ЗА РУБЕЖОМ «ОБЩИЕ КРИТЕРИИ» — ЭТО ДЕЙСТВИТЕЛЬНО «ОБЩИЕ КРИТЕРИИ», А У НАС В СТРАНЕ ЭТО ЕЩЕ ISO 15408

Александр Соколов,
ОАО «ЭЛВИС-ПЛЮС»

Интервью CNews, обзор «Рынок информационной безопасности России 2004»

О том, как «общие критерии» повлияли на развитие российского рынка ИБ, о тенденциях, проблемах и перспективах на этом рынке в интервью CNews.ru рассказал Александр Соколов, генеральный директор компании «Элвис-Плюс».

CNews: *Какие, на ваш взгляд, ключевые тенденции происходят на рынке защиты информации в России в настоящее время?*

Александр Соколов: Одной из основных тенденций, на мой взгляд, является вступление в силу «общих критериев». Пока что ситуация с критериями очень не однозначна. Дело в том, что стандарт есть, и он действует, Гостехкомиссией уже зарегистрировано более 40 профилей, сертифицировано несколько продуктов.

Т.е. технология уже освоена, по крайней мере, несколькими организациями. Однако в массах пока что нет понимания, для чего нужна эта технология. Ведь, по сути, что мы имеем: стандарт принят, но вместе с ним действует закон о техническом «дерегулировании», который предполагает, что сертификация не обязательна. Поэтому возникает что-то типа правовой ниши: если не обязательно сертифицироваться, то зачем это делать? Ведь сертификация — это деньги и время. А что в итоге получается — никто не может сказать.

Хочу сразу обратить внимание на другую сторону проблемы. Стандарт ISO 15408 принят в России, однако, наша страна не участвует в международном соглашении об «общих критериях». Получается, что за рубежом «общие критерии» — это действительно «общие критерии», а у нас в стране это все еще ISO 15408. Да, стандарты похожи по содержанию, однако полученный в нашей стране сертификат не действует за рубежом. И наоборот, полученный «там» сертификат требует дополнительной досертификации у нас в стране. Повторюсь, что технология освоена, а вот авторитета на внутреннем рынке данный стандарт еще не имеет.

В идеале, для развития сертификации по «общим критериям» страховые компании должны начать серьезно продумывать цену сертификата страхования информационных рисков. Это могло бы очень серьезно повлиять на становление «авторитета» ISO 15408. Заказчики и поставщики чувствовали бы за сертификатом реальные деньги. Пока что такого нет, и рынок находится в подвешенном состоянии.

Помимо «общих критериев», о которых можно еще очень долго говорить, можно отметить еще одну тенденцию. Ее суть в том, что в последнее время заметно растет образовательный уровень. Отличия по сравнению, например, с 2002 г., очень большие. Пользователи стали более грамотными, начали разбираться в этих вопросах защиты информации.

Если посмотреть программу практически любой ИТ-конференции, везде можно найти специальные мероприятия, посвященные вопросам информационной безопасности. В российских вузах идет активная подготовка профильных специалистов, что способствует появлению на рынке молодых, талантливых и энергичных профессионалов.

Государственные структуры стали уделять очень много внимания популяризации вопросов информационной безопасности. Так что, в целом растет грамотность, а вместе с ней — и качество потребителя. Все это, несомненно, должно отразиться на качестве предложения.

CNews.ru: *Известно, что Гостехкомиссия при президенте РФ перешла в подчинение Минобороны. Как, на ваш взгляд, это событие отразится на российском рынке ИБ?*

Александр Соколов: Любая реорганизация приводит к сбою. Всегда так было. По крайней мере, к задержкам. Скажем так, административная реформа еще не закончена. Как это будет выглядеть в завершенном состоянии — я думаю, что придется подождать до осени. Но то, что будут определенные задержки, — безусловно.

Такова любая административная реформа — люди не знают, за какие вопросы будут отвечать. Раньше у них было все известно — существовала какая-то сфера деятельности, существовал список вопросов, которые решала Гостехкомиссия. А сейчас непонятно — в каком составе, какова мера ответственности, какая зона вопросов. Одно время звучало название — Комиссия по экспорту, но это совершенно другой спектр вопросов. Поэтому давайте, наверное, подождем окончания административной реформы. Так будет видно. Но какие-то задержки будут, безусловно.

То же самое сейчас происходит и с ФАПСИ. Произошло переподчинение. Казалось бы, ну уж совсем родственная структура, откуда вышли — туда и вернулись. А, тем не менее, задержки происходят.

CNews.ru: *Специалисты в сфере ИБ полагают, что спрос на решения защиты информации более-менее сформировался. Основным заказчиком выступают крупные компании и государство. А что можно сказать о среднем и малом бизнесе?*

Александр Соколов: Со стороны малого и среднего бизнеса спрос пока что очень неустойчив. Ну, наверное, формирование спроса произойдет тогда, когда станет заметен ущерб от некорректной работы с информацией и непринятия меры информационной безопасности. Ведь пока этого нет, трудно рассчитывать, что кто-то всерьез озаботится защитой информации.

Кроме затратной стороны — нужно приобретать дополнительные средства, тратить силы и время, — существует еще один аспект — защита информации, — а это все-таки ограничение корпоративной системы и ее функционала. Последнее всегда воспринималось несколько напряженно.

CNews.ru: *На деле это означает, что средний и малый бизнес не сталкивается с серьезными проблемами в сфере защиты информации?*

Александр Соколов: Если говорить о защите информации, то формирование спроса со стороны корпоративного сектора, средних и мелких компаний очень четко проявилось на рынке антивирусов. Точнее, на вирусах и, как следствие, на росте спроса на антивирусное обеспечение. Пока вирусы были где-то, как-то, случайно, изредка и, как говорится, у соседа, на антивирусы не было особого спроса.

Антивирусный сегмент промышленности развивается очень давно. Но только в последние несколько лет появился устойчивый спрос. Когда люди стали обнаруживать то, что именно их компьютер выходит из строя, когда они начали терять информацию, которую готовили месяцами, тогда, конечно, появился спрос.

Сейчас, видимо, большим спросом (из продуктов) с опережением будут пользоваться антиспамные решения. Когда человек приходит на работу и у него среди сотни накопившихся сообщений только два-три полезных, это начинает раздражать. Поэтому какой-то эффективный продукт должен появиться.

В принципе, с этим можно бороться уже сейчас. Проблем нет. И технология известна. Она немного ограничивает пользователя. Все предельно просто: если настроить систему (даже корпоративную) так, чтобы она работала только по заведенному изнутри списку адресов, то, может, кто-то и проскочит, сымитировав адрес отправителя, но это уже мелочи, с этим уже можно бороться по-другому.

Но ведь в основном проблема в том, что системы открыты для всех адресатов. Найти адрес пользователя на сегодняшний день не составляет труда. А ведь достаточно просто ограничить себя. Я имею в виду не принимать неизвестную корреспонденцию. Но почему-то не очень это еще воспринимается. Сколько у каждого человека может быть адресов? Несколько сотен, тысяч адресов, максимум. Это тоже конечный список. А современные средства легко позволяют создать списки электронных адресов, от которых допускается принимать корреспонденцию. Встроенных в популярные ОС приложений должно хватить для того, чтобы создать такие списки.

Так косвенно решалась бы проблема вирусов. Вирус тоже, как правило, приходит извне и очень редко — со знакомого адреса. Хотя там немного сложнее. Буквально происходит следующее… Есть список адресов. Если вирус попадает, то он выбирает этот список адресов, а далее идет имитация. Он подставляет в адрес отправителя известный адрес, и произошла замена, подмена.

Однако и тут есть средства для борьбы. Вот, возьмите, например, те же удостоверяющие центры. Если бы мы работали с правильно настроенной системой, которая имела бы электронные сертификаты, то большая

часть проблем уже была бы решена. Но на сегодняшний день у нас еще нет работающей системы сертификатов, однако рост их количества уже заметен. И я думаю, если не в этом, то, наверное, в следующем году как-то это уже будет практически использоваться.

CNews.ru: *Говоря о государстве и его роли на рынке информационных технологий, хотелось бы узнать, придерживаетесь ли вы мнения, согласно которому государство должно позволить ИТ-рынку развиваться самостоятельно, позволить ему вырабатывать механизмы саморегулирования и т.п.?*

Александр Соколов: Да, безусловно, я так считаю. Но давайте посмотрим на две вещи. На рынке информационной безопасности все должно определяться собственниками информации, владельцами. У них должно быть право устанавливать правила при обращении к их информации. И при таком подходе все становится прозрачным.

Если государство — собственник информации, а государство владеет определенной информацией, то оно имеет право установить правила игры. Вплоть до тех самых нормативов: какие средства использовать, как их использовать и т.д. Если государство не является собственником какой-либо конкретной информации, то, наверное, было бы правильным не вмешиваться и не устанавливать дополнительные правила, то есть не ограничивать этого собственника. Ну, не хочет он вообще, допустим, скрывать свою информацию, зачем же ему навязывать какие-то средства? Зачем ему вводить дополнительные расходы? Вот оно, сразу же проводится грань — до какого предела возможно вмешательство государства. До тех пор, пока используется принадлежащая ему информация.

Де-факто, так уже и есть, государство в последние годы практически не вмешивается, в том числе, и в вопросы защиты информации. Не секрет, что многие коммерческие, особенно мелкие структуры пользуются, в том числе, средствами шифрования, которые далеко не сертифицированы, далеко не проверены, и даже далеко не российские. Но их же за это никто не наказывает.

Однако совсем уж забывать об ИТ-рынке государство не должно. В Индии, например, государство активно взялось за индустрию программного обеспечения — результаты все видят: считанные годы — и такие объемы.

Ну, пока у нас государство еще, видимо, не доросло до помощи каким-то сегментам. Да и какой смысл, если баррель нефти за 40 долларов перевалил? Если ситуация изменится, то тогда возможно будет рассчитывать на более пристальное внимание. Пока ориентация на высокотехнологичные сегменты ограничивается только декларацией. А дальше — посмотрим…

CNews.ru: *Не вызовет ли, на ваш взгляд, административная реформа стагнацию ИТ-рынка вследствие того, что чиновники в значительной степени отвлечены «борьбой за власть»? Ведь не секрет, что государство в значительной степени способствует своими заказами росту данного рынка…*

Александр Соколов: В принципе, допустимый вариант. Но стагнация или кризис вряд ли произойдет: развитие ИТ-рынка остановить уже нельзя. Определенная задержка может произойти в силу административных перестроений, в силу того, что структура еще только проясняется.

Но, поскольку развитие остановить нельзя, проекты по информатизации будут осуществляться и дальше. А это значит, что постоянно будет появляться новая информация, которую необходимо защищать. Поэтому я считаю, что, если и произойдет какая-то заминка в развитии ИТ-рынка в целом и рынка ИБ в частности, то она будет очень кратковременной.

CNews.ru: *Какие, на ваш взгляд, вопросы игнорируются или упускаются из вида при разработке корпоративной политики безопасности?*

Александр Соколов: Очень часто ошибки возникают на уровне методологической разработки, когда определяется, какая информация подпадает под защиту, кому она принадлежит, где она изначально хранится, как она должна вырабатываться, куда и как она должна распространяться. Если эти вопросы успешно решены, то дальше все просто. Политика безопасности — это, по сути, ответы на вопросы: «кому?», «когда?», «что?» и «как?».

Нельзя начинать выдвигать требования к защите конкретного рабочего места, если не решен вопрос: а нуждается ли оно вообще в защите или нет. Лучше начинать строить всю систему сверху, рассматривая каждый из отдельных блоков. Тогда больше шансов, что пробелов не обнаружится. И будут приняты адекватные меры для защиты того или иного участка этой системы. В любом случае, набор политик должен быть оптимальным. Известно: чем меньше правил — тем проще система и тем надежнее она функционирует. В том числе, и с точки зрения защиты информации.

CNews.ru: *Расскажите о наиболее значимых проектах, реализованных вашей компанией на рынке защиты информации за последнее время?*

Александр Соколов: Для начала необходимо отметить, что есть проекты, о которых можно говорить открыто, а есть такие, о которых заказчик и исполнитель стараются не говорить вообще. Ведь любой поставщик решений и услуг в контракте берет на себя обязательства, что если он в процессе работы столкнется с критичной информацией заказчика, он обязуется не распространять ее направо и налево. В области защиты то же самое: практически все контракты выполняются именно с такой оговоркой. И, конечно, ту информацию, которая оговорена ее владельцем как конфиденциальная, мы никогда не будем открывать публично.

С другой стороны, существуют заказы, которые полностью или частично могут быть раскрыты (с предварительного согласия заказчика, разумеется). Например, мы не скрываем, что в прошлом году был начат проект (сейчас завершен его первый этап) в РАО ЕЭС по созданию беспроводной корпоративной сети. Несомненно, что это на сегодняшний день один из крупнейших проектов с использованием радиосетей. В рамках проекта «Элвис Плюс» реализует такой же уровень защиты, как и на физических каналах (типа оптоволокна или провода).

Еще один очень интересный проект… Правда, он еще не завершен и находится на уровне пилотного образца. Но в третьем квартале он уже полностью заработает. Суть проекта заключается в определении инфраструктуры удостоверяющих центров. При реализации проекта достигнута очень высокая однородность средств. То есть, в чистом виде проект реализован на продукции, в основном, трех производителей.

Помимо этих серьезных проектов, мы выполняем огромное количество небольших. Очень много проектов по аудиту безопасности. Однако самые интересные проекты — объемные. Во-первых, такие проекты интересны специалистам, т.к. позволяют им расти. Во-вторых, подобные проекты интересны организации, позволяя нам расширять кругозор. В результате и мы, и заказчик осваиваем новые технологии и продукты, стремительно продвигаясь вперед в своем развитии.

CNews.ru: *Какие тенденции будут определять развитие рынка защиты информации в России в ближайшие год-два?*

Александр Соколов: Это зависит от того, к чему будет расти потребность. Если определять тенденции, исходя из анализа продуктов, вряд ли можно получить результат.

Нужно определять их из общих требований. Поскольку государство уже не может закрыться внутри себя, оно обязано постоянно развиваться. Это значит, что общее развитие необходимо рассматривать с учетом широкого взаимодействия с внешним миром. А значит, тенденция будет такова: все больше и больше будет расти потребность в продуктах, соответствующих мировым стандартам.

Не секрет, что часть российских средств, в силу специфики, не может взаимодействовать ни с кем, кроме как сама с собой. Рассчитывать на широкое распространение систем международного масштаба в России, наверное, нельзя. С другой стороны, существует очень четкое движение в сторону стандартизации. И вот тут могут и должны работать «общие критерии».

Точно так же и с точки зрения управления. Если продукция может управляться из одной точки, то, наверное, спрос на такую продукцию будет расти. Это справедливо потому, что в настоящее время явно выражена тенденция к оптимизации процесса сопровождения. Если раньше оценивалась стоимость первоначальной закупки, то теперь уже видно, что, насколько бы ни была велика стоимость первоначальной спецификации, очень быстро стоимость сопровождения перекрывает эти цифры.

Поэтому уже, по крайней мере, в крупных организациях четко проявляется тенденция к оптимизации сопровождения, то есть, и административную структуру минимизируют, так как стоимость специалистов в России все-таки растет. Поэтому то, что может управляться удаленно, будет пользоваться устойчивым спросом. Это, условно говоря, когда один администратор может обслуживать большую территориальную сеть.

Ведь сейчас же вообще вопросы аутсорсинга в широком плане становятся все более интересными. Многие организации рассматривают вопрос сокращения внутренних подразделений за счет привлечения внешних структур. На Западе этот процесс, как всегда, идет с опережением. Но и в России он начал развиваться.

То же самое и в области безопасности. Конечно, психологически очень тяжело отдать вопросы безопасности во внешний мир, но когда эти вопросы воздействия четко специфицированы, то в этом нет ничего страшного.

Внешнее управление меняет параметры, переконфигурирует систему, обеспечивает ее работоспособность. Но оно совсем не означает доступ управляющего к информации структурирующей системы. Если внимательно рассмотреть принципы построения, то собственник системы может убедиться, что ничего страшного в этом нет. Все в строго ограниченных пределах.

Не секрет, что все сети общего пользования, за исключением специальных, сейчас функционируют на продуктах далеко не отечественного производства. А это объективно говорит о том, что кнопки управления находятся за пределами государства. Но это уже риск государства. Как оно собирается решать эту проблему — вопрос весомый. Можно предположить, что в какой-то момент связь, по крайней мере, общего пользования в государственных масштабах может на время прекратиться. Зарубежные примеры имеются. Кто и как будет решать эту проблему — будем надеяться, что новая реформированная администрация будет уделять этому особое внимание. Потому что этот вопрос имеет государственное значение. Если прекратится связь, последствия просчитать будет очень тяжело.

Таковы тенденции. Конечно, будет расти спрос на решения в сфере ИБ. Хотелось бы сказать, что на простые решения, но так не получится. Потому что сложность будет возрастать. Если растет пропускная способность каналов, то, естественно, будет расти и сложность продуктов.

CNews.ru: *Спасибо.*
