09 октября 2024

Перелицованный Open Source угодил под подозрение

Реестр отечественного ПО нуждается в четких критериях для определения собственной разработки ИТ-продуктов на базе решений Open Source. По мнению экспертов, такими критериями могут стать безопасная разработка и наличие добавленного функционала.

Об этом рассказал технический директор АО "Лаборатория Касперского" Антон Иванов 8 октября 2024 г. на круглом столе "ИБ в промышленности" на форуме "Кибертех". В ходе выступления он отметил, что некоторые отечественные разработчики выдают "перелицованные" решения Open Source за собственные разработки.

"Недавно я видел заявку на включение в реестр отечественного программного обеспечения, пришедшую от одного разработчика на систему виртуализации. С точки зрения соответствия формальным критериям все замечательно, все необходимые требования выполнены, все есть. Но само ПО - перелицованный Open Source, а мы формально не можем им отказать. Я считаю, что нужно быть пожестче и поддержать реального отечественного производителя", - отметил он.

Позднее в разговоре с корреспондентом ComNews, Антон Иванов сказал, что такой поддержкой могли бы стать метрики для реестра, с помощью которых можно отличать собственную разработку от "перелицованного" решения Open Source. По его словам, такими метриками могли бы стать безопасная разработка и количество добавленного функционала.

"По моему мнению, эта тема должна начать обсуждаться внутри экспертного совета, потому что мы видим заявки на включение в реестр от многих новых компаний. Однако в рамках экспертного анализа мы понимаем, что это не собственная разработка, а перелицованный Open Source. Я думаю, что ключевыми критериями для включения в реестр должны быть метрики по безопасной разработке, чтобы заявитель проводил статический анализ, демонстрировал, как проходит сборка, чтобы внутри был динамический анализ и дополнительные функции, которые добавил разработчик. Мы не против решений Open Source, мы считаем, что они должны быть безопасными", - рассказал он.

Что касается разработок, которые уже числятся в реестре, но не пройдут по потенциальным новым критериям, по мнению Антона Иванова, их не стоит вычеркивать. Хороший выход из ситуации, по его словам, дать возможность обновить разработку для соответствия критериям.

ДРУГИЕ МНЕНИЯ

"Предлагаемую Антоном Ивановым идею я не разделяю, - сказал генеральный директор АНО "Национальный центр компетенций по информационным системам управления холдингом" (НЦК ИСУ) Кирилл Семион. - Она предполагает явное лоббирование интересов ряда вендоров, что, конечно, неправильно. Правила попадания в реестр определены регулятором, и попытка их как-то модифицировать "со стороны" - совершенно нерыночный подход".

С позицией Антона Иванова согласен менеджер по развитию бизнеса АО "Актив-софт" (Guardant) Михаил Чухломин. По его словам, доля клонов свободного программного обеспечения (СПО) в реестре российского ПО превышает 20%. Он рассказал, что Министерство цифрового развития, связи и массовых коммуникаций поэтапно ужесточает условия добавления СПО в реестр, но многие перелицованные продукты Open Source без нового функционала уже в нем. Но есть и другая проблема - активное использование компонентов зарубежных вендоров.

"Многие продукты, разработанные российскими компаниями, представлены в реестре, но имеют "под капотом" множество проприетарных библиотек от зарубежных вендоров. Это могут быть SDK для компьютерного зрения, инженерных вычислений, обработки документов или защиты и лицензирования ПО. Использование таких компонентов добавляет множество рисков и угроз как компании-вендору, так и конечным пользователям, поэтому оно требует особого внимания со стороны регулятора", - отметил Михаил Чухломин.

Простоту, с которой любой разработчик может попасть в реестр отечественного ПО, признает и руководитель департамента информационных технологий ООО "Обит" Кирилл Тимофеев. Однако, по его мнению, ключевой метрикой могут стать сертификаты Федеральной службы по техническому и экспортному контролю, подтвержденные отраслевые внедрения, информация о статусе последнего обновления продукта и открытость/закрытость API.

"Если софт долгое время не обновляется, - рассказал он, - это ставит под сомнение его соответствие актуальным требованиям безопасности. Из-за отсутствия таких метрик в реестре, мы, будучи поставщиком ИТ-продукта и партнером целого ряда российских разработчиков, производим отбор этих решений в соответствии с бенчмарками, сформированными нами на реальных проектах".

Однако, по мнению CEO Security Vision Руслана Рахметова, не все так однозначно с метрикой наличия добавленного функционала. Он отметил, что в идеале российский продукт должен отличаться от решения Open Source на 100%, но это непростое дело - определить объем, необходимый для признания разработки российской.

Он отметил, что потенциальными метриками для реестра отечественного ПО могли бы стать проверки на совместимость с наиболее распространенными российскими операционными системами, системами управления базами данных, браузерами, процессорами, отсутствие зарубежных программных компонентов (модулей, библиотек), наличие у компании-разработчика

собственных или авторизованных центров обучения для корпоративных пользователей.

"Я считаю, что целесообразно рассмотреть введение балльной системы, - заметил Руслан Рахметов. - По аналогии с оценкой, применяемой для уровня локализации микроэлектроники и вычислительной техники. Начисление баллов за каждое из выполненных требований помогло бы диверсифицировать усилия российских разработчиков, а постепенное повышение проходного балла позволило бы планомерно увеличивать степень импортонезависимости отечественных программных продуктов".

Реестру нужны бенчмарки для оценки эффективности, масштабируемости, отказоустойчивости и других характеристик ИТ-разработок, а также ряд проверок программного обеспечения по стандартам OWASP, Clean Code и др. В идеале можно создать тестовый департамент, где опытные тестировщики будут разрабатывать и внедрять государственные стандарты качества для программного обеспечения и разработки, но как рейтинговую ознакомительную систему. Я уверен, что аудиты и постановка тестирования по стандарту были бы востребованы компаниями по всей стране и облегчили прохождение тендеров.

Авенир Воронов,
технический директор департамента логистика ГК «КОРУС Консалтинг»

Менеджер продуктов ООО "Инностейдж" Евгений Сурков обратил внимание, что дополнительные проверки на отсутствие недекларированных возможностей и наличие правильным образом реализованных функций защиты могут представлять ценность даже для "чистых" продуктов Open Source.

"Важно, чтобы эти проверки и функции не оставались на страницах отчетов, а стоимость "укрепленного" таким образом решения была адекватна и

соизмерима приносимой пользе с учетом закрытия рисков", - сказал Евгений Сурков.

Однако, по мнению Кирилла Семиона, менять нужно не условия, а процедуру добавления в реестр. Он считает, что в этот процесс можно включить проверку ПО на недекларированные возможности и уязвимости доверенной третьей стороной и дать разработчикам срок на устранение изъянов.

РАБОТА НАД ОШИБКАМИ

У экспертов нет единого мнения насчет продуктов, которые не подойдут под новые метрики, если последние будут приняты. Так, по словам сооснователя и заместителя генерального директора компании Postgres Professional, главы комитета по интеграции российского ПО Ассоциации разработчиков программных продуктов "Отечественный софт" Ивана Панченко, программное обеспечение, не соответствующее требованиям, нужно исключить из реестра.

Однако с ним не согласен его коллега по АРПП Руслан Рахметов. Он отметил, что большинство ответственных российских разработчиков непрерывно дорабатывают продукты и было бы разумно дать им время на приведение софта в соответствие новым метрикам.

"Переоценка уже внесенных в реестр решений на соответствие обновленным требованиям может проводиться с привлечением отраслевых ассоциаций, таких как АРПП "Отечественный софт", - отметил он.

С Русланом Рахметовым согласен **Авенир Воронов.** Он предложил провести аудит тех, кто не подойдет по новым метрикам, а результаты опубликовать напротив решений, чтобы разработчики знали, что им нужно исправить, а пользователи знали о потенциальных угрозах.

"Мы видим, что многие игроки рынка выступают за системную чистку реестра. Не так давно на законодательном уровне проходило обсуждения сортировки продуктов на предмет несовместимости с российскими ОС и СУБД. С продуктами, несоответствующими этим требованиям, возможны два варианта развития событий: либо их исключают из реестра, либо выделят время на доработку. Общий вывод очевиден: сегодня рынок находится на стадии перестраивания, систематизации и консолидации", - заключил Кирилл Тимофеев.