Александр Соколов: Спрос на средства защиты со стороны предвыборных штабов компенсирует «предвыборный» спад в других сегментах рынка

В интервью CNews. ru Александр Соколов, генеральный директор компании «Элвис-Плюс» высказывает свою точку зрения на перспективы реформирования ФАПСИ, ситуацию с развитием рынка защиты информации в условиях начинающихся предвыборных кампаний 2003-2004 годов и другие актуальные проблемы отрасли.

CNews. ru: Беседуя с некоторыми вашими коллегами, мы сталкивались с мнением, что в 2003-м году, в год выборов в Думу, не стоит ожидать крупных проектов в сфере защиты информации. Есть ли, на ваш взгляд, связь между этими двумя процессами?

Александр Соколов: Пока данное утверждение не подтверждается на практике. С другой стороны, можно ожидать повышенного интереса к вопросам защиты информации со стороны политических партий. Не составляет секрета, что в период предвыборной гонки существенно растет цена информации, особенно оперативной, о состоянии дел у соперников по выборам.

Безопасность информации и, соответственно, необходимость ее защиты непосредственно не зависят от политических процессов. Однако, связь между крупными проектами по защите информации и предвыборными мероприятиями конечно же есть.

С одной стороны, естественно предположить, что крупные организации, поддерживающие того или иного кандидата, не в состоянии в этот период расходовать достаточно большие средства для реализации затратных проектов по безопасности — деньги нужны, в первую очередь, на другие цели. Но с другой стороны, не секрет, что политическая борьба в этот период меду отдельными кандидатами резко обостряется. Это подтверждает и опыт «первой волны» выборов, которая прошла в регионах. В предвыборных штабах скапливается большой объем очень важной оперативной информации, которая, в случае ее несвоевременного разглашения, может резко изменить положение на политической арене, а в некоторых случаях затрагивает и конституционные права граждан.

Естественно, что в этих условиях, люди, ответственные за проведение предвыборной кампании заинтересованы в повышенных мерах соблюдения конфиденциальности и обеспечении своевременной и достоверной доставки информации. Именно поэтому можно ожидать, что услуги по обеспечению безопасности информации будут востребованы. Нельзя сказать, что это будет какой-то всплеск, но потребность в этом сегменте будет компенсировать спад в других сегментах и, в целом, усредненная картина должна быть достаточно стабильной. Кстати, подтверждением этого является то, что уже сейчас к нам обратились несколько PR-агентств, которым требуются консультации по вопросам безопасности информации. Мы ведем с ними переговоры о возможности проведения аудита безопасности существующих информационных систем и создания мобильных, легко развертываемых в любом месте, но защищенных информационных систем, для обеспечения деятельности предвыборных штабов.

CNews. ru: Как, на ваш взгляд, отразится на рынке упразднение ФАПСИ?

Александр Соколов: Это вопрос не простой. Прежде всего, не будем забывать, что пока принято только политическое решение об упразднении ФАПСИ (в принципе, нельзя упразднить Указом Президента РФ организацию, которая образована Федеральным Законом — для этого необходимо, как минимум отменить Закон «О Федеральных органах правительственной связи и информатизации» и внести изменения в целый ряд других законов, а это делается не в одночасье), техническая реализация упразднения отложена по крайней мере до середины этого года. Так что

говорить как изменится ситуация пока преждевременно — не определены конкретные наследники тех или иных функций, которые выполняло ФАПСИ. Сейчас можно только с той или иной степенью вероятности, делать весьма приблизительный прогноз. Но все-таки, давайте посмотрим, каковы же ожидания общественности от такой реорганизации и насколько они обоснованы.

Во-первых, ФАПСИ многие отождествляют с понятием криптографии и криптографических средств и, соответственно, с проблемами либерализации их применения. Но вопросы применения криптографии затрагивают интересы безопасности государства в целом и, естественно, государство имеет полное право держать их под своим контролем. Собственно, такое положение является стандартным для всех развитых государств. И если организация, которая этим занималась — упразднена, можно ожидать, что эти функции будут переданы какому-либо другому государственному органу. Это может быть и ФСБ России, и Гостехкомиссия России, которым эта проблема достаточно близка по характеру выполняемых ими задач. Скорее всего, это будет ФСБ России. А может быть «тяжелая» криптография, предназначенная для защиты государственной тайны, останется за ФСБ России (ведь это ее основная функция), а более «легкая», предназначенная для конфиденциальных сведений, перейдет в лоно Гостехкомиссии России, которая и отвечает за их защиту. И, если в области обеспечения защиты сведений, составляющих государственную тайну, вряд ли что изменится, то в случае с защитой конфиденциальной информации, видимо, можно надеяться на упрощение процедуры применения таких средств. Кроме того, на мой взгляд, более сильное влияние на рынок средств криптографии, используемой для защиты конфиденциальной информации скорее окажет новый Закон «О техническом регулировании», который предполагает перевод стандартов по безопасности информации (в том числе и криптографических) в разряд добровольных, что может расширить номенклатуру используемых криптографических алгоритмов. Сейчас складывается благоприятная ситуация, чтобы ввести понятие «технологическая криптография».

CNews. ru: Что вы имеете ввиду под «технологической криптографией»?

Александр Соколов: Поясню. Традиционно средства криптографии использовались для того, что бы исключить возможность ознакомления с содержанием какого либо сообщения, его сокрытия от посторонних глаз и ушей. То есть, можно сказать, что обеспечение конфиденциальности сообщений — «классическая» криптография. Вместе с тем, сейчас достаточно широко средства криптографии используются не для скрытия самого сообщения, а для решения других задач, без которых нельзя обеспечить безопасность информации, но которые оставляют само сообщение в открытом виде, например, классический пример цифровой подписи — для подтверждения юридической значимости электронного документа достаточно передать само открытое сообщение и к нему хеш-функцию, полученную с применением криптографического алгоритма. Аналогично и при аутентификации пользователей, и при создании виртуальных каналов. Таким образом, существует область где криптографические алгоритмы используются не по «классическому» предназначению, а в «технологических» целях. Это и можно отнести к «технологической криптографии». Такой подход может значительно упростить все процедуры ее применения, не затрагивая государственные интересы.

Во-вторых, ФАПСИ многие отождествляют с понятием ЭЦП и, соответственно, с Законом «Об электронной цифровой подписи» и лицензированием деятельности удостоверяющих центров. Здесь вряд ли что-то кардинально изменится. По всей вероятности лицензирование деятельности удостоверяющих центров останется, тем более, что это прописано и в упомянутом законе, и в Законе «О лицензировании отдельных видов деятельности». Но, как уже неоднократно отмечалось раньше, сами эти законы не внесли резких корректив в области применения ЭЦП, по крайней мере, для коммерческих организаций и корпоративных систем. Во многих случаях лицензирования не требуется — можно вполне эффективно использовать корпоративные удостоверяющие центры и решить все задачи. Правда, в некоторых

случаях, особенно в сфере взаимоотношений государственных органов между собой, без лицензированных удостоверяющих центров не обойтись.

CNews. ru: Какие ведомства наиболее вероятные претенденты на лицензирование данной деятельности?

Александр Соколов: Это, скорее всего, либо Минсвязи России (это ведомство все-таки отвечает за информатизацию и телекоммуникационные системы), либо Гостехкомиссия России (потому что применение ЭЦП — элемент защиты конфиденциальной информации, ее целостности). Но логичнее данную функцию было бы передать в Минюст России (все-таки деятельность удостоверяющих центров сродни деятельности нотариусов, а сама подпись — элемент придания документу юридической значимости). По большому счету разницы в том, кто будет выдавать лицензию нет. Главное, что сам процесс ее получения вряд ли усложнится — он и так был не простой, скорее, исходя из общей тенденции проведения в жизнь политики «дерегулирования» и «дебюрократизации» деятельности, как об этом говорит А. В. Данилов-Данильян, можно ожидать упрощения этих процедур.

В-третьих, ФАПСИ многие отождествляют с понятием электронной «подслушки», а его упразднение с ожиданием ее прекращения, так сказать, перестанет существовать «старший брат». Ну, объективно надо сказать, что и раньше ФАПСИ этим не очень занималось, хотя бы в силу отсутствия достаточных технических и финансовых средств. Вряд ли с изменением организационной структуры что-то изменится. Сама по себе возможность «прослушивания» электронных сообщений как раньше имелась, так и дальше будет иметься. Главное, что бы такие действия осуществлялись в строгом соответствии с действующими нормативными актами и ни в коей мере не ущемляли конституционные права граждан. Но этот процесс скорее лежит в области совершенствования правового регулирования деятельности государственных органов, независимо от их принадлежности, а не их организационных изменений.

CNews. ru: Известно, что вы являетесь сторонником развития системы ЭЦП «снизу» — от корпоративных решений к более масштабным. Нет ли угрозы получить в этом случае несогласованные между собой проекты, созданные в условиях отсутствия общих подходов и стандартов?

Александр Соколов: Проблема несогласованности проектных решений существует всегда. На наш взгляд, и это уже неоднократно отмечалось и раньше, решить ее можно только строгим соблюдением определенных стандартов. Такие стандарты есть, в основном они международные. Мировые лидеры производства программного обеспечения уже широко используют стандартизацию в своих продуктах. Наша компания также ставит во главу угла своей деятельности максимальное соблюдение этих стандартов. Но полностью ликвидировать некоторую разобщенность вряд ли удастся. Всегда найдется кто-то, кто использует «колею другого размера». Да и потом, в пределах корпоративной системы такая проблема не стоит, она наиболее актуальна в момент общения пользователей различных корпоративных систем между собой. Но здесь она разрешима путем создания специальных центров пересертификации (или кросс-сертификации), которые могут поддерживать различные стандарты и возьмут на себя заботу о сопряжении различных систем ЭЦП.

CNews. ru: В последнее время широко обсуждается вопрос создания глобальной электронной сети, параллельной интернету? Основной стимул — создание безопасной среды для развития бизнеса. Что вы думаете о перспективах реализации подобного проекта? Насколько подобный подход способен решить проблему защищенности обмена данными?

Александр Соколов: Глобальные системы для безопасного бизнеса есть и сейчас, достаточно вспомнить, например, банковскую систему S. W. I. F. T. Но они действуют в строго определенной и ограниченной сфере. Проект создания глобальной

электронной сети, параллельной и сопоставимой по масштабам с сетью интернет, если имеется ввиду построение соответствующей инфраструктуры, считаю, в лучшем случае, научной фантастикой, в худшем — попытками направить средства из и так не слишком переполненного государственного бюджета на еще один проект из разряда «поворота сибирских рек».

Давайте посмотрим, нужен ли такой проект? Основным стимулом для проекта называется создание безопасной среды для развития бизнеса. Целью создания безопасной среды является обеспечение защищенного от несанкционированного доступа обмена информацией. В свое время никто не ставил задачу создания безопасной среды между Юстасом и Центром, но множество Штирлицев регулярно передавали свои сообщения.

Теперь предположим, что глобальная электронная сеть, параллельная но не пересекающаяся с интернетом создана. Если сеть глобальная, то подразумевается обеспечение всемирного доступа в нее без ограничения количества пользователей. Это означает, что построена инфраструктура, охватывающая все страны и континенты, поскольку бизнес заинтересован, прежде всего, в расширении рынка. В общем случае получаем Интернет № 2 со всеми его достоинствами (за исключением величины первоначальных вложений) и недостатками. Но насколько он будет безопасен? Ведь создать открытую защищенную информационную систему в принципе невозможно. Нельзя сделать сейф и всем раздать ключи от него — теряется смысл самого сейфа.

Решение лежит в другой плоскости.

Чтобы обеспечить защиту надо установить, кому что разрешено и что запрещено, а для этого, по крайней мере, число пользователей должно быть счетным. Далее, каждого пользователя достаточно обеспечить средствами защиты имеющейся у него и получаемой извне информации, и проблема получает практическое решение даже на открытых системах. Другое дело разработка новых защищенных технологий обмена информацией, создание надежных сетевых протоколов, использование для защиты аппаратных средств. Для этого, вполне возможно, потребуется изменение существующих стандартов обмена данными, а это может повлечь необходимость перехода к новой, более совершенной, чем интернет, сети, обладающей высокой скоростью передачи информации, надежностью каналов, позволяющей хранить и обрабатывать большие объемы информации.

И в заключение можно сказать, что безопасная среда для развития бизнеса, на мой взгляд, состоит в отсутствии чрезмерных бюрократических ограничений, обеспечении цивилизованных правил деятельности, защите бизнеса со стороны государства от внутренних и внешних опасностей.

CNews. ru: Насколько остро сегодня вы чувствуете конкуренцию на российском рынке со стороны западных разработчиков средств сетевой защиты? Есть ли основания считать, что конкуренция будет усиливаться?

Александр Соколов: Наша компания является интегратором в области создания защищенных информационных систем, поэтому, мы для создания эффективной и оптимальной защиты информации одинаково успешно используем как отечественные, в том числе и собственные, так и зарубежные разработки и особой конкуренции с западными компаниями не испытываем. Надо отметить, что в настоящее время существует разделение средств сетевой защиты по сегментам. По действующим требованиям, во многих случаях требуется применение только средств, прошедших сертификацию по требованиям безопасности, действующим в России. Для такой сертификации часто требуется наличие исходных кодов программных продуктов. Это сильно сдерживает процесс сертификации зарубежных продуктов.

Однако, в последнее время наметилась тенденция к большей открытости со стороны иностранных производителей основных программных продуктов. Всем известно, что не так давно компания Microsoft заявила об открытии исходного кода для российских испытательных лабораторий. Компания SUN Microsystems активно развивает процесс сертификации своих продуктов. В процессе сертификации в настоящее время находятся также несколько систем на основе LINUX. Учитывая, с одной стороны грядущие изменения в системе стандартизации, когда в некоторых случаях можно будет использовать механизм декларирования выполнения требований самим производителем (Закон «О техническом регулировании»), а с другой стороны гармонизацию российских требований по безопасности информации с международными (ГОСТ ИСО/МЭК 15408 «Общие критерии»), можно предположить, что конкурентная борьба на рынке средств защиты обострится.

CNews. ru: Какие сегодняшние разработки станут технологиями завтрашнего дня на мировом рынке защиты информации?

Александр Соколов: Трудный вопрос. Сейчас все так быстро развивается, что границы между «сегодня» и «завтра» очень призрачны. Еще пять лет назад VPN-технологии были экзотикой, а сейчас это обычное явление. Сейчас бурно развивается направление встроенных программно-аппаратных средств защиты, например, разработки IBM, Intel и Microsoft. Большую популярность приобретают карманные компьютеры и коммуникаторы, технологии беспроводной передачи информации, для которых существующие технологии защиты не всегда приемлемы. Вот это, наверное, и будет в ближайшем будущем определять развитие технологий защиты информации

CNews. ru: Какие сегменты отечественного рынка ИБ, на ваш взгляд, будут расти наиболее быстро в ближайшие годы?

Александр Соколов: В интервью для обзора по информационной безопасности CNews за 2001 год я отметил, что все более заметной становится тенденция перехода заказчиков к комплексному решению проблемы. Также мы тогда говорили о том, что последнее время все больше появляется заказов на проектирование и создание комплексных систем информационной безопасности, объединяющих организационные, технические, инженерно-технические и программные решения, что большее внимание начинают уделять оценке экономической целесообразности и эффективности внедрения средств ИБ.

Теперь по прошествии времени могу только подтвердить свои же слова двухлетней давности. Более того, теперь этому еще больше подтверждений! Например, наблюдается явный сдвиг спроса в сторону именно услуг в области обеспечения безопасности информации. Заметно повысился спрос на такие услуги, как аудит в области безопасности информации, и даже начинает постепенно развиваться такой подвид аудита, как «сюрвей». Например, наша компания является партнером (сюрвейером) «Ингосстраха» в вопросах страхования информационных рисков.

Несомненно, будет опережающими темпами развиваться сегмент систем управления средствами защиты.

CNews. ru: Насколько бизнес компании «Элвис Плюс» сегодня нуждается в дополнительном финансировании? Есть ли проекты, которые вам хотелось бы осуществить, но на это пока не хватает средств (экспорт решений, разработка новых продуктов)?

Александр Соколов: Бизнес всегда испытывает недостаток средств. Практически всегда имеется потребность в средствах, как на обеспечение текущей деятельности, так и на развитие.

CNews. ru: Какие источники внешнего финансирования были бы для вас более предпочтительны: размещение акций или облигаций на бирже, сотрудничество с западными или российскими партнерами, банковские кредиты? Какова ваша стратегия в этом вопросе?

Александр Соколов: Невозможно в общем случае выделить предпочтительный источник финансирования. Стратегия заключается в выборе оптимального источника финансирования для решения конкретной задачи. На практике мы не пользовались из перечисленных инструментов только размещением акций и облигаций на бирже.

CNews. ru: Какие ключевые проекты запланированы вашей компанией на текущий год?

Александр Соколов: Внедрение инфраструктуры открытых ключей на основе продуктов как отечественных, так и зарубежных производителей с использованием сертификатов для работы реальных приложений в защищенном режиме. Проекты по управлению системами защиты.

CNews. ru: Спасибо.