Визитка

СЕРГЕЙ ГОРБУНОВ,
главный инженер-программист службы внедрения и сопровождения, компания «Форс – Центр разработки»

Импортозамещение ПО:
возможные риски и способы их избежать

В последние годы в России наблюдается устойчивый тренд на импортозамещение, охватывающий различные сегменты рынка, включая программное обеспечение. Первоначально акцент делался на замещение коммерческого ПО, однако в настоящее время заказчики всё чаще требуют и замены продуктов с открытыми лицензиями. Рассмотрим потенциальные риски и вызовы, связанные с этим процессом, которые не всегда могут быть очевидны для заказчиков.

Проблемы совместимости и безопасности

Один из ключевых аргументов в пользу импортозамещения – обеспечение информационной безопасности. Отечественные продукты часто позиционируются как защищённые от санкционных рисков, а наличие сертификатов ФСТЭК подтверждает успешное прохождение проверок. Однако это не всегда гарантирует полную безопасность.

Одним из наиболее распространённых методов выявления уязвимостей в программном обеспечении является использование базы данных CVE (Common Vulnerabilities and Exposures). Этот международный публичный реестр, содержащий информацию о выявленных уязвимостях в различных программных продуктах. Однако стоит отметить, что в базу данных CVE не входят отечественные решения, поскольку большинство из них не являются самостоятельными продуктами, а представляют собой форки иностранных разработок.

> В отечественных решениях исходный код, как правило, является закрытым, что ограничивает возможности самостоятельной проверки программного обеспечения на наличие уязвимостей. В связи с этим, остаётся только метод «black box» — попытка воспроизведения известных уязвимостей, обнаруженных в открытых продуктах

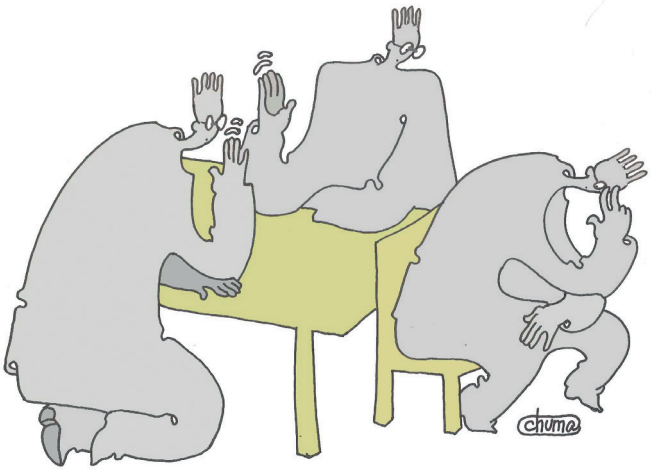
Необходимо учитывать уникальные особенности отечественных решений. В частности, они часто имеют собственные системы нумерации версий, которые могут отличаться от международных стандартов. Кроме того, в некоторых случаях обновления пакетов в отечественных операционных системах могут осуществляться путём применения патчей к более старым версиям, а не путём выпуска новых версий с обновлёнными компонентами.

В качестве примера можно рассмотреть уязвимость CVE-2022-41742, которая была обнаружена в программном обеспечении nginx версии 1.22.0 и устранена в версии 1.22.1. Однако в комплекте с некоторыми отечественными операционными системами может поставляться версия nginx 1.22.0-1, которая не упоминается ни в базе данных CVE, ни на официальном сайте проекта. В данном случае суффикс «-1» указывает на то, что к версии nginx был применён какой-то патч, но какой конкретно патч – определяется только поставщиком операционной системы, необходимо каждый раз изучать документацию.

Следует отметить, что в отечественных решениях исходный код, как правило, является закрытым, что ограничивает возможности самостоятельной проверки программного обеспечения на наличие уязвимостей. В связи с этим, остаётся только метод «black box» – попытка воспроизведения известных уязвимостей, обнаруженных в открытых продуктах, для определения подверженности отечественных решений этим уязвимостям.

Казалось бы, добавить ещё больше сложностей отделу безопасности уже не получится, но существует ещё один аспект, который следует рассмотреть. Сканеры безопасности, как правило, основаны на базе данных CVE, что предполагает использование версий программного обеспечения, предоставляемых исходными поставщиками. Они не учитывают форки, а также модификации, вносимые в отечественные операционные системы, что делает их менее эффективными в выявлении уязвимостей.

Но для этой проблемы есть частичное решение – База



Необходимо учитывать уникальные особенности отечественных решений

Данных Уязвимостей (БДУ) ФСТЭК, российский аналог CVE. Также существуют отечественные сканеры уязвимостей, которые умеют работать с БДУ и способны обнаружить уязвимости в отечественных решениях. Хотя эти инструменты ещё только развиваются, в будущем они могут стать надёжным решением.

Иностранное ПО постоянно развивается, добавляя новые полезные функции. Форк же начинает свою жизнь только после релиза базового ПО, что приводит к его отставанию. Затем требуется время на доработку и сертификацию. В результате, сертифицированное отечественное решение может получить новый функционал лишь через год или два

Особенности сертификации приводят к значительному увеличению сроков поставки новых версий программного обеспечения. После релиза версия должна быть направлена в испытательную лабораторию для проведения тестов на уязвимости, качество кода и другие параметры. Это приводит к тому, что поставка новой версии становится невозможной в кратчайшие сроки, и процесс может затянуться на период от месяца до года.

Информационная безопасность является важным, но не единственным критерием при выборе поставщика. Современные организации стремятся к функциональности, удобству администрирования, стабильности и другим характеристикам. И в этом контексте отечественное программное обеспечение тоже сталкивается с рядом проблем.

Средства автоматизации и DevOps являются ключевыми элементами современной IT-инфраструктуры. Инструменты DevOps – такие как Terraform и Ansible, широко используются в мировой практике. Однако их внедрение в отечественные решения сталкивается с определёнными трудностями.

При использовании Terraform с популярными зарубежными операционными системами – например, Debian или Red Hat, не возникает проблем. Однако при попытке развернуть с их помощью отечественные операционные системы возникают ошибки в «customization tools». Для решения этой проблемы приходится использовать нестандартные методы, такие как изменение файла /etc/issue, указывая исходный дистрибутив Linux вместо фактически используемого форка.

Применение Ansible также может вызвать проблемы, связанные с совместимостью с отечественными решениями. Готовые роли и плейбуки часто отсутствуют, что требует создания собственных сценариев. Аналогичная ситуация наблюдается и в области CI/CD, где готовых скриптов для отечественных систем также нет.

Кроме того, в случае возникновения проблем, которые не описаны в документации, администраторы и разработчики вынуждены искать решения на специализированных порталах, таких как Stack Overflow. Однако количество вопросов и ответов, связанных с отечественными решениями, крайне ограничено. Для решения проблемы можно было бы использовать искусственный интеллект, но источников информации для него недостаточно. Мало освещаются отечественные решения на специализированных ресурсах – блогах, ИТ-форумах и прочее.

Основным критерием выбора решения часто является цена, и здесь отечественные разработки оказываются

в невыгодном положении. Стоимость решения часто является довольно высокой, особенно в сравнении с бесплатными и открытыми аналогами. Бюджеты заказчиков ограничены, и часто приходится вычитать стоимость программного обеспечения из бюджета проекта, что вынуждает искать более дешевых исполнителей или отказываться от части функционала.

Говоря о функционале, мы возвращаемся к вопросу скорости поставки новых версий. Иностранное программное обеспечение постоянно развивается, добавляя новые полезные функции. Форк же начинает свою жизнь только после релиза базового ПО, что приводит к его отставанию. Затем требуется время на доработку и сертификацию. В результате, сертифицированное отечественное решение может получить новый функционал лишь через год или два.

Ярким примером являются отечественные операционные системы. Лишь в 2024 году они перешли на базу Debian 12, а летом 2025 года уже выходит Debian 13. Еще какое-то время уйдет на закупку новых лицензий, перевод серверов на новую версию, доработку заказного программного обеспечения, работающего на них, и так далее. В результате в России промышленные системы перейдут на базу Debian 12, когда остальной мир уже будет разрабатывать Debain 14.

Решением большей части проблем является развитие открытых сообществ и популяризация отечественных решений, а также смена лицензий на условно-бесплатные модели. Одним из таких примеров является Arenadata Greengage — они взяли под крыло проект Greenplum, перешедший на закрытые лицензии

Существует и проблема совместимости. Допустим, мы используем операционную систему на базе Debian 10 и хотим установить Zabbix. Актуальная версия 7.2 на неё не установится, 7.0 тоже. И даже 6.4 нам не подходит, максимум, на что можно рассчитывать – 6.0. Это касается практически любого решения. Некоторые вендоры создают собственные сборки программного обеспечения, повышая версию выше публично доступной, но рассчитывать на самую свежую версию все равно не стоит.

Ещё одна проблема, которая красной нитью проходит через всю статью, – это иностранный софт. Подавляющее большинство отечественных решений базируются на иностранном программном обеспечении. В случае ужесточения санкций и прекращения доступа к зарубежным репозиториям развитие отечественных решений окажется под большим вопросом.

Несмотря на существующие недостатки, в некоторых сферах применение отечественного программного обеспечения является обязательным и обеспечивает высокий уровень защиты. В частности, в закрытых центрах обработки данных (ЦОД) и военной индустрии внешние атаки практически невозможны, поэтому приоритетной задачей становится защита от внутренних угроз. Использование отечественного программного обеспечения и сертификатов ФСТЭК значительно снижает вероятность проникновения вредоносного ПО, что минимизирует риски негативных событий.

Свет в конце туннеля

Российская ИТ-отрасль демонстрирует высокий уровень развития, а отечественные программисты занимают ведущие позиции на мировой арене. Это создаёт благоприятные условия для разработки конкурентоспособного импортонезависимого программного обеспечения.

Важно, чтобы отечественный софт конкурировал на рынке на основе своих технических характеристик, таких как качество, функциональность, доступность и стоимость, а не только в силу требований регуляторов. Это будет способствовать формированию здоровой рыночной среды и стимулировать дальнейшее развитие российской ИТ-индустрии.

Решением большей части описанных проблем является развитие открытых сообществ и популяризация отечественных решений на международных площадках, а также смена лицензий на условно-бесплатные модели. Одним из таких примеров является Arenadata Greengage – они взяли под крыло проект Greenplum, перешедший на закрытые лицензии. Arenadata не только создали отечественный форк, но и стараются развивать открытое сообщество на GitHub.

Стоит упомянуть проект Angie, который так же развивается на GitHub и поощряет сообщество, а коммерциализируют в основном техническую поддержку. Хорошим примером является и компания Ред Софт, которая позволяет любому желающему скачать и использовать в некоммерческих целях – при этом даже не надо заполнять анкеты или подписывать какие-то документы.

Отечественным вендорам необходимо сосредоточиться и на работе с ИТ-блогерами и СМИ, предоставляя им бесплатные версии софта для написания статей, записи обучающих видео на YouTube и других платформах, поощряя их творчество и прислушиваясь при этом к их критике. Для производителей приглашение блогеров на производство может стать отличной рекламой. К сожалению, часто мы видим обратную картину, когда демонстрационные версии доступны только после подписания множества бумаг, а за малейшую критику – лишение статуса партнёра, а иногда и иски в суд.

Заказчикам же мы рекомендуем подходить к выбору программного обеспечения осознанно. Переходя на отечественное ПО, важно помнить, что помимо плюсов существуют и минусы. Эксперты компании Форс помогут грамотно оценить риски использования иностранного ПО и необходимость перехода на отечественные решения, а также помогут с вопросами миграции на него и обеспечения бесперебойной работы систем. EOF

Ключевые слова: импортозамещение ПО, отечественный софт.