2025/09/22 13:52:18

Алексей Комаров, УЦСБ — об импортозамещении в 2025 году. Что реально работает, а где пока остаются только обещания?

В каких технологических сегментах ИБ российские решения догнали западные аналоги, а где отставание сохраняется? Сколько времени еще понадобится, чтобы устранить разрыв в отстающих нишах, рассказывает Алексей Комаров, региональный представитель компании УЦСБ в Москве.

Алексей Комаров

«В России много сильных независимых разработок с применением оригинальных технологий.»

TADVISER: В каких нишах ИБ разрыв с западными решениями может быть преодолен в ближайшие 2–3 года, а где потребуется больше времени?

АЛЕКСЕЙ КОМАРОВ: Ситуация со степенью зрелости отечественных решений действительно неоднозначна. Традиционно сильные позиции у российских разработчиков антивирусов. Решения класса EDR (Endpoint Detection and Response) также демонстрируют достойный мировой уровень. Исторически конкурентоспособны и системы защиты данных от утечек (DLP): они хорошо адаптированы под языковые особенности и национальные законодательные требования, например, 152-ФЗ. В российских реалиях эти продукты не только не уступают западным аналогам, но и зачастую превосходят их.

За последние годы заметно выросло число разработок межсетевых экранов (NGFW) и платформ оркестрации и автоматизации реагирования (SOAR). Многие из решений уже готовы к успешной эксплуатации в организациях малого и среднего масштаба. Вместе с тем существуют и определенные объективные трудности, продиктованные недостаточностью опыта эксплуатации и ограниченной инсталляционной базой.

Так, российские SIEM (Security Information and Event Management) пока уступают признанным мировым лидерам, за плечами которых многолетнее преимущество в виде мощных движков корреляции, машинного обучения и наработанных словарей парсеров (нормализации событий) под тысячи устройств. Отечественным решениям порой не хватает глубины анализа и зрелости.

Сложность создания глобальных сетей сбора данных об угрозах наиболее остро сказывается на решениях по защите от целевых атак (APT) и сервисах данных о киберугрозах (Threat Intelligence). Необходимо время и международное присутствие — то, чем уже давно обладают западные вендоры.

В профессиональном сообществе при обсуждении импортозамещения регулярно упоминают трудности с решениями для крупнейших инфраструктур, где критична высокая производительность — важно для тех же NGFW и систем предотвращений вторжений (IPS).

Но важно понимать: ни один ИБ-продукт не может быть заменен на свой аналог «один в один»: неизбежно изменение самого подхода к построению комплексной системы ИБ, что, как ни странно, дает определенные преимущества. Как и в спорте: с грамотным тренером даже команда из игроков второго эшелона может заиграть не хуже именитого клуба, сплошь состоящего из звезд, за счет слаженности действий и продуманной стратегии.

TADVISER: Какие факторы тормозят процесс импортозамещения в ИБ?

АЛЕКСЕЙ КОМАРОВ: Условно приоритетные факторы можно расставить в таком порядке:

- **Кадры**: не хватает высококлассных разработчиков базового уровня, архитекторов сложных систем и специалистов по Data Science. Крупные ИТ-компании переманивают их зарплатами, которые зачастую не могут предложить ИБ-вендоры;
- **Слабая кооперация и фрагментация рынка**: вместо создания единых сильных экосистем часто видим множество небольших компаний, которые изобретают «свои велосипеды» и не хотят стандартизировать API для глубокой интеграции, что создает проблему «лоскутного одеяла» у Заказчиков;
- **Болезни роста:** многие разработчики, чьи продукты годами применялись в нишевых сегментах, столкнулись с необходимостью резко масштабироваться в десятки раз, да еще и в сжатые сроки. Это выявило проблемы с архитектурой, документацией и технической поддержкой на этапах как внедрения, так и последующей эксплуатации.

Финансирование, вопреки расхожему мнению, сейчас не главная проблема. Есть инвестиции и господдержка, в том числе косвенная, через ужесточение требований законодательства. Вопрос скорее в его эффективном применении.

TADVISER: Если бы вам дали «бюджет мечты» на развитие российских ИБ-решений, куда бы вы вложили средства в первую очередь?

АЛЕКСЕЙ КОМАРОВ: В соответствии с ключевыми трудностями было бы разумно инвестировать:

- **В людей:** тематические стипендии, гранты, финансирование лабораторий в вузах, создание привлекательных условий для привлечения лучших специалистов, включая обратную релокацию;
- **В открытые платформы:** финансирование создания открытых стандартов, протоколов и эталонных систем, которые могли бы стать основой для разработок многих вендоров, позволили бы избежать дублирования усилий и поднять уровень зрелости отрасли в целом;
- **В фундаментальные исследования:** вкладываться в создание не прикладных продуктов, а отечественных аналогов ключевых технологий: своих операционных систем, собственных процессоров и, как следствие, — средств защиты для них.

Неограниченность бюджета позволила бы сделать ставку на стратегические задачи с бóльшим сроком окупаемости (или вообще без таковой), но и с более долгосрочными позитивными эффектами.

TADVISER: В каких направлениях отечественные решения уже закрывают потребности Заказчиков, а где по-прежнему больше обещания?

АЛЕКСЕЙ КОМАРОВ: Российские DLP адаптированы под национальные требования и часто более гибкие. Отечественные антифрод-решения и защита от мошенничества в финтехе выглядят конкурентно в том числе и по мировым меркам. Нет существенных проблем и при внедрении базовых средств защиты (антивирусы, межсетевые экраны) для SMB и среднекорпоративного сегмента.

А вот единые платформы кибербезопасности — это часто попытка соединить разрозненные модули или продукты, которые слабо интегрированы между собой. Глубокая, действительно бесшовная интеграция — это пока из разряда обещаний. Не упрощает жизнь разработчикам (а следом за ними и самим заказчикам) и агрессивная политика поглощений в погоне за созданием комплексных экосистем ИБ.

Не хватает замены и комплексным западным ECM / ERP -системам со встроенной безопасностью. Впрочем, для таких продуктов первична их основная функциональность, где пока разрыв существенен.

Традиционно ощущается нехватка решений по защите уникальных и унаследованных инфраструктур: готовых решений часто нет, все делается руками интеграторов, а вместо технических — реализуются компенсирующие организационные меры.

TADVISER: Есть мнение, что большинство российских решений — лишь «косметически причесанные» западные продукты или сборки на open source. Так ли это? Хватает ли у нас сильных полностью независимых разработок?

АЛЕКСЕЙ КОМАРОВ: Распространенный миф, верный лишь отчасти. Open source активно используется как основа для многих продуктов, но в этом нет ничего плохого. Это стандартная практика, ускоряющая разработку и снижающая затраты. Другой вопрос — что разработчик делает с этой основой. Глубокие доработки, добавление собственной логики или экспертизы — это уже самостоятельная разработка.

Тезис про «причесанные западные продукты» уже не актуален. Все серьезные вендоры давно провели аудит исходного кода и избавились от прямых заимствований, чему в немалой степени поспособствовала и осложнившаяся процедура включения в реестр отечественного ПО .

Более того, в рамках процедур сертификации или оценки выполнения требований по безопасной разработке ПО дополнительно проводится проверка отсутствия уязвимостей во всех внешних подключаемых библиотеках и модулях с обязательным их исправлением.

Сегодня в России есть множество сильных независимых разработок с нуля с применением оригинальных технологий, защищаемых патентами. Сводить все только к «сборкам» и «причесыванию» — несправедливо и неверно.

TADVISER: Как изменились требования бизнеса к ИБ-решениям за последние годы? Стали ли компании более лояльны к российскому ПО?

АЛЕКСЕЙ КОМАРОВ: Лояльность к российскому ПО, безусловно, выросла. Оно уже не воспринимается как «бюджетный вариант» или то, что нужно закупить «для галочки». Сейчас это стратегический выбор для многих Заказчиков, которые готовы учитывать некоторые «детские болезни» отечественных продуктов и активно участвуют в их доработке и развитии, понимая, что это гарантия технологического суверенитета в будущем.

Задачи бизнеса тоже кардинально поменялись: формального соответствия требованиям регуляторов уже мало. Заказчики понимают, что ИБ — это не про затраты, а про условия выживания, поэтому требуют бесшовную интеграцию, централизованное управление, масштабируемость и качественную техническую поддержку.

TADVISER: С какими вызовами сталкиваются крупные компании при переходе на отечественные ИБ-решения?

АЛЕКСЕЙ КОМАРОВ: Основная трудность заключается в успешной интеграции в сложную гетерогенную среду. Заменить один продукт относительно просто, а вот интегрировать без вреда для отлаженных бизнес-процессов десяток новых продуктов друг с другом и с унаследованными системами — уже задача со звездочкой.

К недостаточной зрелости процессов технической поддержки отечественных разработчиков добавляется нехватка компетенций у внутренних команд Заказчика, годами работавших с привычным набором вендоров, а теперь столкнувшихся с необходимостью быстро освоить целую палитру новых продуктов.

При масштабных внедрениях сказываются и проблемы с масштабированием и производительностью при больших нагрузках, что особенно критично для крупного бизнеса.

TADVISER: Как вы оцениваете готовность отечественных решений к защите инфраструктуры органов власти?

АЛЕКСЕЙ КОМАРОВ: Точно нет никаких проблем с точки зрения формального соответствия требованиям. В то же время, в вопросах создания целостной, глубоко интегрированной системы обеспечения ИБ, способной эффективно противостоять сложным целевым атакам, определенно есть возможности для совершенствования.

TADVISER: Какой самый неожиданный вызов в работе пришлось преодолеть вам лично за последнее время?

АЛЕКСЕЙ КОМАРОВ: Запомнился случай не столько технический, сколько лингвистически-логистический. При создании комплексной системы ИБ крупного промышленного предприятия пришлось решать нетиповую задачу: тестировать совместимость отечественных наложенных средств защиты с прикладным ПО от разработчика из дружественной страны.

Разработчик про отдельные классы тестируемых средств ранее даже не слышал, и передавать, пусть и демонстрационную, версию своего продукта для испытательного стенда на нашей площадке категорически не хотел. Предоставлять удаленный доступ к собственному стенду российским «ИБшникам» разработчик также не горел желанием. Дело в том, что планировалось не просто подключение, а установка незнакомого ему ПО с интерфейсом только на русском языке и активное проведение проверок в соответствии с объемной и загадочной Программой и методикой испытаний (ПМИ).

Вынужденный язык общения — английский, не являющийся родным ни для одного из участников процесса, вносил дополнительные сложности в коммуникации.

Пришлось расширить и без того объемную методику испытаний, добавив в нее детальное описание средств защиты, а затем перевести документ на английский язык. Перевод должен был максимально полно и точно передать все планируемые действия и ожидаемые результаты по каждому шагу. Параллельно наши аналитики подготовили и также перевели развернутую Аналитическую записку. В ней разъяснялись требования российского законодательства в области безопасности критической информационной инфраструктуры — чтобы обосновать для зарубежных коллег, зачем вообще все эти средства нужны, и почему без них не получится успешно сдать проект.

В итоге удалось найти общий язык и тестирование, занявшее, правда, с перерывами на обед и сон без малого неделю, успешно провели.