ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НУЖНА, ЕСЛИ ИЗВЕСТНА ЦЕНА ИНФОРМАЦИИ

Александр Соколов,
ОАО «ЭЛВИС-ПЛЮС»

Интервью CNews, обзор «Средства защиты информации и бизнеса 2005», 13.09.2005

О проблемах и перспективах отрасли информационной безопасности России рассказал CNews Александр Соколов, генеральный директор компании «Элвис-Плюс».

CNews: *В минувшем году рост ИТ-рынка России замедлился более чем вдвое. Отразилось ли это на рынке ИБ и в частности на вашей компании? Какие причины повлияли в наибольшей степени на изменение объемов рынка ИБ?*

Александр Соколов: В целом, конечно, отразилось. Информационная безопасность прочно связана с ИТ-рынком. Поэтому, если сокращается объем работ на ИТ-рынке, это тут же сказывается на его сегменте — рынке ИБ. Наибольшее влияние на отрасль оказала административная реформа. Она задержала многие запланированные проекты, что вызвало замедление темпов роста. На примере нашей компании могу сказать, что в 2004 г. рост не превысил 10%. Мы работаем с очень крупными заказчиками, поэтому оказались особенно чувствительны к проведенной реформе. Дело в том, что такие клиенты тесно связаны с макроэкономикой, независимо от того являются ли они государственной структурой или коммерческой, и любое изменение на государственном уровне приводит к замедлению процесса взаимодействия с ними. Однако уже этот год значительно активней предыдущего, ИТ-рынок растет хорошими темпами, а проведенная административная реформа вызвала лишь временное замедление роста, поскольку других объективных причин нет.

CNews: *Год назад эксперты отмечали, что еще не ясна перспектива стандартов «общие критерии» в России. Что изменилось за прошедшее время? Какую роль сыграло принятие стандартов отрасли?*

Александр Соколов: Действующий в России стандарт ГОСТ/ИСО МЭК 15408 и международный стандарт ISO 15408 по содержанию одинаковы, поскольку российский вариант «common criteria» был создан по западному аналогу. Однако процедура присоединения России к «common criteria» еще не произошла. Сегодня сертификат, выданный любой западной сертификационной лабораторией по «common criteria», в России силы не имеет. Верно и обратное. Федеральная служба технического и экспортного контроля (ФСТЭК), бывшая Государственная Техническая Комиссия, больше двух лет работала над этой проблемой, но до настоящего времени вопрос не решен. Сложно сказать, что полезнее: присоединяться или нет. С одной стороны, присоединение выгодно, потому что в этом случае продукты, сертифицированные в России, потенциально могут быть признаны на западе. С другой стороны, на рынке практически не будет ограничений на западные продукты.

Частично проблема решаема, поскольку международными соглашениями предусмотрена возможность дополнительных ограничений в случае, если степень защиты выше 4 уровня. На самом деле, нужно рассматривать поведение широкого рынка решений ИБ. В этом случае с очень большой вероятностью можно сказать, что российские продукты будут иметь меньше преимуществ. Бюджеты иностранных компаний больше, и отечественные разработчики еще не могут сравниться с ними по масштабам, маркетинговому бюджету и пр. Тем не менее, рынок крупного бизнеса и особенно государственный рынок могут оказаться в не худшей ситуации, поскольку требования «общих критериев» не запрещают устанавливать национальные дополнительные ограничения или требования.

Безусловно, в такой борьбе далеко не каждая компания сможет выжить. Однако, возможно часть компаний смогут выйти действительно на мировой уровень по качеству продукции.

На сегодняшний день отечественный стандарт ГОСТ/ИСО МЭК 15408 носит добровольный характер, т.е. нет ни одного требования, которое обязывало бы разработчика пройти сертификацию. Несмотря на это, сертификации начались, зарегистрировано уже несколько десятков профилей на различные виды продукции. Положительный эффект сертификации заключается в том, что мы начинаем относиться к своим продуктам с позиции международных стандартов, поскольку по содержанию наши стандарты с ними совпадают. Набирается практический опыт, который может оказаться необходимым в случае положительного решения о присоединении.

CNews: *Прошедший год стал рекордным по размерам ущерба, нанесенного мировой экономике вирусными эпидемиями, спамом и злоумышленными действиями в сети. Каково на ваш взгляд соотношение между ущербом, нанесенным «случайными» преступлениями и намеренными заказными атаками на компании? Как оно изменилось за последний год?*

Александр Соколов: Мы занимаемся предотвращением угроз, анализируем, какие возможны угрозы и в соответствии с приоритетом, заявленным владельцем системы, помогаем их предотвращать. Поэтому точных статистических данных у меня нет, точнее, те данные, которые имеются по конкретным организациям, с которыми мы работаем, не подлежат разглашению.

На сегодняшний день проще всего считается экономический ущерб от спама. Хакерские атаки на конкретную организацию случаются достаточно редко, и они не всегда успешны. Сейчас элементарные меры безопасности принимаются практически каждой компанией, и наличие, например, межсетевого экрана позволяет снизить вероятность успешной атаки. Поэтому акцент сдвигается в другую область: наиболее экономически вредным является спам, на втором месте—внутренние угрозы.

CNews: *По статистике до 80% потерь, связанных с ИБ вызваны утечкой информации в результате неграмотных или умышленных действий внутри компаний. Насколько востребованы компаниями средства защиты от своих сотрудников?*

Александр Соколов: Подчеркиваю, я могу опираться только на опыт нашей компании и на ту информацию, с которой мы сталкиваемся, т.е. заказчиков, с которыми мы работаем. За последние два, максимум три года, интерес к этим вопросам резко вырос, многие начинают понимать, что, прежде всего, в системах нужно навести элементарный порядок.

В данной ситуации вернее говорить не об умышленных действиях, а о нарушениях. Преступления в данном случае достаточно редки, а вот нарушения, вплоть до ошибок — распространенное явление, и, в среднем, ущерб от них намного больше. В связи этим, организации начинают задумываться о наведении порядка, в том числе и о разграничении доступа к информации. Прежде всего, должно действовать элементарное правило: если у информации есть стоимость, то надо минимизировать к ней доступ.

Современные технические средства позволяют разграничивать доступ любым способом. Доступом может обладать один человек или группа пользователей, но обязательно счетная — это еще один принцип ИБ: все должно быть счетно. Если количество пользователей не счетное, говорить об ИБ просто не имеет смысла.

CNews: *Насколько на ваш взгляд перспективны биометрические средства защиты и разграничения доступа? Проявляют ли заказчики интерес к биометрическим технологиям? Какие факторы сдерживают развитие биометрии в нашей стране?*

Александр Соколов: Отношение к биометрическим технологиям неоднозначное. У любого продукта есть свои плюсы и минусы. У современных биометрических устройств достаточно велика вероятность ложного отказа в доступе клиенту, имеющему право доступа. Несмотря на имеющиеся преимущества, биометрия не является панацеей. Нужно подходить к ней так же, как и к другим решениям.

CNews: *Все компании, занимающиеся интеграцией, оказывают услуги консалтинга. Какую роль играет консалтинг в сфере ИБ? Насколько востребована данная услуга в России?*

Александр Соколов: Услуги консалтинга востребованы, и, опять же, именно в последние 2-3 года заметен существенный рост спроса. Нет стандартизованного определения, что такое консалтинг. Поэтому можно провести грань: там, где заканчивается выработка некоторых рекомендаций, и есть граница консалтинга.

Все чаще и чаще приходится заниматься выработкой концепции ИБ для конкретного предприятия. Многие положения стандартны, но каждая организация уникальна, поэтому к каждой требуются индивидуальный подход. После разработки концепции следует подготовка документов и рекомендаций по ее реализации. Где-то на этом уровне можно провести границу, дальше начинается проектирование конкретной системы. В нашей работе 70% времени занимает упорядочение организационных структур, разработка схем

ответственности, определение правил и инструкций пользователей, должностных полномочий и пр., и только 30% времени занимает техническая сторона вопроса.

Наведение элементарного порядка в системе дает заметные результаты. Порой не требуется даже дополнительных вложений. Почти всегда в современных организациях уже есть достаточное количество средств безопасности, но зачастую они не используются вообще, иногда используются не в полной мере, а иногда просто неправильно.

CNews: *Какую часть своего ИТ-бюджета готовы тратить российские компании на обеспечение информационно безопасности? Как изменилась доля бюджета ИБ в общем ИТ-бюджете за последние год-два?*

Александр Соколов: В мировой практике существуют оценки, согласно которым бюджет ИБ составляет от 10% до 15% от ИТ-бюджетов, а в некоторых компаниях доходит до 25%, но это скорее исключения. В российских компаниях этот показатель находится на уровне 3% — 7%. Больше практически не бывает. Не могу сказать, чтобы были заметны изменения в последние годы. Вместе с ростом самих компаний растут их ИТ-бюджеты и соответственно затраты на ИБ. Однако я не могу уверенно говорить, что выросла доля затрат на ИБ в общем ИТ-бюджете.

CNews: *Соответствует ли финансирование, которое готовы потратить компании на системы ИБ конфиденциальности информации, которую они хотят защитить?*

Александр Соколов: Если в организации четко поставлена задача, если определена стоимость информации, то проблем с бюджетом ИБ не возникает. Но, к сожалению, пока что это очень редкое явление. Тем не менее, многие компании стали задумываться над вопросом: «как оценить информацию» и положительные примеры в моем опыте уже есть. Более того, появляется интерес со стороны страховых компаний и даже со стороны ассоциации оценщиков к методике экономической оценки информации. Правда тут же стоит подчеркнуть, что и у нас, и на западе возникает вопрос: «как рассчитать возврат от инвестиций в ИБ». Ответ однозначный: возврат от инвестиций в ИБ рассчитать нельзя, точно так же, как нельзя рассчитать возврат от инвестиций в сейф. Если не будет ни одной попытки внешнего взлома, если ни один сотрудник не совершит ошибки, и не найдется ни одного сотрудника, который сознательно задумает причинить вред, тогда все деньги, потраченные на систему обеспечения ИБ, окажутся выброшенными на ветер. Обеспечение ИБ — это определенная страховка, а значит, основной вопрос заключается в определении стоимости информации и оценки величины риска от нарушения правил ИБ в отношении данной информации.

CNews: *Какие наиболее интересные проекты были реализованы вашей компанией в прошедшем году?*

Александр Соколов: Практически все без исключения контракты в области ИБ содержат раздел конфиденциальной информации. Исключения бывают только в том случае, когда с подписано отдельное соглашение. Каждый конкретный проект, точнее информация о каждом конкретном проекте требует предварительного согласования с клиентом.

Я имею возможность говорить только о двух таких проектах. Первый — это проект «Национального удостоверяющего центра». Была разработана однородная масштабируемая система с центром в Москве и филиалами в пяти основных регионах РФ. Использовались продукты четырех производителей: аппаратная вычислительная база IBM, коммуникационное оборудование Cisco, операционная система Microsoft и удостоверяющий центр на основе продуктов KEON RSA с криптографией КриптоПро, на основе которых с чистого листа было создано решение ИБ.

Второй проект—это создание «Базового доверенного модуля» на основе продуктов IBM.

С учетом решения политических вопросов данный проект длился около 2,5 лет. В результате был создан российский продукт — мобильное рабочее место с большим объемом функций безопасности, соответствующее требованиям ИБ Российской Федерации. Качество продукта отмечено «юбилейным» сертификатом №1000 в системе сертификации ФСТЭК России.

CNews: *На какие технологии защиты делается акцент вашей компании? Какие перспективные разработки вы собираетесь предложить в будущем?*

Александр Соколов: Мы не имеем право делать акцент на технологиях, мы, прежде всего, ставим задачу защиты информации с таким уровнем, который является приемлемым для ее владельца. Не существует универсального продукта, который решает все проблемы. Необходимая степень защиты информации определяет и технологии и продукты, которые буду затем использоваться.

Если говорить о перспективах, то я упоминал спам, с которым хорошо бы разобраться. Вторая проблема — это мобильные коды. В конце 80-х такого понятия как вирус не было, но, тем не менее, в серьезных организациях было выработано определенное требование: настоятельно не рекомендовалось использовать в программах самомодифицируемые сегменты. Это было достаточно модно, потому что памяти не хватало и приходилось ее экономить. Программисты писали код таким образом, что программа в зависимости от исходных данных могла сама себя модифицировать и по-разному реагировать на исходные данные. Это идеология вирусов.

С одной стороны, такой подход позволяет в определенных ситуациях достигнуть большей эффективности и функциональности, но с другой, появляется неуверенность в том, какую функциональность программа несет в данный момент. Это значит, что наличие элементарной ошибки в коде может привести к такой модификации программы, которая приведет к порче информации или другим последствиям.

Поэтому, наверное, технологии работы с мобильным кодом можно отнести к разряду перспективных. Необходимо выработать определенные правила, чтобы быть уверенным, что в любой заданный период времени программ будет выполнять заданные ей функции.

CNews: *В каком направлении, на ваш взгляд, будет развиваться рынок ИБ России в ближайшие годы? Какие факторы будут определять спрос на средства ИБ в крупных организациях и среднем бизнесе?*

Александр Соколов: Определенно могу сказать, рынок будет расти. Причина общая, независимо от того, крупная компания или нет: все больше и больше владельцев информации правильно ее оценивают.

Спрос на решения проблем ИБ в крупных организациях, кроме прочего, определяется еще одним важным моментом. Такие организации относятся к топливно-энергетическому комплексу, телекоммуникациям, машиностроению и являются стратегически важными для любого государства. Это означает, что в них будет часть информации, на которую государство накладывало и будет накладывать ограничения. Кроме того, перед большинством крупных компаний рано или поздно возникает вопрос выхода на международный рынок. В этом случае начинают работать международные правила, и компаниям необходимо выполнять определенные требования к стандартизации информационной структуры, неотъемлемой частью которых являются требования по информационной безопасности.

CNews: *Спасибо.*
