PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
СЕНТЯБРЬ • 2014 • МОСКВА
http://www.pcweek.ru

Импортозамещение и российский рынок ИБ

ВАЛЕРИЙ ВАСИЛЬЕВ

На фоне международных интеграционных процессов в экономике и политике все резче стало обозначаться противостояние стран в киберпространстве. Фактически туда сместился центр тяжести экономической конкуренции и задач информационной безопасности, актуальных как для отдельных компаний, так и для целых стран и межгосударственных союзов.

ОБЗОРЫ

Начавшиеся процессы стимулируют пересмотр сложившихся к началу XXI века международных экономических и политических связей, упразднение ранее эффективно действовавших межнациональных политических и бизнес-структур и попытки выстраивания иных, их функционально замещающих, политизацию направления информационной безопасности (ИБ).

Одной из важнейших мер, принимаемых государственным руководством России в ответ на изменение международной ситуации, является стратегия импортозамещения, в рамках которой среди прочего стартуют крупнейшие национальные проекты вроде построения Национальной платежной системы или недавно заявленной новой глобальной системы персональной космической связи военного и правительственного назначения.

К обсуждению возможных последствий влияния этой стратегии на российский рынок ИБ мы привлекли представителей компаний, занимающих активные позиции в различных сегментах российского рынка ИБ, специалистов, связанных с разработкой передовых ИБ-технологий. К сожалению, среди откликнувшихся на наше предложение не оказалось ни одного эксперта из иностранных компаний, работающих на российском рынке ИБ. Однако из предшествующего общения с ними ясно, что при настоящем положении дел эти компании в качестве адекватной реакции на импортозамещение видят для себя развитие локального производства и разработок в России и ожидание дальнейших ясных заявлений и действий со стороны руководства нашей страны в этом направлении.

Импортная и национальная составляющие рынка ИБ

На фоне общей сложной экономической и политической ситуации в стране и мире российский рынок ИБ, согласно данным компании IDC, ощущает себя лучше многих других, демонстрируя по итогам 2013 г. рост на 4,2% при годовом объеме примерно в 413 млн. долл. При этом среди наиболее активных игроков этого рынка много иностранных компаний, доля которых в общем объеме весома.

Проведенный нашим изданием онлайн-опрос с участием компаний разного масштаба подтвердил, что стратегия импортозамещения активизируется в нашей стране в условиях доминирования импортных ИБ-продуктов. Однако это доминирование не является подавляющим. Так, среди компаний, принявших участие в онлайн-опросе, только 38% используют для организации корпоративной ИБ преимущественно иностранные продукты и сервисы; тех, у кого преобладают отечественные, — 11%; а паритетно сочетающих те и другие — 35%.

Среди мотивов, побуждающих российские корпоративные структуры применять зарубежные ИБ-продукты, 54% участников опроса назвали отсутствие российских аналогов, 40% — их низкое качество, 27% — плохую техническую поддержку, а 11% — их высокую стоимость.

При этом онлайн-опрос показал явное преобладание использования российских разработок в таких критически важных областях, как антивирусная защита (68%), электронная подпись (60%), шифрование данных при хранении и передаче (32%).

Заметную конкуренцию российские продукты составляют импортным в управлении пользовательским доступом (32% респондентов используют российские решения, 54% — импортные); межсетевом экранировании (38% против 68%); VPN (30% против 43%); обнаружении и предотвращении вторжений (32% против 35%).

В итоге проблему импортозамещения актуальной, но только в госструктурах и на отраслеобразующих предприятиях, считают 35% респондентов; актуальной безотносительно к сегменту использования — 24%; не считают ее актуальной вообще — 27%.

Свои оценки привели и наши эксперты. Исходя из практического опыта, заместитель руководителя Центра компетенций информационной безопасности компании "АйТи" Аркадий Прокудин заключает, что среди средств защиты информации (СЗИ), подпадающих под российское регулирование, 80—85% являются отечественными, а среди СЗИ, не подпадающих под российское регулирование, отечественных уже только 30%; в государственных организациях и предприятиях доля национальных СЗИ достигает 70% (отмечу, что, по данным компании "Код безопасности" за 2013 г., в закупках крупных госзаказчиков доля ИБ-продуктов российского производства составила более 90%), в то время как в коммерческих их только 20%.

Александр Мормуш, руководитель направления ИБ дистрибьюторской компании Treolan, оценил долю продуктов и построенных на них решений, представленных иностранными ИБ-производителями, как доминирующую: в программном обеспечении она составляет не менее 65% и около 90% в аппаратной части СЗИ. Вместе с этим он отметил лидирующее положение отечественных разработок в таких ИБ-направлениях, как антивирусная защита, системы защиты от утечек данных, системы анализа защищенности, что объясняется более глубоким пониманием российскими специалистами особенностей локального рынка.

Схожее мнение высказал и управляющий директор "Лаборатории Касперского" в России, странах Закавказья и Средней Азии Сергей Земков. В качестве конкурентного преимущества отечественных разработчиков от отмечает то, что они делают узконаправленные решения с высоким качеством исполнения, в то время как более широкая продуктовая линейка крупных иностранных производителей, как правило, позволяет закрыть одним решением несколько задач, но при этом их продукты не отличаются столь же глубокой проработкой, как российские.

Руководитель отдела информационной безопасности системного интегратора IBS Platformix Джабраил Матиев объяснил сложившееся разделение российского ИБ-рынка между иностранными и отечественными ИБ-вендорами и ИБ-провайдерами его реалиями. С одной стороны, из-за сильной зарегулированности рынка отечественные разработки имеют более высокие уровни сертификации, с другой — зарубежным решениям присущи лучшие современные механизмы защиты и меньшая стоимость при равной производительности. По этим же причинам есть технологические и продуктовые ниши, где позиции российских производителей неизменно сильны или же они просто вне конкуренции. Это шифрование данных, модули доверенной загрузки, СЗИ от несанкционированного доступа.

В целом, подчеркнул Сергей Котов, эксперт по информационной безопасности компании "Аладдин Р.Д.", соотношение импортной и национальной (к ней он предлагает относить всю ту продукцию, которая создается и распространяется под российской юрисдикцией) составляющих в области ИБ адекватно уровню технологического развития страны. Поскольку развитие ИБ неразрывно связано с развитием информационных технологий, которые сегодня пронизывают все области человеческой деятельности, то именно здесь он видит основную проблему: отставание в ИТ ведет к глубокому проникновению иностранных технологий и продуктов на наш рынок, что существенно усложняет задачи ИБ.

ИБ-сегменты, перспективные для импортозамещения

Заместить на отечественное можно все, полагает г-н Котов, осторожно оговаривая при этом необходимые для этого средства и сроки. Одной из самых насущных задач он считает производство элементной ИКТ-базы. Усилия, направленные на ее решение, как он считает, уже видны. Если программы, принятые правительством, сработают в установленные сроки, то часть проблемы, по его оценкам, будет решена к 2020 г. Однако, не рассчитывая на быстрый положительный результат, он как временную меру предлагает замещение импортного на импортное же, не поясняя, однако, как из нескольких зол выбирать меньшее, особенно в условиях выбора, ограниченного экономическими санкциями против нашей страны.

По мнению г-на Земкова, стимулировать переход на отечественные продукты нужно в тех направлениях, где наши компании традиционно сильны, в первую очередь — это разработка ПО. Отечественная школа программирования, как он отметил, признана во всем мире, у нас есть сильные компании практически во всех сегментах, имеющих отношение к разработке ПО: от ERP-систем до специализированных приложений САПР. Там, где мы отстаем от иностранных компаний, как, например, в области аппаратного обеспечения, наши компании должны, по его мнению, работать в сотрудничестве с мировыми лидерами, а там, где это необходимо (например, в критически важных инфраструктурах или в защите информации ограниченного доступа), диктовать правила использования отечественных и импортных продуктов через институции лицензирования и сертификации.

ПРОДОЛЖЕНИЕ НА С. 18 ▸

Наши эксперты

АНДРЕЙ ГОЛОВ, *генеральный директор, "Код Безопасности"*

СЕРГЕЙ ЗЕМКОВ, *управляющий директор, "Лаборатория Касперского" в России, странах Закавказья и Средней Азии*

СЕРГЕЙ КОТОВ, *эксперт по информационной безопасности, "Аладдин Р.Д."*

ВАЛЕНТИН КРОХИН, *заместитель директора Центра информационной безопасности, "Инфосистемы Джет"*

ДЖАБРАИЛ МАТИЕВ, *руководитель отдела информационной безопасности, IBS Platformix*

АЛЕКСАНДР МОРМУШ, *руководитель направления ИБ, Treolan*

АРКАДИЙ ПРОКУДИН, *заместитель руководителя Центра компетенций информационной безопасности, "АйТи"*

ВЛАДИМИР ШИБАНОВ, *старший вице-президент, "Аквариус"*

Российский рынок сертифицированных СЗИ для ОС GNU/Linux

ОКСАНА УЛЬЯНИНКОВА

На рынке не утихают споры о том, что будет означать для России курс на импортозамещение в сфере информационных технологий (ИТ) и какой путь самый быстрый и безболезненный — перевод информационных систем на СПО (свободное программное обеспечение) или создание собственной ОС на базе все тех же дистрибутивов Linux, способной заменить продукцию зарубежных вендоров.

При этом задолго до введения санкций в области ИТ перспективы использования СПО в России были подкреплены планом на 2011—2015 годы по переходу федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование СПО, который был утвержден распоряжением Правительства от 17 декабря 2010 г. № 2299-р за подписью Владимира Путина. Однако с момента принятия этого курса информации о внедрении СПО в госорганы было крайне мало, в основном это были точечные проекты в регионах.

Главным препятствием для полноценной реализации планов по переходу на СПО в первую очередь являются недостаток квалифицированных кадров для внедрения и обслуживания таких систем, а также опасения, связанные с использованием "сложного и незнакомого" ПО. По сути, эти факторы актуальны не только для России, но и для других стран.

Также в соответствии с действующим законодательством при обработке персональных данных, государственной тайны и другой конфиденциальной информации должны использоваться сертифицированные средства защиты информации (СЗИ). Таким образом, возможный переход органов исполнительной власти на использование Linux создаст дополнительный стимул для развития рынка сертифицированных СЗИ для новой платформы.

Вместе с тем на российском рынке уже существуют локализированные дистрибутивы Linux со встроенными программными СЗИ, сертифицированными ФСТЭК России. Это системы ALT Linux СПТ, Astra Linux SE, ROSA, Mandriva Linux, GosLinux и др. Однако наличие встроенных механизмов защиты в дистрибутиве не означает, что нужно отказаться от применения дополнительных СЗИ, даже если они дублируют какие-либо возможности защитных подсистем. Для этого есть ряд объективных причин, связанных не только с возможными архитектурными недостатками и ошибками программирования, но и с наличием определенных ограничений, которые появляются при использовании специализированных дистрибутивов. Среди таких ограничений стоит выделить потерю гибкости системы ввиду невозможности изменения конфигурации и состава файлов из комплекта поставки после фиксации набора файлов при сертификации дистрибутива. Таким образом, пока издатель не сертифицирует обновления, их нельзя применять, что влияет и на степень надежности ОС. Также к невозможности аттестации объекта информации приводит установка приложения, вносящего изменения в общесистемное программное обеспечение. С другой стороны, наложенное СЗИ дает не только свободу при выборе дистрибутива и возможность расширения функционала ОС, но и наиболее полное выполнение мер, определяемых, в частности, приказами №№ 21, 17 и 31 ФСТЭК России. Наличие дополнительных защитных механизмов и функционала для управления системой защиты, напротив, значительно повышает уровень защищенности информационной системы.

Рассмотрим более подробно, что предлагает сегодня российский рынок сертифицированных средств защиты для ОС Linux.

Средства антивирусной защиты

В этой категории традиционно присутствуют два российских разработчика — "Лаборатория Касперского" и "Доктор Веб" с сертифицированными по линии ФСТЭК и ФСБ России антивирусными решениями.

Средства аутентификации

Здесь рынок делят семейства идентификаторов Рутокен и eToken.

Межсетевые экраны и средства организации VPN-соединений

В этом сегменте присутствуют как лидеры рынка — надежные и проверенные решения, так и решения, которые имеют узкий круг заказчиков:

- АПКШ "Континент"/СКЗИ "Континент-АП" для ОС Linux (находится на сертификации)
- ViPNet Coordinator для Linux
- VPN/FW "ЗАСТАВА"
- ПАК "РУБИКОН"
- Программный комплекс "FORT"

Криптографическая защита данных

- КриптоПро CSP

Аппаратно-программные модули доверенной загрузки

Все представленные на рынке АПМДЗ различаются списком поддерживаемых ОС Linux и файловых систем.

- ПАК "Соболь"
- МДЗ-Эшелон
- ПАК "Аккорд-АМДЗ"
- ALTELL TRUST
- АПМДЗ "Максим-М1"

Средства защиты информации от несанкционированного доступа

Российский рынок предлагает два решения:

- СЗИ от НСД Secret Net LSP
- ПАК "Аккорд-X"

Если первое решение программное и имеет модульную архитектуру, то второе представляет собой программно-аппаратное решение, состоящее из АПМДЗ и программного обеспечения для разграничения доступа.

Очевидно, что сертифицированных средств защиты, предназначенных для ОС Linux, отнюдь не такое большое количество, как для ОС Windows. Связано это с незначительным распространением СПО и малым числом специалистов, ориентирующихся на эту платформу, а в ряде случаев и с технологической сложностью реализации того или иного защитного функционала. Кроме того, список поддерживаемых ОС Linux у каждого производителя свой, что создает определенные трудности для создания эшелонированной комплексной системы защиты.

В настоящий момент нет четкого понимания того, что и как будет внедряться в федеральных органах. Однако "движение" законодательной базы и текущие инициативы государства должны вызвать увеличение спроса на СПО среди российских госструктур. Государство является крупнейшим пользователем ИТ, поэтому и перспективы внедрения СПО в этом сегменте довольно масштабны. Все эти факторы, несомненно, будут стимулировать развитие рынка сертифицированных средств защиты информации для ОС GNU/Linux.

Автор статьи — менеджер по продукту компании "Код Безопасности".

Импорто...

◂ ПРОДОЛЖЕНИЕ СО С. 17

Аркадий Прокудин напомнил, что в стране наряду с ПО производятся также качественные программно-аппаратные решения: сканеры поиска и анализа уязвимостей, VPN, средства защиты от несанкционированного доступа, межсетевого экранирования, управления пользовательским доступом, контроля утечек данных, поддержки электронной подписи. В то же время он отметил наше сильное отставание в системах предотвращения вторжений, в межсетевом экранировании и обнаружении вторжений на уровне приложений, элементной базе для сетевого оборудования.

Перечень наших слабых позиций г-н Мормуш дополнил системами управления ИБ-событиями и ИБ-информацией (SIEM), управления рисками (GRC), контроля конечных пользователей и высказал сомнение в возможности быстро заменить на отечественные аналоги большую часть зарубежных ИБ-решений с этим функционалом. По его оценкам, на данный момент отечественные разработки в части ИБ способны покрыть примерно половину функционального спектра ИБ.

По мнению г-на Матиева, на отечественные ИБ-продукты целесообразно перевести государственный сектор, который должен стать примером и драйвером развития отечественных разработок в области ИБ. Вмешиваться же в коммерческий сектор, по его мнению, неразумно, так как это прямой путь к разрушению механизма конкуренции.

Чтобы составить иностранным компаниям достойную конкуренцию на внутреннем рынке, российские разработчики, полагает Андрей Голов, генеральный директор компании "Код Безопасности", нуждаются в инвестициях и времени (в некоторых направлениях счет идет на годы), а не в знаниях и компетенциях. Критичными в организации ИБ он считает пограничные участки между механизмами обеспечения безопасности и управления ею, т. е. те, где появляется новая информация высокой ценности. Переход на российские решения для этих областей, считает он, следует стимулировать в первую очередь, поскольку от них критично зависит безопасность данных и бизнес-процессов. В то же время, по его мнению, недопустимо форсировать импортозамещение в критически важных системах, таких как АСУ ТП, где наряду с ИБ важны такие свойства, как отказоустойчивость и доступность: иностранные разработки для АСУ ТП гораздо качественнее отечественных (которые к тому же охватывают здесь далеко не весь спектр потребностей).

Возможным направлением развития импортозамещения может также стать укрепление связей между неконкурирующими между собой производителями, работающими в смежных областях. Такие альянсы позволят разрабатывать качественно новые классы продуктов.

Плюсы и минусы

Импортозамещение и во многом стимулирующие этот процесс экономические санкции, принятые ведущими экономиками мира против России, неизбежно сказываются на конкретных игроках российского ИБ-рынка. Уже наблюдается снижение долей некоторых иностранных вендоров в различных сегментах ИБ. Подтверждая неполную зависимость нашего рынка от импорта и упомянутую г-ном Котовым возможность совершать маневры в поисках альтернативных поставщиков, на освободившиеся ниши спроса слетаются конкуренты как из числа иностранных (но более лояльных на данное время), так и из среды российских разработчиков, которым импортозамещение открывает зеленую улицу.

По мнению г-на Земкова, импортозамещение может дать положительный экономический результат ИБ-рынку в целом и отдельным российским компаниям, работающим на нем. Однако, отметил он, большая часть российских компаний-разработчиков, как правило, не имеет достаточно средств, чтобы, даже обладая хорошими продуктами, противостоять в маркетинге и ценовой борьбе с представленными в России крупными международными компаниями.

У г-на Прокудина на этот счет есть свои рекомендации по схеме перехода на российские ИБ-продукты. По его мнению, процесс можно организовать двумя путями: принудительно и через снижение цен, повышение качества продукции и технической поддержки. Сделать отечественные продукты дешевле зарубежных, сохранив производителям доходность, можно за счет государственных компенсаций (одновременно введя жесткий контроль за использованием преференций). Государство также в силах поднять пошлины на импорт до такого уровня, чтобы зарубежные продукты оказались заметно дороже отечественных.

Заместитель директора Центра информационной безопасности компании "Инфосистемы Джет" Валентин Крохин предложил стимулировать переход на отечественные продукты сразу во всех сегментах ИБ, поддерживая г-на Прокудина в идее предоставления преференций отечественным разработчикам, т. е. в вытеснении иностранных конкурентов рыночными и административными механизмами.

Г-н Крохин считает общей проблемой всех отечественных разработчиков недостаточную ориентированность на массовый рынок, что обусловливает средний уровень качества их продуктов. Поэтому под стимулированием отечественных вендоров он понимает прежде всего подталкивание их к улучшению качества, повышению конкурентоспособности за счет других аспектов (и не только на отечественном рынке).

На недостаточно высокое качество российских продуктов указывает и г-н Матиев. Перед запуском предлагаемых механизмов стимулирования отечественных вендоров он предлагает учесть, что российский потребитель за годы пребывания в рыночной экономике успел хорошо узнать технические возможности зарубежных ИБ-решений, уровень передового иностранного маркетинга и обслуживания клиентов. И хотя качество отечественных ИБ-продуктов за последние годы заметно выросло, оно все еще заметно ниже, чем у представленных в стране зарубежных. По мнению г-на Матиева, российские продукты находятся в стадии развития, то же самое можно сказать и о российском сервисе.

Корпоративная безопасность для частных компаний (особенно для средних и малых) слабо зависит от юрисдикции поставщика решений ИБ до тех пор, пока, как отметил г-н Котов, частный бизнес не начинает взаимодействовать с государственными заказчиками или государство не приходит к нему в лице регулятора. Поскольку это взаимодействие происходит все чаще, то граница между подходами к организации ИБ в госструктурах и в частных компаниях, по его мнению, размывается. А так как госсектор традиционно является самым крупным ИБ-потребителем в стране, то протекционизм российских ИБ-продуктов с его ▸

стороны как заказчика может стать положительным примером для заказчиков и из коммерческого сектора. То есть переход к импортозамещению должен, очевидно, осуществляться через госзакупки.

Об этом сказал также г-н Мормуш. Он предлагает сконцентрироваться на поддержке отечественных ИБ-разработчиков, сформулировать и зафиксировать преимущественное использование отечественных решений в государственном сегменте ИБ-потребления, т. е. применить в технологической политике государства аналог американского документа "The Buy American Act", в котором установлены ограничения на закупку решений иностранного происхождения в пользу национальных аналогов. Такая поддержка отечественного производителя придаст сильный импульс росту рынка, поскольку деньги, выделяемые на госзакупки, останутся внутри страны, их можно будет направить на создание новых рабочих мест и создание инновационных отечественных решений.

Вместе с тем, отметил г-н Крохин, импортозамещение длительный процесс, которым нужно управлять, а именно такого стратегического управления в стране пока не видно. В реализации стратегии импортозамещения эксперты отмечают немало организационных проблем, важнейшая из которых — отсутствие прозрачной для активных участников ИБ-рынка программы, они ожидают ее от руководства страны и отрасли.

Для нашего ИБ-рынка, по мнению г-на Крохина, важна открытая для его участников среднесрочная стратегия: все заинтересованные стороны должны понимать, что и в какие сроки предполагается делать, а практикуемая ныне смена парадигм (по нескольку раз в год) ведет только к тому, что ни один отечественный вендор не в состоянии сформировать нормальную стратегию собственного развития, без которой сложно говорить о качественных и конкурентных разработках.

Г-н Голов воспринимает тему импортозамещения как возможность сформулировать стоящие перед страной вопросы шире и острее: собираемся ли мы вообще заботиться о своей безопасности? Ведь государство, которое использует для решения задач ИБ ультрасовременные, но иностранные решения, не имеет контроля над этими средствами. Проблему он также видит еще и в том, что в стране, по его мнению, нет органа, который бы в целом отвечал за ее безопасность. Совет Безопасности РФ он рассматривает как исключительно консультативный орган, ФСТЭК и ФСБ отвечают за отдельные направления безопасности в рамках вполне конкретных и ограниченных полномочий. При этом у нас создается все больше новых критичных информационных систем, таких как электронное правительство, множественные ГИСы и ГАСы, обеспечение ИБ которых должно быть отнесено к первоочередным задачам.

Пример должной организации процессов в области ИБ он видит в организации антитеррористической деятельности; многие министерства и ведомства объединились для борьбы с этим явлением, создан национальный антитеррористический центр. А ведь возможный ущерб от современной компьютерной атаки на критически важные информационные системы может оказаться масштабнее даже, чем от теракта. Г-н Голов считает уместным основную активность в создании национального центра противодействия компьютерным атакам (не только со стороны киберзлоумышленников, но и со стороны стран-агрессоров) возложить на ФСБ России, которая занялась бы объединением ресурсов как государственных, так и коммерческих организаций, специализирующихся на вопросах ИБ, а также высококлассных экспертов.

Импортозамещение, протекционизм национального экспорта и международное разделение труда

Как сопрягается спровоцированная внешними санкциями эскалация импортозамещения с используемыми (с тем или иным успехом) в области ИБ протекционизмом национального экспорта и встраиванием в международное разделение труда?

По мнению г-на Земкова, это вовсе не разнонаправленные процессы. Импортозамещение и внутренняя поддержка российских компаний должны сопровождаться поддержкой экспорта отечественных продуктов. Государство обязано проводить планомерную работу по продвижению российских продуктов на международном рынке, рассматривать это как часть процесса обеспечения независимости от иностранных решений.

Протекционизм экспорта, отметил г-н Котов, это действующие международные правила, и, раз уж мы играем по общим правилам, не стоит от протекционизма отказываться, более того — он нам необходим.

Однако г-н Крохин скептически оценивает протекционистские усилия нашего государства в области ИБ-экспорта: если бы государство реально помогало в этом, констатирует он, наши разработчики имели бы все шансы стать заметными игроками на мировом ИБ-рынке. Однако, по его оценкам, экспорт в области ИБ был и остается либо организационно чрезмерно сложным, либо вообще запрещенным. Г-н Крохин надеется, что, возможно, в нынешних изменившихся условиях поддержка ИБ-экспорта наконец улучшится, что к тому же станет хорошим стимулом для улучшения качества ИБ-продуктов.

Г-н Котов согласен с тем, что нецелесообразно противопоставлять протекционизм экспорта импортозамещению. Однако у импортозамещения есть и свое предназначение — он жизненно необходимо нам там, где этого требуют задачи национальной безопасности, порой даже если их решение не вполне сообразуется с экономической целесообразностью, т. е. ради национальной безопасности нам, возможно, придется жертвовать своим экономическим благополучием.

В России, считает г-н Прокудин, предстоит создать среду, возможно, даже искусственную (нерыночную), ориентированную на многолетний внутренний протекционизм собственного производства широкого спектра ИБ-продуктов. Однако, преследуя цель развить масштабное национальное производство качественных продуктов (ведь никто не побежит завтра покупать товары абы какого качества только потому, что они российские), есть риск убить частное предпринимательство. Г-н Прокудин призывает всячески постараться избежать этого — ведь в немалой степени ради бизнеса как ИБ-потребителя это производство, собственно, и затевается.

Глобальное разделение труда в области безопасности, по мнению г-на Котова, пока вряд ли возможно. Зато нам необходимо искать локальных союзников. Задачу эту он считает непростой, но без ее решения экономически выдержать гонку за национальную безопасность будет очень сложно. С кем и по каким направлениям партнерствовать, а в чем полагаться только на себя, следует рассчитывать заранее.

Достойно встроиться в международное разделение труда непросто. Нужно понимать, что на международном рынке никто нас не ждет. К примеру, никто не пускает нашу вполне конкурентоспособную криптографию в "свой огород" — для некритичных вариантов давно применяются рыночные стандарты де-факто, а для критичных (таких как государственная тайна) — национальные стандарты шифрования.

Вот еще один яркий пример из области международного разделения труда от г-на Котова. Китай запрещает использование продуктов "Лаборатории Касперского" в своих госструктурах даже на фоне активно развивающегося партнерства с Россией. Что это со стороны Китая — протекционизм или импортозамещение? На взгляд г-на Котова, это обусловлено более чем десятилетним горизонтом планирования, предпринимаемого китайским руководством: пока не разобрались с движком иностранного антивируса, китайцы используют готовый продукт, а разберутся — уберут его со своего рынка.

В нынешней ситуации импортозамещение в области ИБ г-ну Голову видится более актуальной задачей, чем развитие экспорта и участие в международном разделении труда. Чтобы заниматься национальным экспортом, как он считает, нам требуются дополнительные мощности, которых у нас пока нет. При этом, конечно, не стоит забывать про, как он выражается, "дружественные" нам рынки, с которыми мы могли бы сотрудничать в области ИБ — это Латинская Америка и Юго-Восточная Азия. Для начала как первоочередную задачу он предлагает оформить информационную безопасность как самостоятельный сектор экономики — по его мнению, недостаточно того, что ИБ существует только как часть ИТ.

Старший вице-президент компании "Аквариус" Владимир Шибанов, напротив, не видит необходимости в подобных трасформациях ИБ-направления, он оценивает рынок ИБ в России как вполне сформировавшийся, со своими очевидными драйверами (основными из которых выступают регуляторы), со своими традиционными крупными заказчиками (в лице госструктур, которые, кстати, ориентируются благодаря регуляторам на российских производителей). Курс на дальнейшее импортозамещение в сфере ИБ с позиции национальных интересов, как он считает, должен способствовать укреплению технологического суверенитета страны.

Задача ИБ на национальном уровне, в представлении г-на Котова, должна быть сформулирована так: доведение максимально возможного числа рисков ИБ до приемлемого уровня при условии "неразорения" страны. С тем, какой уровень считать приемлемым, он предлагает разбираться отдельно в каждом конкретном случае, но все, что касается обороны и ИКТ-инфраструктуры, находится в зоне первоочередного внимания. Сегодняшние реалии, как ему видится, таковы, что в области ИБ мы вынуждены еще довольно долго искать заграничных партнеров с нужными компетенциями, одновременно учитывая политические реалии.

В заключение хочется сказать, что тем, кто в стране работает в области ИБ, предстоит заниматься и замещением импорта на внутреннем рынке, и продвижением своих решений на внешние рынки, и встраиваться в международное разделение труда, не забывая, что мир меняется и сегодняшние союзники и партнеры завтра могут перестать быть таковыми. При этом следует помнить, что Россия — не Китай и не Индия, емкость нашего внутреннего рынка несравнимо ниже, что неизбежно отражается на себестоимости российской продукции и, как следствие, на ее конкурентоспособности.

Те из российских разработчиков, которые это учитывают, должны стремиться создавать продукты, стандартизованные по международным критериям, к тому же адаптируемые к смежным международным стандартам, что позволит им получать конкурентные преимущества и расширять рынок сбыта.