

COSS-продукты

и их перспективы на российском рынке



Михаил САМИЧЕВ,
директор по разработке и архитектуре ПО
Fork-Tech

Однако от ПО с полностью открытым исходным кодом (pure open source) COSS отличается сразу по нескольким ключевым признакам. Во-первых, у продукта есть понятный владелец и центр ответственности, публичная дорожная карта развития, коммерческая поддержка и SLA, мотивация развивать продукт не «пока есть энтузиазм», а системно и на горизонте многих лет.

Во-вторых, важную роль играет лицензионная модель. Pure open source под лицензиями вроде GPL, Apache или MIT, как правило, не накладывает ограничений на коммерческое использование. В COSS же часто используются двойное лицензирование (open source-ядро + коммерческая версия), лицензии с ограничениями на коммерческое использование (SSPL, BSL) и enterprise-модули под проприетарной лицензией. Это не недостаток, а фундамент бизнес-модели: вендор открывает базу, но зарабатывает

COSS-продукты (Commercial Open Source Software) – это открытый код плюс коммерческая ответственность. В основе таких продуктов лежит open source, который можно посмотреть, изучить, использовать и при необходимости доработать. Но при этом за продуктом стоит компания, которая зарабатывает на нем деньги и, что принципиально важно, несет ответственность перед заказчиком. От классического проприетарного программного обеспечения COSS отличается тем, что код не закрыт. Заказчик не работает с «черным ящиком» и не оказывается полностью зависимым от одного конкретного вендора и его решений – будь то изменение цен, лицензий или внешнеполитическая ситуация.

на зрелых, корпоративных сценариях использования. Именно так работают GitLab, Redis, Elastic, Confluent – и по той же логике развиваются российские продукты вроде Postgres Pro или Tarantool. На практике COSS – это компромисс между свободой и гибкостью open source и требованиями корпоративного рынка к стабильности, поддержке и управляемости.

COSS-модель: плюсы и минусы

Для российских компаний и особенно для госсектора ключевое преимущество COSS – это независимость и контроль над критически важными ИТ-системами. Цена действительно важна, но она не является решающим фактором.

Здесь важны несколько принципиальных моментов: доступ к исходному коду и возможность его аудита, в том числе с точки зрения информационной безопасности; отсутствие жесткой зависимости от зарубежного вендора и его экосистемы; возможность развивать продукт своими силами или привлекать альтернативных подрядчиков, а также более долгий и предсказуемый жизненный цикл системы.

Для государства и крупных организаций это критично, потому что речь идет не просто об ИТ-инструментах, а о стабильности, непрерывности и управляемости ключевых процессов. В этом смысле COSS лучше вписывается в логику цифрового суверенитета, чем классическое проприетарное ПО.

Текущая геополитическая ситуация и санкционное давление стали мощным катализатором, но не первопричиной всплеска интереса к этой модели в России. Интерес к open source и COSS в нашей стране существовал и раньше, однако он был скорее точечным и редко доходил до уровня стратегических решений. После 2022 года компании столкнулись не только с уходом вендоров, но и с более широкими рисками экосистемы, такими как отзыв и блокировка лицензий, прекращение технической поддержки без переходного периода, закрытие доступа к репозиториям и сервисам, ограничения на использование CI/CD и облачных платформ (показательный пример – ограничения GitHub для отдельных регионов), а также сложности с оплатой и юридическое сопровождение контрактов.

В этот момент стало очевидно, что зависимость от внешней экосистемы – это отдельный риск. Поэтому логично было бы предположить, что это – не временный тренд, а системный сдвиг. ИТ все чаще рассматриваются как стратегический актив, который должен быть контролируемым, развиваемым и устойчивым в долгосрочной перспективе.

Часто звучит тезис о том, что open source безопаснее, так как код можно проверить. Но с другой стороны, у COSS-продуктов есть коммерческая «надстройка». Как же обеспечивается безопасность? Отметим, что безопасность в COSS-продуктах строится на двух уровнях. Первый уровень – open source-ядро. Исходный код доступен



На чем зарабатывает вендор?

Разберемся, как устроена бизнес-модель успешного COSS-продукта, на чем именно зарабатывает вендор и насколько эта модель устойчива в условиях российского рынка. Как правило, вендор COSS

Elastic, Redis) и постепенно укореняется в России – на примере Postgres Pro, Arenadata, Tarantool и других платформенных решений. В целом, для российского рынка она выглядит устойчивой: бюджеты ниже, чем на Западе, но спрос на надежные, управляемые и независимые решения остается высоким, особенно в госсекторе и крупном корпоративном сегменте.

Одна из существующих проблем – нехватка специалистов, способных работать с open source-стеком. Может показаться, что стоимость специалистов становится скрытым минусом, который съедает экономию на лицензиях. Этот момент действительно нельзя игнорировать. Квалифицированные специалисты по open source-стеку стоят дорого, и это увеличивает первоначальные затраты. Но здесь есть важное стратегическое отличие: если в случае пропри-

Для российских компаний и особенно для госсектора ключевое преимущество COSS – это независимость и контроль над критически важными ИТ-системами.

для анализа, аудита и независимой проверки. Это снижает риск скрытых уязвимостей, упрощает контроль цепочек поставки и повышает доверие к базовой логике продукта, особенно в критических системах.

Второй уровень – коммерческая надстройка. Здесь включаются стандартные корпоративные практики: формализованные процессы безопасной разработки (Secure SDLC); регулярные обновления и исправления уязвимостей; ответственность вендора за качество и безопасность, а также поддержка и оперативное реагирование на инциденты.

В результате COSS сочетает прозрачность open source и дисциплину коммерческого продукта, что на практике дает более сбалансированный и управляемый подход к безопасности.

зарабатывает не на продаже самого кода, а на сервисах вокруг него: подписках на поддержку и обновления, enterprise-функциях и расширениях, облачных

и managed-сервисах, внедрении, консалтинге и сопровождении, обучении и сертификации специалистов.

Эта модель доказала свою жизнеспособность в мире (GitLab,

ИТ все чаще рассматриваются как стратегический актив, который должен быть контролируемым, развиваемым и устойчивым в долгосрочной перспективе.

етарного ПО деньги в основном уходят на лицензии, то в случае COSS – на людей и внутреннюю экспертизу.

При этом экспертиза в области open source и COSS не привязана

к конкретному вендору. Инженер, который умеет работать с PostgreSQL, Kubernetes или Kafka, не привязан к одному вендору, как это часто бывает с закрытыми корпоративными системами. Это повышает устойчивость компании и делает такие инвестиции более долгосрочными.

Если отвлечься от политических рисков, в некоторых сценариях COSS объективно лучше проприетарного софта, а в некоторых – все же проигрывает. COSS особенно хорошо подходит, когда требуется гибкость и масштабируемость, если важны прозрачность и безопасность, система критична для бизнеса или государства и предполагается долгий срок эксплуатации.

Однако при системном подходе COSS, наоборот, помогает уйти от монолитных вендорских стеков, строить модульную и масштабируемую архитектуру и стандартизировать интеграции через API и открытые протоколы. Во многих случаях это не шаг назад, а шаг к более гибкой и управляемой ИТ-архитектуре.

Будущее COSS в России

Рассмотрев все плюсы и минусы, можно предположить, что COSS-модель может стать доминирующей в государственном и корпоративном секторе России в ближайшие 5–7 лет. Для этого необходимо продолже-

(«купили коробку – поставили галочку») к OPEX-подходу, где ИТ – это постоянно развиваемый стратегический актив, требующий инвестиций, внимания и экспертизы.

Существует определенный риск, что развитие COSS может привести к фрагментации рынка и росту форков. Когда код открыт, всегда возможны форки и альтернативные версии продукта. Однако нельзя считать это однозначным минусом. Форки обеспечивают защиту от монополии одного вендора, дают возможность продолжить развитие продукта при смене стратегии компании и обеспечивают естественный механизм конкуренции. Для заказчика это, скорее, плюс, при условии, что он понимает, на каком продукте и под какой лицензией строит свою систему.

В перспективе Россия и сама сможет стать экспортером COSS-продуктов, и предпосылки для этого есть, особенно в инфраструктурном ПО, базах данных, DevOps и платформенных решениях. Именно эти классы продуктов проще экспортировать, потому что они основаны на глобальных open source-стандартах, не привязаны к локальной бизнес-логике, хорошо масштабируются и понятны международному рынку.

Основные сложности могут быть связаны не с технологиями, а с продуктовым мышлением, маркетингом и выходом на ме-

В результате COSS сочетает прозрачность open source и дисциплину коммерческого продукта, что на практике дает более сбалансированный и управляемый подход к безопасности.

Проигрывает COSS там, где нужен полностью готовый «коробочный» продукт без доработок, и где бизнес не готов инвестировать в собственную ИТ-экспертизу. Полной замены всему проприетарному ПО пока действительно нет, но в инфраструктурных и платформенных решениях – операционные системы, базы данных, контейнеризация, DevOps – COSS уже фактически стал стандартом.

Еще один дискуссионный момент – насколько легко интегрировать COSS-решения в уже существующую ИТ-инфраструктуру, построенную вокруг проприетарных продуктов. Становится ли это «лоскутной автоматизацией» или, наоборот, путем к созданию более гибкой архитектуры?

Если внедрять COSS-решения без общей архитектурной концепции, риск лоскутной автоматизации действительно существует.

не государственной поддержки, регуляторная ясность, развитие кадров и образовательных программ, рост зрелости российских вендоров, переход бизнеса от логики разовой покупки лицензии к логике долгосрочного управления ИТ-активами.

COSS-модель может стать доминирующей в государственном и корпоративном секторе России в ближайшие 5–7 лет.

Главное препятствие здесь кроется не в технологии как таковой, а в управленческом мышлении. Фактически речь идет о смене парадигмы: от CAPEX-подхода

к международным рынкам. Если эти барьеры будут преодолены, у российских COSS-продуктов есть реальные шансы занять свою нишу на глобальном рынке. ■