

АЛЕКСЕЙ ЛУКАЦКИЙ:
**«СТОПРОЦЕНТНОГО ИМПОРТОЗАМЕЩЕНИЯ СЕГОДНЯ
ДОСТИЧЬ НЕЛЬЗЯ НИ В ОДНОМ ИЗ СЕГМЕНТОВ РЫНКА»**



*Алексей Викторович Лукацкий,
Консультант по безопасности бизнеса Cisco Systems*

Меры, направленные на поддержку разработчиков отечественной ИБ отрасли разрабатывались и предлагались и прежде, однако в нынешнем году эта задача вышла на новый уровень. Вместе с тем, сегодняшняя экономическая, рыночная и международно-политическая конъюнктура существенно осложняют эту и без того нетривиальную задачу. «Пульс кибермира» обсудил перспективы импортозамещения в отрасли информационной безопасности (ИБ), реалистичность поставленных целей и вызовы для иностранных компаний, работающих на этом рынке в России, с консультантом по безопасности бизнеса Cisco Systems Алексеем Лукацким.

ПУЛЬС КИБЕРМИРА: *В каких критических сегментах российского ИБ-рынка, на Ваш взгляд, возможно выстроить и эффективно воплотить стратегию импортозамещения? Существуют ли сегменты рынка ИБ в России, в которых эффективное импортозамещение не представляется возможным на данный момент?*

ЛУКАЦКИЙ: Если говорить о стопроцентном импортозамещении, то его сегодня достичь нельзя ни в одном из сегментов рынка, включая и критические для национальной безопасности. Так уж сложилось, что весь мир давно уже живет в условиях глобализации и выстраивания цепочек поставок различных электронных и ИТ-компонентов из разных стран мира. В одночасье повернуть эти процессы вспять невозможно. Я боюсь, что и за 10 лет это сделать нельзя. Хотя бы по причине отсутствия у нас массового производства собственных процессоров; подчеркиваю, массового. Без собственной элементной базы

говорить об эффективном импортозамещении не приходится. Если же посмотреть в будущее, то я бы ограничился только теми сферами, которые действительно критичны для обороны страны и национальной безопасности – это преимущественно ВПК. В остальных секторах проблема импортозамещения не так остра.

ПУЛЬС КИБЕРМИРА: *Как Cisco Systems оценивает курс на импортозамещение в сфере ИТ в России с учетом собственных бизнес-интересов на российском рынке? Как меняется стратегия Cisco на рынке РФ с учетом общего курса на импортозамещение в сфере ИТ и ИБ? Могут ли зарубежные компании с выгодой для себя участвовать в реализации стратегии импортозамещения на ее отдельных этапах?*

ЛУКАЦКИЙ: Несколько лет назад мы взяли курс на создание в России центров разработки и локального производства своей продукции. За последние годы нам удалось начать производство в России целого спектра наших решений – первой ласточкой стал VPN-модуль, сертифицированный в ФСБ. Затем были точки беспроводного доступа, IP-телефоны, IP-приставки для цифрового телевидения, маршрутизаторы и т.п. И наши планы на этом не прекращаются – мы планируем развивать локальное производство оборудования Cisco на территории России и, там, где необходимо, проводить его оценку соответствия требованиям российских регуляторов в области безопасности – ФСТЭК России, ФСБ России и др. Однако говорить о выгодах, как и о конкретных шагах взятого на импортозамещение курса, пока рано – официально критериев признания продукции отечественной пока нет. Как только они будут утверждены и в отечественное законодательство будут внесены соответствующие поправки, обязывающие приобретать именно локальные продукты, тогда и мы сможем учесть эти новые требования в своих планах по локальному производству.

ПУЛЬС КИБЕРМИРА: *Каков ежегодный объем государственной поддержки, требуемый, по Вашей оценке, для решения ключевых задач по импортозамещению для российской отрасли ИБ? Какие финансовые, в том числе налоговые механизмы наиболее востребованы для решения задач импортозамещения в различных нишах рынка информационной безопасности?*

ЛУКАЦКИЙ: На мой взгляд, в текущих условиях говорить о серьезных инвестициях в развитие данной отрасли не приходится. Рост курса доллара, снижение цен на нефть, определенная нестабильность в экономике заставляют государство помогать другим сферам экономики и выполнять социальные обязательства. Вот когда ситуация утрясется, можно будет говорить и о мерах поддержки отечественной отрасли ИБ. Такие меры уже разрабатывались не раз. И в середине 90-х годов российские ученые готовили целый план поддержки индустрии российских разработчиков средств защиты информации. Вторая попытка была совсем недавно, - на площадке Совета Федерации, при разработке проекта Стратегии кибербезопасности России предусматривались и меры поддержки отечественных ИБ-разработчиков. Но, к сожалению, данная работа по ряду причин была свернута. А ведь там речь шла и о налоговых льготах, госзаказе, преференциях в рамках госконтрактов и т.п.

ПУЛЬС КИБЕРМИРА: *Реалистично ли в краткосрочной и среднесрочной перспективе создание российской полной линейки сетевого программно-аппаратного обеспечения, не уступающего зарубежным аналогам по уровню надежности и обеспечения информационной безопасности? Если да, что для этого потребуется?*

ЛУКАЦКИЙ: Увы, даже в среднесрочной перспективе это невозможно. Мы слишком отстали от лидеров ИТ/ИБ-рынка. Для устранения разрыва, а то и захвата лидирующих позиций, мы должны семимильными шагами возрождать научную школу и производственную базу, которые и лежат в основе собственной отрасли ИБ. Затем понадобится немалое количество высококлассных специалистов. Все это требует немало финансовых и, конечно же, временных ресурсов. Можно пойти по китайскому сценарию – копированию чужих технологий, но не уверен, что Россия к этому сейчас готова. Слишком высоки репутационные риски и последствия от их принятия.

ПУЛЬС КИБЕРМИРА: *В качестве одной из возможных стратегий в русле курса на импортозамещение в сфере ИТ часто упоминается создание отечественных разработок на основе ПО с открытым кодом (Open-Source Software). Как такая стратегия соотносится с обеспечением ИБ, и достаточно ли она учитывает угрозы, связанные с возможными уязвимостями такого ПО?*

ЛУКАЦКИЙ: Эксперты, включая и специалистов ФСБ и ФСТЭК, уже не раз заявляли, что наличие исходных кодов практически ничего не дает с точки зрения оценки защищенности продукта. Сегодня многие производители и так готовы предоставлять исходные коды на свою продукцию, чтобы получить заветные сертификаты, открывающие двери многих компаний и предприятий. Поэтому у решений open source нет преимуществ перед проприетарными технологиями с точки зрения ИБ. А вот недостатков гораздо больше – неконтролируемый процесс разработки и внесения изменений, множество непонятных участников, отсутствие документации и комментариев в коде... Все это мешает обеспечивать безопасности ПО, построенного по принципу open source.

ПУЛЬС КИБЕРМИРА: *Обладают ли перспективные российских импортозамещающие ИБ-разработки шансами на продвижение на международных рынках? Если да, то в каких нишах (гражданская криптография, защищенное сетевое оборудование, антивирусы?) и какова география перспективных рынков?*

ЛУКАЦКИЙ: При текущем драконовском законодательстве в области криптография наши технологии (даже гражданские) мало кому интересны. А если эти узы контроля со стороны ФСБ ослабить, то мы наткнемся на нежелание отдельных западных стран допускать Россию со своими криптоалгоритмами в святая святых – финансы и телекоммуникации. Попытки продвигать наши криптографические решения в арабские страны, Индию и Китай пока тоже не увенчались успехом – они хотят иметь свою криптографию, не боясь закладок отечественных спецслужб (все спецслужбы одинаковы во всем мире). А вот у других защитных технологий есть все шансы для выхода на международную арену. Например, антивирусы (продукция Лаборатории Касперского известна во всем мире), сканеры защищенности (тут страну представляет отечественная

Positive Technologies), средства защиты Web (в этом сегменте недавно вышел отечественный стартап *Wallarm*). Все они работают как на Востоке, так и на Западе от России. Но пока активному продвижению наших технологий по миру мешает текущая геополитическая ситуация.

24.12.2014