Александр Соколов: предложение на рынке ИБ России существенно опережает спрос

В интервью CNews.ru Александр Соколов, генеральный директор компании «Элвис-Плюс», рассказал об основных принципах, на которых должна строится современная система ИБ на предприятии и о своем взгляде на наиболее заметные тенденции рынка России.

Корр.: Каковы, на ваш взгляд, основные тенденции на рынке информационной безопасности в России?

А.С.: Насколько я понимаю, речь идет о тенденциях, охватывающих две основные составляющие рынка: спрос и предложение. Существует расхожая фраза «Спрос рождает предложение». Ситуация на рынке средств информационной безопасности аналогична положению во всем сегменте IT-индустрии в России: предложение существенно опережает спрос. Прежде всего это связано с низкой оценкой стоимости информационных ресурсов их владельцами и, конечно, с экономическим состоянием предприятий. Если первый фактор не стимулирует внимание потребителей к технологиям и средствам информационной безопасности, то второй ограничивает их возможности в случае принятия решения о мерах по защите информационных ресурсов.

Россия находится только в начале пути в международное информационное общество и отстает от промышленно развитых стран мира. Вместе с тем, процесс ее вхождения в такое сообщество является неотвратимым. Немалую роль в этом играет начатая процедура вхождения России во Всемирную торговую организацию и интеграции отечественных телекоммуникационных и информационных систем с международными. Разработка таких федеральных программ, как «Электронная Россия», «Электронное правительство» и прочих. В результате постепенно создаются благоприятные условия для формирования единого инновационного и информационного пространства на базе общего рынка информации, товаров, услуг, капиталов и рабочей силы.

Корр.: Насколько я понимаю из ваших слов, в России темпы роста предложения опережают темпы роста спроса. Когда тогда стоит ожидать скачок спроса и стоит ли его ожидать вообще в ближайшем будущем?

А.С.: На рынке средств ИБ такой качественный скачок происходит уже сейчас. В настоящее время информатизация является наиболее динамично развивающейся, перспективной базовой инфраструктурной отраслью, обладающей потенциалом долгосрочного роста. Идет динамичный процесс иностранных капиталовложений в российскую информационную инфраструктуру. Начинают активно действовать все новые и новые компьютерные и телекоммуникационные сети, информационные базы данных. Использование локальных компьютерных сетей, объединение их в глобальные информационные сети обеспечивает доступ к любым базам и банкам данных, но в то же время, повышает риск утечки конфиденциальных информационных ресурсов.

Кроме того, можно отметить тенденцию повышения уровня защиты интеллектуальной собственности, технических и юридических средств контроля за ее использованием в компьютерных сетях. Российские поставщики информационных услуг и потребители получают возможность защиты от неравной конкуренции с западными производителями, все яснее перспектива выхода конкурентоспособных российских продуктов, технологий и услуг в области защиты информации на международные рынки.

Все яснее в России прослеживается и тенденция перехода от частного решения проблем защиты к комплексному подходу. И это несмотря на то, что по оценкам западных

аналитиков, сложные решения по защите информации пока еще не пользуются большой популярностью и 97% потребителей останавливают свой выбор на упрощенных схемах защиты.

Корр.: Какие продукты пользуются повышенным спросом?

А.С.: На сегодня наиболее популярными в Росси средствами защиты информации являются межсетвые экраны, средства криптографии, встраиваемые в приложения средства ЭЦП, средства построения VPN, ну, и конечно, средства обнаружения атак

Все более заметной становится тенденция перехода заказчиков к комплексному решению проблемы. Это оценка угроз, выбор оптимальных подходов к обеспечению безопасности и применение разнородных организационных, технических и программно-аппаратных средств защиты.

По опыту «ЭЛВИС+» могу отметить, что последнее время все больше появляется заказов на проектирование и создание комплексных систем информационной безопасности, объединяющих организационные, технические, инженерно-технические и программные решения. Большее внимание начинают уделять оценке экономической целесообразности и эффективности внедрения средств ИБ.

Территориальное распространение информационных систем наряду с ростом количества их пользователей вызывает необходимость в построении серьезных систем управления безопасности и, соответственно повышает интерес к средствам формирования инфраструктуры открытых ключей, мониторинга состояния, интегрированного управления продуктами защиты различных производителей. Именно поэтому «ЭЛВИС+» уделяет значительное внимание расширению количества и качества решений, предлагаемых пользователю. Например, только что успешно прошло внедрение в ГК АРКО новой версии продуктового ряда «ЗАСТАВА» на базе технологий нашего «любимого» производителя – компании Trustworks Systems.

Данная версия обладает существенно расширенными возможностями по построению сложных и многофункциональных систем защиты информации. Так еще в начале прошлого года специалисты Trustwork Systems получили положительные результаты совместных испытаний на совместимость данной версии по протоколу IPsec с продуктами таких известных производителей, как RSA Security Inc., Entrust Technologies Inc., Baltimore, VeriSign Inc., SSH, Microsoft . В средствах управления уже реализована возможность управлять не только агентами ряда «ЗАСТАВА», но и продуктами CISCO. До конца года будет реализована и функция управления продуктами такого известного производителя как CheckPoint.

Корр.: И все же, нельзя ли подробнее остановится именно на прогнозах развития данного рынка в России?

А.С.: Прогнозы являются прерогативой специализирующихся на таких исследованиях организациях. Поэтому, не претендуя на роль Нострадамуса в данной сфере, можно только попробовать приблизительно оценить некоторые ориентиры. Так, известно, что западные компании тратят 4-5% своих ИТ-бюджетов на реализацию мер по защите информации. По данным газеты «Коммерсант» в России на развитие информационной инфраструктуры различного типа организации тратят от 1% (металлургия) до 30% (финансовый сектор) своих бюджетов. Учитывая отставание России в понимании проблем актуальности защиты информации, можно предположить, что данные статьи составляют порядка 0,1-0,2% в затратной части бюджетов. Таким образом, общий объем рынка СИБ в

2001 г в России можно оценить на уровне 40-80 млн. долл., на 2002 г. в соответствии с данными, заложенными в проект Государственного бюджета – 60-120 млн. долл.

Для сравнения, можно отметить, что в соответствии с последними исследованиями IDC, объем только европейского рынка продуктов защиты информации (программных и аппаратных) возрастет с $1.8 миллиарда в прошлом году до $6.2 миллиарда в 2005 г.

С технологической точки зрения можно в основном согласиться со специалистами The Yankee Group, прогнозирующими, что в ближайшем будущем в индустрии электронной безопасности особенно ярко будут проявляться следующие тенденции:

Первое: образование нового класса сетевого оборудования - защитных сервисных коммутаторов, с помощью которых появится возможность оказывать корпоративным клиентам широкий спектр услуг по обеспечению безопасности в компьютерных сетях;

Второе: формирование рынка услуг по защищенной доставке цифрового контента и рынка технологий такой доставки (в 2001 году ожидается, что его объем составит 200 млн. долл., а к 2005 году - 2 млрд. долл.);

Третье: произойдет возрастание объемов рынка управляемых услуг безопасности, который по прогнозам к 2005 году превысит 2.6 млрд. долл., при этом лидирующее положение на нем будут занимать провайдеры, учитывающие интересы электронной коммерции, пользователей услуг Web-хостинга и виртуальных частных сетей на основе IP;

Четвертое: специалистами прогнозируется формирование нового рынка услуг удаленной "точечной" сетевой защиты в рамках виртуальных частных сетей на основе IP - его участники будут обеспечивать защиту удаленных компьютерных систем, которые клиенты будут использовать для работы в интернете;

Пятое: увеличение объемов рынка интеллектуальных услуг сетевой защиты до 1 млрд. долл. по мере того, как его участники будут превращать адаптивное управление безопасностью сетей из реактивного в предупреждающий процесс, предоставляя пользователям возможность защититься от хакеров, пытающихся проникнуть в их IT-системы;

Кроме того, будут иметь место интеграция систем управления безопасностью с платформами для управления сетями и расширение применения биометрических систем аутентификации для повышения достоверности электронных документов и придания им юридической силы.

Кроме того, несомненно, возрастет спрос на консалтинговые услуги в части подготовки концепций информационной безопасности, проектирования комплексных информационных систем с учетом требований защиты, построения систем управления информационной безопасностью.

Корр.: По утверждениям некоторых участников рынка, разработкой систем информационной безопасности в крупных корпорациях может заниматься только компания системный интегратор, имеющая опыт разработки и построения сетей. Вы согласны с таким утверждением? Или ситуация не столь категорична?

А.С.: Я абсолютно согласен с приведенным утверждением и основываюсь на базе опыта 10-летней деятельности «ЭЛВИС+». Как хорошо известно, «сапоги должен тачать

сапожник а пироги печь – пирожник». Разработчики, прежде всего, решают собственные проблемы, то есть пытаются обеспечить функционирование собственного продукта. Построение же систем связано с необходимостью решения широкого круга проблем, который принципиально не может быть закрыт применением какого-либо, пусть даже очень хорошего продукта.

Корр.: Какими основными особенностями должна обладать современная система ИБ на предприятии?

А.С.: Прежде всего необходимо помнить, что защита от угроз безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу защищенной сети, так как любая система защиты, по определению, всегда налагает ограничения на работу персонала. Поэтому одним из основных принципов создания защищенной сети наша компания видит принцип максимальной дружественности.

Вплотную к этой проблеме стоит принцип прозрачности системы ИБ. Основное назначение любой защищаемой сети - это обеспечение потребностей пользователей в информации. Поэтому система безопасности должна работать в «фоновом» режиме, быть незаметной и не мешать пользователям в основной работе, но при этом выполнять все возложенные на нее функции.

Нельзя не упомянуть и некоторые другие принципы, которые использует наша компания при построении комплексной защиты информационных сетей. Прежде всего это принцип системного подхода к построению защиты, который позволяет заложить комплекс мероприятий по парированию угроз безопасности информации уже на стадии проектирования защищенной сети, обеспечив оптимальное сочетание организационных и инженерно-технических мер защиты информации. Оборудование действующей незащищенной сети средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение ее в защищенном варианте.

Кроме того, важен принцип многоуровневой защиты. Этот принцип предполагает необходимость реализации защиты на всех уровнях жизнедеятельности сети. Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон.

Важен принцип простоты применения защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных трудозатрат или малопонятных для пользователя действий.

И последний по списку, но не по значимости – принцип разумной разнородности. Программно-аппаратные средства, используемые для построения системы защиты на различных уровнях, должны дублировать основные функции. Хорошо если в данном случае используются продукты различных производителей, что существенно затруднит несанкционированные действия за счет различной логики построения средств защиты.

Именно поэтому, несмотря на наличие широкого ряда продуктов построения систем информационной безопасности «ЗАСТАВА», компания «ЭЛВИС+» использует в проектах продукты многих третьих производителей, как отечественных, так и зарубежных.

Корр.: Какую роль на рынке систем информационной безопасности должно играть государство? Насколько данный рынок может быть свободным? Некоторые участники рынка настаивают на принципе «Пусть цветут все цветы», другие ратуют за тотальный контроль.

А.С.: Бесспорно, государство должно устанавливать «правила игры» и обеспечивать их выполнение всеми участниками рынка. Рынок средств защиты не может быть полностью бесконтролен, так же как и рынок оружия. Ограничения, видимо, должны быть. Вопрос только – какие? Более того, существующая система лицензирования в этой области является определенной гарантией для потребителей высокого качества услуг по обеспечению безопасности информации. Другое дело, что процесс лицензирования нуждается в либерализации. По нашему мнению, новый Федеральный Закон № 129-ФЗ «О лицензировании отдельных видов деятельности», который принят Государственной Думой в августе этого года и вступит в силу с февраля следующего года, как раз на это и направлен. Этот закон с одной стороны упорядочит деятельность лицензирующих органов, а с другой стороны, сократит перечень тех видов деятельности, которые подлежат лицензированию. (Хотя, области обеспечения безопасности информации это мало коснется).

Самая сложная ситуация – использование криптографии. Давайте на эту проблему посмотрим вот с какой стороны. Средства защиты, в том числе и криптографические, направлены на защиту информации. Использование сейфов, включая банковские, – не запрещено. Аналогично, можно, на мой взгляд разрешить и использование «коммерческой» криптографии, установив одновременно официальную процедуру вскрытия «информационного сейфа» на законных основаниях примерно аналогичную процедуре доступа к банковским счетам юридических и физических лиц, широко используемую в международной практике. Рынок систем информационной безопасности должен быть максимально свободным, иначе он просто перестанет быть рынком со всеми вытекающими отсюда последствиями.

Корр.: С какими основными трудностями сталкиваются отечественные компании, работающие на рынке ИБ?

А.С.: Проблемы обеспечения безопасности информации содержит в себе два аспекта – технический и правовой. Эти аспекты неразделимы и достичь эффективного результата в решении всей проблемы можно только при совокупном решении вопросов каждого аспекта.

Технический аспект заключается в необходимости создания доверенной среды обмена конфиденциальной информацией с возможностью использования глобальных информационных сетей, в том числе и Internet, в качестве транспорта для сообщений. Этот аспект в настоящее время наиболее проработан. Решение этих проблем возможно с использованием технологий создания виртуальных защищенных сетей (VPN – технологии), включая применение средств криптографической защиты информации. Эти технологии позволяют обеспечить достоверность, целостность и аутентичность передаваемых сообщений. Российские производители в этих вопросах не уступают своим западным конкурентам.

Правовой аспект заключается в необходимости правового регулирования взаимоотношений субъектов в области обеспечения безопасности информации, причем, носящей глобальный характер. Эффективность защиты напрямую зависит от создания правовой базы не только в России, но и на межгосударственном уровне.

Особо нужно отметить необходимость юридического урегулирования вопросов обеспечения электронного документооборота. В процессе использования электронных документов возникает множество юридических проблем, требующих полного правового регулирования. К их числу относятся трансграничное применение средств криптографии; проверка подлинности электронного документа; возможность использования электронных документов в качестве доказательств в арбитражных судах. Сегодня сложности возникают и с такими вопросами как оценка и распределение риска убытков, которые могут возникнуть в процессе функционирования системы электронного документооборота; в вопросах взаимоотношения юридических лиц, использующих электронные документы, с аудиторскими фирмами, налоговыми и другими государственными органами, куда необходимо представлять отчетность о своей деятельности. Требуют решения и международно-правовые проблемы, которые могут возникнуть когда, например, два участника электронной торговли и/или провайдер находятся в разных странах.

В решении этих вопросов необходим разумным компромиссный подход, предусматривающий определенные меры по правовому регулированию использования Internet, при условии, что они будут носить рамочный и гражданский, а не запретительный и административный характер. Большие трудности в обеспечении правильной и надежной защиты вызывает так же и определенное недопонимание этой проблемы со стороны руководителей организаций, но об этом мы уже сегодня говорили.

Не могу не отметить и такую проблему, как необходимость ответов на часто задаваемый вопрос об экономической эффективности внедрения средств защиты. Этот вопрос возникает обычно из неполного понимания назначения средств защиты. Если информационные системы направлены на повышение эффективности бизнеса и методики расчета эффективности их внедрения хорошо известны, то средства защиты непосредственно не могут поднять эффективность бизнеса, если, конечно, не принимать в расчет такие параметры, как его расширение за счет роста доверия клиентов и партнеров к используемым системам. Проблема аналогична расчету эффективности приобретения сейфа для хранения ценностей. Сейф может окупиться на следующий день после его установки в случае неудачной попытки его взлома, а может не окупиться никогда, если таких попыток не будет. С другой стороны, в каждом конкретном случае можно сделать оценочные расчеты потенциального эффекта от внедрения. Например, можно оценить стоимость 1 минуты простоя (из-за нападения хакера) системы обеспечения диспетчерской службы аэропорта или стоимость потери 1 транзакции в системе интернет-трейдинга, или кражи номеров счетов и параметров их владельцев в системе on-line банкинга. Но решение данных вопросов требует существенных затрат со стороны специалистов и, соответственно, стоит достаточно дорого, что не всегда с пониманием воспринимается потенциальным заказчиком.

Корр.: Аппаратные средства защиты – это основа ваших систем ИБ или все же вспомогательное средство по сравнению с программными продуктами?

А.С.: Говоря об основных тенденции на рынке информационной безопасности в России, я уже упомянул о необходимости комплексного подхода к решению проблем обеспечения безопасности информации. Сегодня невозможно выделить системы безопасности, построенные на «чисто аппаратных» или «чисто программных» средствах защиты. Повышение быстродействия, пропускной способности таких систем невозможно без применения аппаратных средств, в то же время, защиту, к примеру, мобильных рабочих станций или обеспечить доверенную загрузку программной среды невозможно выполнить без программных средств защиты. Также невозможно разделить средства защиты на «основные» и «вспомогательные» не только по программно-аппаратной, но и функциональной принадлежности. Основная опасность и кроется именно в попытке

упрощенно подойти к решению проблем защиты. Например, установка межсетевого экрана не решает всех проблем несанкционированного доступа, так же, как и применение электронного ключа совместно с программой шифрования файлов гарантирует сохранность информации только на выключенном компьютере, если он, конечно, имеет сетевое подключение.

Мы проектируем и реализуем системы безопасности с использованием очень широкого набора средств различных производителей как аппаратно-программных, так и программных, а также совокупности организационных, технических и инженерных методов. Причем следует отметить, что организационные методы играют весьма существенную роль практически во всех реализованных системах. Но об этом мы уже сегодня говорили.

Корр.: Спасибо.