

«ЭЛВИС-ПЛЮС»

ИНТЕГРАТОР СИСТЕМ БЕЗОПАСНОСТИ СРОДНИ СЕМЕЙНОМУ ДОКТОРУ

Безопасность остается одним из главных приоритетов компаний, благодаря чему рынку удается не «проседать» даже в непростые времена. При этом крайне важную роль на нем начинает играть доверие. О тенденциях развития рынка ИБ мы поговорили с генеральным директором компании «ЭЛВИС-ПЛЮС» Юрием Ивашковым, первым заместителем генерального директора Виктором Басиным, а также с заместителями генерального директора Сергеем Акимовым и Сергеем Пановым.

Компания работает на рынке ИБ очень давно. Как за прошедшие годы изменился рынок?

Виктор Басин: Действительно, нашей компании исполнилось 25 лет. Можно сказать, мы начали работу еще до появления рынка ИБ, наблюдали все стадии его формирования. Поначалу было очень мало информации, ни у интеграторов, ни у заказчиков не было квалифицированных специалистов, и вся работа сводилась к обычной продаже «коробок». Именно тогда и началась история «ЭЛВИС-ПЛЮС» в качестве высокотехнологичной компании, имеющей подготовленные кадры: появился ряд заказчиков, которые не могли самостоятельно внедрить решения, и мы вышли на рынок интеграторских услуг – доверяли системы безопасности за другими компаниями и настраивали их.

Сейчас ситуация совершенно другая – рынок стал цивилизованным. Компании предъявляют высочайшие требования к квалификации и опыту интегратора, а зачастую – и к отраслевой экспертизе.

Сергей Панов: Сейчас заказчики прекрасно знают, что им нужно. Причем как на уровне специалистов, которые занимаются ИБ, так и на уровне директоров уверенно связывают управление безопасностью, например, с финансовыми рисками. Да, работать стало легче, потому что теперь напротив сидят люди, говорящие с нами на одном языке. И сложнее: ведь уровень требований несоизмеримо выше. Но мы к этому готовы и уверены в своих силах и возможностях.

Сергей Акимов: На западном рынке безопасность уже давно продается финансовым и генеральным директорам. У нас ответственность лежит пока по-прежнему на подразделениях безопасности. Тем не менее точкой принятия решений все больше становится бизнес, он начинает явно осознавать свои потребности, хотя этот переход и находится пока что в начальной стадии. Вопросы безопасности действительно выходят на уровень совета директоров.

Как за последние несколько лет изменились взгляды заказчиков? Что для них стало актуальным?

Юрий Ивашков: Заказчик в конечном итоге ценит не только систему, соответствующую требованиям технического задания, но и решение своих проблем, при этом зачастую таких, о которых он раньше даже не подозревал или которые возникли в ходе реализации проекта. Менеджеры высокого уровня ценят умение решать такие проблемы. Именно на этом базируется доверие, и нам становится проще доказывать свою ценность для конкретного проекта.

Сейчас вопросы безопасности выходят на уровень бизнеса, становятся интересными руководству компаний, поэтому появляются такие потребности, как хорошая визуализация результатов мониторинга. Очень важны надстройки к аналитическим инструментам, позволяющие оценить риски в финансовом выражении, свести статистику в диаграммы – то, что будет полезным руководителю. Становятся популярными и высокоуровневые решения, позволяющие смоделировать, как скажутся те или иные изменения на инфраструктуре, как изменение настроек систем повлияет на безопасность.

Наши клиенты ценят экспертизу, их постоянно надо «удивлять». Интегратор по безопасности сродни семейному доктору. Должны быть доверие на всех уровнях и уверенность в его квалификации.

Для рынка ИБ характерно то, что киберпреступники всегда идут на шаг впереди. Каким образом возможно бороться с ними?

Киберпреступники впереди уже потому, что их деятельность ничем не регламентирована, у них развязаны руки, это влияет в том числе на скорость создания новых инструментов. А вот нам приходится действовать в рамках жестких регламентов. Любой продукт подлежит сертификации, на это уходит не меньше времени, чем на его разработку.

Отрасль безопасности достигла такого уровня, когда с обеих сторон – и атакующей, и защищающейся – находятся бизнесмены. У атакующей стороны есть много инструментов, на которых строится отдельный бизнес, и сформирован свой рынок услуг, включая аутсорсинг. Всему этому можно противостоять только сообща, с помощью уже сформировавшегося сильного сообщества ИБ. Если идти по пути интеграции усилий, обмениваться опытом, информацией и технологиями, то мы вполне способны противостоять угрозам.

Цифровая трансформация, без которой не могут обойтись компании, если они хотят остаться на рынке, радикально повышает их риски. Как должна измениться стратегия их защиты?

Главные изменения напрямую связаны с задачей комплексности защиты. Усложняется реализация бизнес-систем, растут их связность и взаимопроникновение. Это требует на порядок более серьезного контроля. Нужны полная информация обо всех стадиях обработки данных, ее интеллектуальный анализ, выявление критичных точек и оперативная выработка методов компенсации угроз. В идеале все должно происходить в автоматическом режиме, то есть система должна быть самообучаемой.

Можно выделить четыре вида активностей: предотвращение атак, их обнаружение, реагирование и прогнозирование. В реализации первых двух мы широко применяем свои продукты «ЗАСТАВА», а третий и четвертый – это наши услуги и экспертиза. «Базовый доверенный модуль» (БДМ) для защиты мобильных рабочих мест позволяет компенсировать часть угроз – например, тех, что связаны с системами дистанционного банковского обслуживания. VPN «ЗАСТАВА» и «ЗАСТАВА» СОА дают возможность обнаруживать и нейтрализовать угрозы в каналах связи, сегментах и на периметре корпоративной сети.

Компаниям катастрофически не хватает собственных компетенций, из-за этого тормозится развитие рынка. Как, по вашему, следует решать эту проблему?

При разумном подходе заказчик должен обладать ключевыми компетенциями, а все остальное, включая аутсорсинг и аутстаффинг, могут предложить подрядные организации. Предложений на рынке много, и все проблемы вполне решаемы, просто кто-то соглашается на аутсорсинг, а кто-то – нет. Надо отметить, что все наши основные заказчики наращивают собственные возможности. Однако аутсорсинг все равно будет востребован: часть процессов компании вынуждены делегировать.

Ощущаете ли вы на себе курс на импортозамещение и какие для этого предпринимаете шаги?

В ИТ-секторе такого всплеска, как в сельском хозяйстве, конечно, не произошло. Тем не менее определенную динамику рынку придать удалось. Многие заказчики «взяли под козырек» и приступили к выполнению рекомендаций правительства, тем более что в связи с сокращением бюджетов и курсовыми колебаниями ряд продуктов оказался недоступен.

В вопросах внедрения многих систем действительно прослеживается тенденция перехода на отечественные решения. У нас появились заказчики, задумавшиеся о переходе на отечественные разработки при наличии внедренных и хорошо работающих импортных. Для многих крупных компаний, даже не подпадающих под какие-либо ограничения, рекомендации правительства не являются пустым звуком. Если говорить о развитии, отдельно стоит упомянуть проект «Тайзен.ру», в котором мы являемся одними из учредителей.

Именно сегмент ИБ является пионером импортозамещения. Сейчас мы как интегратор и разработчик средств защиты активно работаем над развитием технологического партнерства с производителями средств АСУТП. Импортозамещение – безусловный стимул для формирования новых экосистем вокруг критически важных направлений развития ИТ.



На фотографии слева направо: Сергей Акимов, Юрий Ивашков, Виктор Басин, Сергей Панов