

ГОСПОДДЕРЖКА ЗАКУПОК ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: НУЖНА ИЛИ НЕТ ДЛЯ ОТРАСЛИ СИСТЕМ БЕЗОПАСНОСТИ?

Свирин Илья Сергеевич
к.т.н., член правления РАСПО

По данным Министерства связи и массовых коммуникаций Российской Федерации лишь 25% используемого в России программного обеспечения является отечественным! Однако, это картина по IT-отрасли в целом. Попробуем разобраться, что происходит на российском рынке программного обеспечения систем безопасности, какова реальная расстановка сил и изменит ли что-то законодательное регулирование в сфере государственных закупок ПО.

Развитие отрасли цифровых систем безопасности в России началось в конце 1990-х – начале 2000-х и, в принципе, совпало с наметившейся в мире тенденцией перехода с аналогового видеонаблюдения на цифровое. У истоков российского ПО для систем видеонаблюдения стоят такие компании, как DSSL (Trassir), Нордавинд (ТелеВизард), КомКом (Ewclid) и ряд других имен, многие из которых уже ничего не скажут современным специалистам в области систем безопасности. Таким образом, говорить про какое-то серьезное временное отставание в развитии нашей отрасли систем безопасности от зарубежных аналогов не приходится. Однако отставание все-таки есть, и связано оно с фундаментальными различиями в целеполагании – изначальная направленность зарубежных продуктов на мировой рынок и существенные инвестиции позволили обеспечить большее количество инсталляций, больше обратной связи, а следовательно, более качественный и функциональный продукт на выходе за то же время, которое потребовалось российским продуктам, сменяя друг друга на российском же рынке, чтобы выйти на качественно средний по мировым меркам уровень. В результате мы имеем ситуацию, когда доля российского ПО систем видеонаблюдения, не смотря на активные попытки мировой экспансии таких уважаемых компаний как ITV, Macroscop и ряда других, не превышает долей процента в сравнении с мировыми гигантами видеонаблюдения, такими как Milestone Systems, NICE и др.

Кардинально иную структуру рынка мы видим в России, где подавляющее большинство объектов оборудовано отечественными системами безопасности: ITV (Интел-

лект, AxxonNext), Девлайн (Линия), АРМО-Системы (SmartStation), Macroscop, Trassir (DSSL), VideoNet (Skyros), ISS (SecurOS) и др. Однако при ближайшем рассмотрении оказывается, что это, как правило, малые и средние объекты, а большие системы все равно строятся на зарубежных продуктах, как правило, Milestone. В контексте наметившегося в последние годы тренда к импортозамещению российские разработчики и производители серьезно нацелены «заменить» иностранные аналоги собственными разработками и в этом сегменте. Чтобы разобраться, насколько оправданы эти ожидания и какого эффекта в отрасли систем безопасности можно ожидать от новых законодательных инициатив, попробуем разобраться в том, в чем собственно будет состоять поддержка и защита российского производителя, а самое главное, какие базовые цели лежат в ее основе.

1 июля 2015 года Президент России В.В. Путин подписал закон о предоставлении преференций российским разработчикам программного обеспечения при государственных закупках. Данный закон по сути является рамочным и скорее обозначает твердое намерение обратить внимание на российских разработчиков, нежели прописывает конкретный алгоритм осуществления их поддержки. Важным инструментом исполнения этого закона является запуск реестра отечественного программного обеспечения, который планируется ввести с 1 января 2016 года. Надо отдать должное Ассоциации разработчиков программных продуктов (АРПП) «Отечественный софт» и лично исполнительному директору ассоциации Евгению Василенко, усилиями которых эта инициатива все же обрела законодательную форму!

Предполагается, что в реестр войдут продукты, соответствующие набору критериев, определенных Постановлением правительства РФ. Важным аспектом является то, что государство не планирует монополизировать экспертизу в части включения или не включения того или иного продукта в реестр, оставив за собой лишь роль регулятора процесса. Экспертиза продуктов будет возложена на экспертный совет при Министерстве связи и массовых коммуникаций России, куда в свою очередь войдут представители всех заинтересованных сторон, в т.ч. ведомств, научных организаций, институтов развития и, конечно же, разработчиков отечественного программного обеспечения. Справедливости ради, надо отметить, что разработчики отечественных систем безопасности не стоят в очередь на вхождение в экспертный совет и не принимают какого-либо заметного участия в процессах формирования реестра. Почему? Может быть, пока еще не знают о том, что идет такая работа? А может быть, понимают, что в нашей отрасли не требуется такого рода законодательного регулирования.

Все продукты в реестре будут сгруппированы по классам, а при осуществлении закупки заказчик должен будет указать конкретный класс, которому принадлежит закупаемое ПО. Если оказывается, что под требованием заказчика подходит хотя бы одно российское решение, иностранные продукты не участвуют в тендере. Приведу выписку из проекта постановления Правительства РФ «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»:

В целях защиты внутреннего рынка Российской Федерации, развития национальной экономики, поддержки российских товаропроизводителей установить запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд, за исключением следующих случаев:

а) если в реестре отсутствуют сведения о программном обеспечении, соответствующем тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке;

б) если программное обеспечение, сведения о котором включены в реестр и которое соответствует тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке, по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке программному обеспечению;

в) если исключительное право на программное обеспечение, планируемое к закупке, принадлежит российской органи-

зации, и сведения о таком программном обеспечении и (или) о закупке составляют государственную тайну.

Следует понимать, что классификатор реестра будет охватывать всю IT-отрасль, поэтому не надо ожидать, что продукты систем обеспечения безопасности будут детально и подробно структурированы. Может показаться, что это не позволит должным образом дифференцировать представленные на российском рынке отечественные продукты, найдя свою нишу для каждого из них, однако если отталкиваться от глобальной задачи введения реестра, направленную на ограничения закупки иностранного софта, более логичным выглядит подход, когда классификатор формирует максимально общие группы, не давая возможности «манипулирования» классами при осуществлении закупки, когда может быть указан близкий по смыслу класс, содержащий наименее слабых российских конкурентов для максимально простой аргументации необходимости закупки зарубежного программного обеспечения.

Какой же можно сделать вывод из написанного выше? Сегодня российский рынок систем безопасности достаточно сбалансирован, а права отечественных производителей в большинстве своем не ущемляются, как это происходит во многих других IT-сегментах, как антивирусное ПО, офисные средства, базы данных и др. Отечественный софт видеонаблюдения установлен почти везде, где он проходит по тактико-техническим характеристикам, а конкуренция идет, как правило, между различными отечественными же производителями. Это объясняется тем, что заказчики хотят получать быструю техническую поддержку на родном языке, а это на сегодня могут предложить только отечественные производители, в то время как иностранные компании концентрируются в российских представительствах в основном маркетинговые ресурсы, пуская техническую поддержку «по большому кругу» через зарубежные RnD-офисы. Санкционные прецеденты, связанные, как правило, с ограничениями поставок на территории Республики Крым и Севастополя, носят эпизодический несистемный характер и, скорее всего, временны. Это означает, что какое-либо дополнительное законодательное регулирование не только никак не изменит расстановку сил на российском рынке систем обеспечения безопасности, но и может иметь негативные последствия – именно конкуренция является основным драйвером развития, а конкурировать надо с теми, кто объективно лучше, а не с себе подобными. Будущее несомненно за теми компаниями, которые пытаются найти место своим продуктам на сложном и высококонкурентном мировом рынке, а не ищут лазейки в законодательстве, чтобы обосновать применение своего продукта взамен более качественного зарубежного!

РОССИЙСКАЯ АССОЦИАЦИЯ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (РАСПО)

*Источник –
официальный сайт
Ассоциации
<http://www.raspo.ru>*

Ассоциация создана в 2010 году при активной поддержке Министерства связи и массовых коммуникаций Российской Федерации. Миссией РАСПО ее участники объявляют содействие разработке, внедрению и популяризации свободного программного обеспечения (СПО) в России, развитие отечественной индустрии программного обеспечения, основанного на открытом исходном коде и свободных лицензиях, и ее вхождение в мировой рынок разработки программного обеспечения.

Участники Ассоциации считают, что развитие сегмента свободного программного обеспечения необходимо как для устойчивого развития рынка информационно-коммуникационных технологий, так и для создания полноценного информационного общества, в котором все его члены имеют возможность свободного доступа к передовым технологиям.

РАСПО действует в интересах всех потенциально вовлеченных в процесс использования СПО лиц и организаций – занимается активным продвижением и популяризацией СПО всеми доступными средствами и во всех возможных форматах: организует конференции, конкурсы, практикумы, интервью, социальные сети, специализированные вебсайты, образовательные программы для школ и ВУЗов.