетающие ядро на базе open source и коммерческую надстройку (например, Red Hat OpenShift, Elastic Stack с платными модулями). В анкете респонденты относили их либо к open source, либо к коммерческому ПО, исходя из доминирующего сценария использования в их организации.
СУБД — Системы управления базами данных — программные комплексы для создания, управления и доступа к данным (PostgreSQL, Oracle, MySQL, Postgres Pro и др.).
CI/CD, IaC — Инструменты автоматизации разработки и эксплуатации:

- CI/CD — Continuous Integration / Continuous Delivery (Jenkins, GitLab CI, TeamCity).
- IaC — Infrastructure as Code (Ansible, Terraform).

TCO (Total Cost of Ownership, совокупная стоимость владения) — Методика оценки общих затрат на владение ИТ-решением, включая лицензии, поддержку, обучение, интеграцию, модернизацию и эксплуатацию.

Методологические комментарии к анкете

1. Профиль организации (вопросы 1.1–1.3)
Сбор базовой информации о размере и отрасли организации, а также уровне информированности респондента. Эти данные позволяют сегментировать результаты и выявлять различия между отраслями и масштабами бизнеса.
2. Стек по уровням инфраструктуры (вопросы 2.1–2.7)
Оценка доминирующего типа решений (open source, западное ПО, отечественное ПО) на ключевых уровнях ИТ-инфраструктуры. Формулировка «в большей степени присутствуют» предполагает выбор варианта, который покрывает наибольшую долю инсталляций в организации.
3. Практика использования Open Source (вопросы 3.1–3.2)
Измеряет зрелость процессов эксплуатации open source, частоту обновлений и уровень кастомизации (использование «как есть» или с доработками).
4. Риски (вопросы 4.1–4.4)
Позволяют выявить приоритетные угрозы в восприятии ИТ-директоров: от ИБ и отказоустойчивости до кадрового дефицита и правовых рисков. Множественный выбор (до 3 пунктов) даёт возможность выделить ключевые факторы.
5. Экономика и выгоды (вопросы 5.1–5.3)
Оценивается, какие преимущества респонденты считают главными (стоимость, гибкость, независимость, комьюнити) и насколько TCO является фактором принятия решений.
6. Отечественные альтернативы (вопросы 6.1–6.2)
Идентификация барьеров для перехода на российские решения. Множественный выбор (до 3 пунктов) отражает комплексность проблем — от цены и функционала до доверия и зрелости продукта.
7. Стратегия и прогнозы (вопросы 7.1–7.3)
Вопросы, формирующие представление о стратегической роли open source в компаниях и оценках его доли в будущем. Также выявляют готовность компаний к гипотетическому запрету иностранного open source.
8. Дополнительно (вопрос 8.1)
Открытое поле для комментариев, дающее возможность респондентам выразить мнение за рамками формализованных вопросов.
Примечание по погрешности:
Объём выборки n=138 (для отдельных вопросов, где применялся фильтр, база могла быть меньше). При уровне доверия 95% погрешность составляет ±8 п.п.