РЫНОК УСЛУГ И ЕГО ИГРОКИ

Максим Филиппов,
ОАО «ЭЛВИС-ПЛЮС»

Журнал "Сети", №11-12, 2003 г.

Уже не первый год российский бизнес в сфере информационной безопасности (ИБ) демонстрирует устойчивый рост, причем не только в отношении продаж средств защиты. Постоянно увеличивается спрос на услуги обеспечения ИБ, расширяется спектр оказываемых услуг.

Отметим: рынок сервисов в данной области моложе рынка средств защиты, поэтому неудивительно, что потребление услуг растет более высокими темпами, чем спрос на готовые продукты. На сегодняшний день уже можно сказать, что определен перечень основных технологий защиты информации, и сенсационные изменения в нем не предвидятся. Но поскольку отечественный рынок услуг в этой сфере не закончил своего формирования, определены еще не все его ключевые игроки.

Постоянное расширение спектра услуг вызывает необходимость в их классификации, которую удобно провести на базе модели, разработанной специалистами компании ЭЛВИС+ (рис. 1). Ее преимущество заключается в обеспечении наглядности как взаимосвязей между услугами (поскольку существует рекомендуемая последовательность их оказания), так и возможных «точек входа» для заказчиков. На основании этой модели можно установить, какие услуги и в какой последовательности потребуются конкретному клиенту для достижения его целей, а какие окажутся для него пустой тратой денег.

Согласно данной модели, услуги обеспечения ИБ можно сгруппировать по следующим категориям:
- технико-экономическое обоснование;
- проектирование и реализация;
- ввод систем в эксплуатацию;
- консалтинг;
- аудит.

Важно отметить, что представленная модель позволяет не только классифицировать услуги, но и произвести сегментирование рынка ИБ с точки зрения как потребителей, так и продавцов. Сегментацию клиентов удобно проводить на основе сопоставления той или иной их категории с определенным набором «точек входа».

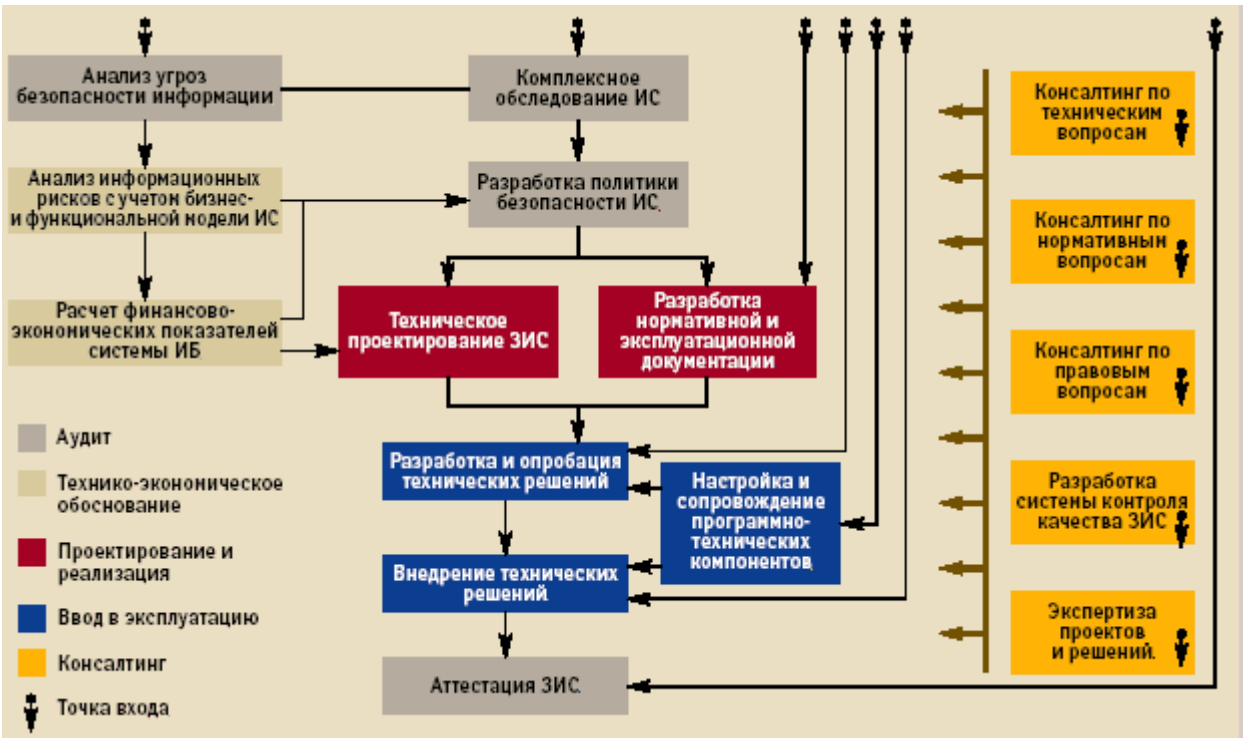

Рис. 1. Модель услуг компании ЭЛВИС+

Подобный анализ представляет интерес, в первую очередь, для самих игроков рынка, поскольку позволяет им выработать стратегию позиционирования. Кроме того, с его помощью можно оценить потребности любой фирмы в предлагаемых услугах и найти удовлетворяющую им «цепочку». При этом чем крупнее компания-заказчик и чем больше в ней осознают проблемы в области защиты информации, тем длиннее получается «цепочка» востребованных сервисов.

Очень интересно выявить ключевые принципы компетенции на этом рынке и провести анализ игроков, чтобы получить возможность прогнозирования дальнейшего развития событий. Кроме того, такой анализ позволяет дать потенциальным заказчикам начальные рекомендации по выбору оптимального поставщика услуги.

Итак, на российском рынке ИБ сформировались следующие группы игроков.

1. Системные интеграторы, специализирующиеся на построении систем обеспечения безопасности информации (СОБИ) и защищенных информационных систем (ЗИС); далее мы будем называть их системными интеграторами СОБИ.
2. Системные интеграторы, специализирующиеся на построении информационных систем (ИС); далее — системные интеграторы ИС.
3. Консалтинговые компании.
4. Производители средств защиты информации.
5. Провайдеры телекоммуникационных услуг.

Для всего рынка услуг ИБ характерна одна общая особенность: игроки, представленные в различных категориях, нередко выступают в качестве не конкурентов, а партнеров. Объяснить это достаточно просто. Как вы могли заметить, вместе со словосочетанием «информационная безопасность» зачастую используется слово «комплексная». С точки зрения рыночных игроков термин «комплексная ИБ» означает следующее: чем шире спектр предложений компании, тем более комплексный подход к обеспечению ИБ она предлагает. С другой стороны, по вполне понятным причинам заказчики хотят, чтобы допуск к их секретам получали как можно меньше сторонних фирм, поэтому стараются выбирать поставщиков услуг, способных решить максимальное число проблем защиты информации и данных.

Таким образом, за подобного рода партнерством рыночных игроков стоит стремление максимально полно удовлетворить потребности заказчика. Безусловно, это положительная тенденция. Но иногда партнерские отношения могут выстраиваться и внутри одной категории компаний-поставщиков. Дело в том, что, как уже говорилось, этот рынок только формируется, и спектр предложений постоянно меняется.

Другая особенность российского рынка услуг защиты информации — относительно невысокий уровень конкуренции. Как предложения, так и «стоящая за ними» методология различаются у большинства игроков. Поэтому конкурентная борьба возникает, как правило, лишь в тех случаях, когда условия для нее искусственно создаются заказчиком. В принципе, это логично, поскольку в рыночных отношениях соблюдается известный принцип «Кто платит, тот и заказывает музыку!».

Мы попробовали отобразить в таблице спектр предложений вышеуказанных групп игроков рынка ИБ. Конечно, приведенная сегментация рынка методом Чекановского позволяет получить лишь обобщенную картину — в каждом конкретном случае возможны варианты. Тем не менее подобное представление позволяет охарактеризовать текущее состояние отдельных сегментов и спрогнозировать дальнейшее поведение игроков. Для этого полезно рассмотреть взаимное расположение четырех выделенных сегментов рынка в обобщенной модели услуг (рис. 2), сопоставив с ними «точки входа», а соответственно, и группы потенциальных потребителей.

1. Красный сегмент. Его можно охарактеризовать как предварительный этап работ по созданию СОБИ. В этом сегменте между игроками идет серьезная борьба за каждого клиента. Причин тому несколько:

- основными потребителями услуг данного сегмента являются крупные корпоративные клиенты, которым необходимо еще перед началом работ получить четкое представление о «масштабах бедствия», оценить затраты на построение СОБИ и сопоставить их с возможными рисками при отказе от создания/модернизации СОБИ;
- как правило, завершив работу в красном сегменте, крупные фирмы продолжают создавать СОБИ заказчика, то есть переходят в синий, а затем и в желтый сегмент. Смена исполнителя работ осуществляется крайне редко.

В красном сегменте широко практикуются альянсы между различными категориями игроков (системные интеграторы СОБИ — системные интеграторы ИС — консалтинговые компании). За каждого крупного корпоративного клиента разворачивается серьезная конкурентная борьба, в которой обычно побеждает фирма (или альянс), способная предложить самый полный комплекс услуг.

2. Синий сегмент. В нем можно выделить две категории потребителей услуг:

- крупные корпоративные заказчики, которые перешли из красного сегмента и продолжают работы по построению СОБИ. Как уже отмечалось, они не склонны менять поставщика услуг;
- заказчики, которые начинают пользоваться внешними услугами в области ИБ именно с этого этапа. Как правило, существование «точки входа», привязанной к синему сегменту, обусловлено тем, что услуги красного сегмента являются достаточно дорогим удовольствием, и не всякая компания располагает соответствующим бюджетом. Часто практикуется такой подход: «У нас есть необходимость в построении СОБИ. Так давайте сразу приступим к делу! А количественные оценки эффективности и прочего оставим до лучших времен».

Тем не менее это не означает, что работы в области красного сегмента не проводятся вовсе. Например, обследование информационной инфраструктуры, предшествующее техническому проектированию, заказчик порой выполняет своими силами. Как альтернатива, он может попросить исполнителя реализовать данный этап работ бесплатно — под гарантии получения заказа на услуги, например, из желтого сегмента.

3. Желтый сегмент. Безусловно, он — самый емкий и насыщенный предложениями сегмент рынка. Косвенно это подтверждается тем наблюдением, что для него характерно наибольшее количество «точек входа» (см. рис. 1) и компаний-игроков (см. таблицу). Кроме того, здесь присутствуют все категории потребителей услуг информационной защиты, начиная от физических лиц и заканчивая транснациональными корпорациями.
Предложения в желтом сегменте непосредственно связаны с поставками средств защиты информации. В отличие от синего участка, в этом сегменте клиент, как правило, предпочитает получать услуги доработки, внедрения и сопровождения технических решений либо непосредственно от производителя, либо от его авторизованных партнеров.

4. Зеленый сегмент. Консалтинговые услуги, характеризующие этот сегмент, как правило, необходимы клиентам в течение всего цикла создания и эксплуатации СОБИ. Исключение составляет лишь аттестация — услуга, которая позволяет подвести итоговую черту и констатировать соответствие созданной СОБИ заданным требованиям либо определить ее «слабые места». Аттестация может проводиться на соответствие как руководящим документам (для государственных организаций), так и мировым либо корпоративным стандартам. Поскольку эта услуга является специализированной и поставщики должны иметь полномочия на ее оказание (в частности, лицензию органа аттестации), ее было бы правильно выделить в отдельный сегмент.

Остальные услуги зеленого сегмента обычно заказываются либо у компании, с которой клиент работал в красном и синем сегментах, либо у независимого консультанта. Исключение составляет услуга экспертизы проектов и решений, которую всегда оказывает независимый консультант.

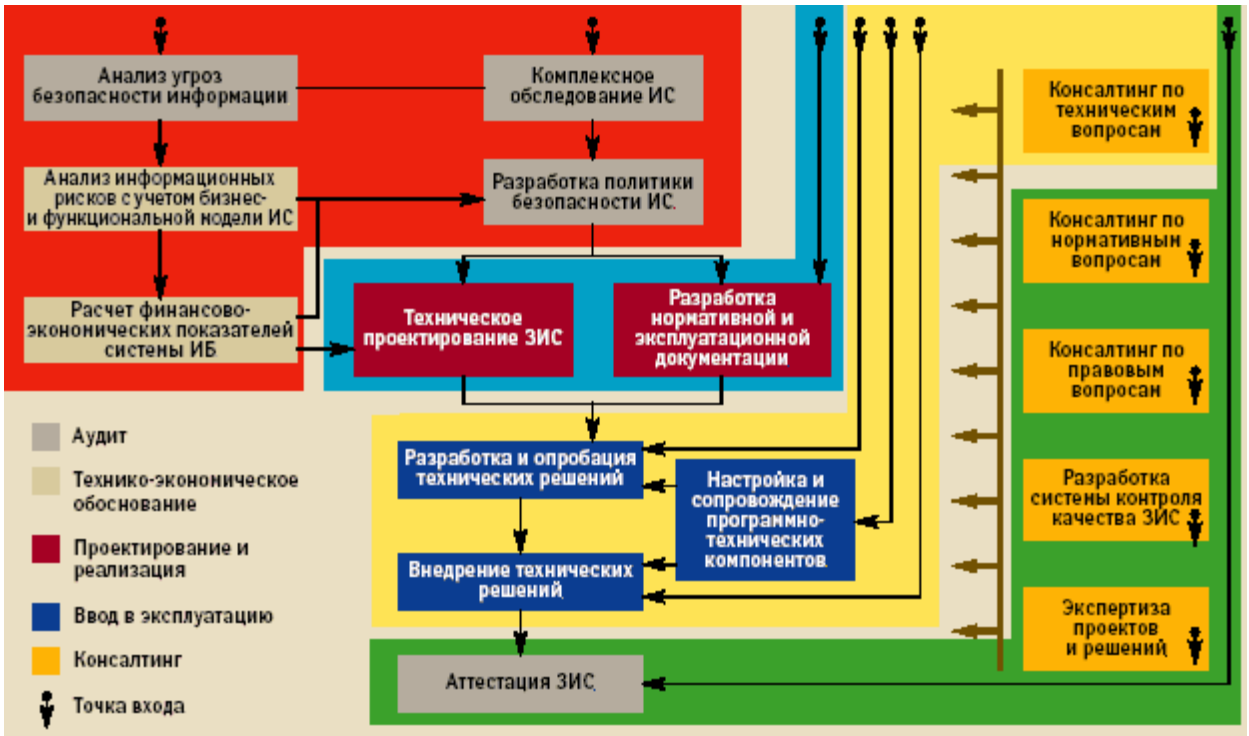

Рис. 2. Сегменты рынка на обобщенной модели услуг

Необходимо отметить, что каждую представленную в модели услугу допускается воспринимать как отдельный рынок. Следовательно, можно проводить более детальный анализ, определять игроков и потребителей такого рынка (но это выходит за рамки нашего обзора).

Перейдем к ключевым характеристикам рыночных игроков, которые необходимы для успешного продвижения услуг. На наш взгляд, таковыми являются известное имя и хорошая репутация компании, профессионализм сотрудников и опыт оказания аналогичных услуг, наличие собственных решений и ноу-хау в этой области, легитимность предлагаемых решений и услуг с точки зрения действующего законодательства, а также возможность тесного взаимодействия с государственными организациями, осуществляющими контроль на рынке ИБ.

Безусловно, список не возбраняется дополнять. Каждый заказчик при выборе поставщика услуг может самостоятельно расставить приоритеты в этом перечне. Например, сравнивать игроков по тем или иным критериям позволяет широко известный метод присвоения весовых коэффициентов.

	ПРЕДЛОЖЕНИЯ КОМПАНИЙ-ИГРОКОВ	Системные интеграторы СОБИ	Системные интеграторы ИС	Консалтинговые компании	Компании-производители средств защиты информации	Компании-провайдеры телекоммуникационных услуг	СЕГМЕНТИРОВАНИЕ РЫНКА	Системные интеграторы СОБИ	Системные интеграторы ИС	Консалтинговые компании	Компании-производители средств защиты информации	Компании-провайдеры телекоммуникационных услуг
Аудит	Анализ безопасности информации	+		+			Анализ безопасности информации	+	+	+		
	Комплексное обследование защищенности ИС	+	+	+			Комплексное обследование защищенности ИС	+	+	+		
	Разработка политики безопасности	+	+	+			Разработка политики безопасности	+	+	+		
	Аттестация ЗИС	+		+			Анализ информационных рисков	+	+	+		
Технико-экономическое обоснование	Анализ информационных рисков	+		+			Расчет финансово-экономических показателей системы ИБ	+	+	+		
	Расчет финансово-экономических показателей системы ИБ	+	+	+			Техническое проектирование ЗИС		+	+	+	
Проектирование и реализация	Техническое проектирование ЗИС	+	+			+	Разработка нормативной и эксплуатационной документации		+	+		
	Разработка нормативной и эксплуатационной документации	+	+				Настройка и сопровождение программно-технических компонентов ЗИС		+	+	+	+
Ввод в эксплуатацию	Настройка и сопровождение программно-технических компонентов ЗИС	+	+		+	+	Разработка и опробация технических решений		+	+	+	+
	Разработка и опробация технических решений	+	+		+	+	Внедрение технических решений	+	+	+	+	+
	Внедрение технических решений	+	+		+	+	Консалтинг по техническим вопросам	+	+			
Консалтинг	Консалтинг по правовым вопросам	+		+			Консалтинг по нормативным вопросам	+	+			
	Консалтинг по нормативным вопросам	+		+			Консалтинг по правовым вопросам	+	+			
	Консалтинг по техническим вопросам	+	+	+	+	+	Разработка системы контроля качества ЗИС	+	+			
	Разработка системы контроля качества ЗИС	+		+			Экспертиза проектов и решений	+	+			
	Экспертиза проектов и решений	+		+			Аттестация ЗИС	+	+			

Таблица. Вариант сегментации рынка методом Чекановского

Рассмотрим более подробно услуги в области ИБ, оказываемые телекоммуникационными провайдерами. Но вначале стоит вспомнить основные цели построения любой системы защиты информации: это обеспечение конфиденциальности, целостности и доступности хранимых и передаваемых по сетям данных.

Очевидно, что обеспечение доступности информации имеет прямое отношение к бизнесу компаний-провайдеров. А вот гарантии целостности и конфиденциальности данных — сопутствующие составляющие, посредством которых можно придать дополнительную привлекательность основному виду услуг. При этом деятельность провайдеров имеет самое непосредственное отношение к организации информационной защиты корпоративных клиентов. Действительно, им все равно, по какой причине они терпят убытки — будь то пожар или сбой телекоммуникационного оборудования. Кстати, согласно результатам опроса, проведенного компанией KPMG и журналом Contingency Planning & Management, 55% респондентов несли убытки именно из-за сбоев в телекоммуникационных системах.

Количественные оценки, характеризующие качество предоставляемых провайдером услуг, могут найти отражение в соглашении о качестве обслуживания (Service Level Agreement, SLA). К сожалению, на российском рынке телекоммуникаций далеко не все провайдеры стремятся взять на себя такие обязательства. Между тем подписание соглашения SLA имеет прямое отношение к обеспечению информационной безопасности клиентов.

Конечно, само по себе подписание SLA — не панацея. Необходимо предусмотреть меры и средства контроля за выполнением провайдером его обязательств. На случай их нарушения в SLA нелишне оговорить размер компенсации, предоставляемой клиенту при возможном ущербе. Кроме того, сегодня на российском рынке доступна услуга страхования информационных рисков. Иногда можно рассчитывать и на компенсацию ущерба, вызванного сбоями телекоммуникационного оборудования.

Вернемся к рассмотренной выше модели сегментации рынка услуг обеспечения ИБ. Присутствие компаний-провайдеров в этой сфере можно объяснить следующим: защита де-факто стала неотъемлемой частью технологий, применяемых в телекоммуникационных системах. Межсетевое экранирование, обнаружение вторжений, виртуальные частные сети, антивирусная защита, аутентификация, анализ защищенности, мониторинг и управление — вот далеко не полный список технологий защиты информации, которые продвигают (а зачастую и интегрируют в собственные решения) производители телекоммуникационного оборудования.

Поэтому нет ничего удивительного, что большинство предложений провайдеров относится к желтому сегменту рынка, услуги которого непосредственно связаны с поставками средств защиты информации. Реализация услуг этого сегмента имеет следующую последовательность: предложение технических решений — их тестирование клиентом — внедрение — техническая поддержка. Спектр предлагаемых провайдерами технических решений, как правило, ограничивается приведенным списком технологий защиты информации. Можно сказать, что на сегодняшней день абсолютное большинство предлагаемых провайдерами средств защиты и сопутствующих услуг обеспечивают решение задачи «защиты периметра».

Тем не менее, в отличие от большинства рыночных игроков, провайдеры имеют чрезвычайно привлекательное для конечного пользователя достоинство — наличие службы технической поддержки, функционирующей в режиме 7x24. Если клиент готов передать администрирование и сопровождение средств защиты периметра в ведение провайдера, он обеспечивает себе единую «точку входа» для решения проблем с каналами передачи информации — будь то сбои телекоммуникационного оборудования или вторжения злоумышленников во внутрикорпоративную сеть. Соответственно, это является безусловным маркетинговым преимуществом данной категории игроков.

Теперь приведем несколько вопросов, ответы на которые помогут компаниям-заказчикам сделать правильный выбор при передаче функций управления их системами безопасности в чужие руки.

- Насколько безопасна собственная сеть поставщика услуги и чем это подтверждается?
- Как решаются вопросы обеспечения физической безопасности? Как осуществляется и чем защищен доступ к консолям управления соответствующими средствами?
- Имеют ли специалисты провайдерской компании сертификаты на администрирование средств защиты?
- Какова периодичность обновления программного обеспечения средств защиты информации, антивирусных баз, сигнатур атак и т. п.?
- Разработан ли план восстановления после сбоев? Протестирован ли он? Определен ли процесс разбора инцидентов? Перефразируя слова Питера Нортона, можно сказать, что вопрос — не в том, случится ли инцидент с системой защиты информации, а в том, когда это произойдет и что будет сделано для устранения последствий.
- Какие методы, средства контроля защищенности и действия обслуживающего персонала приняты у провайдера услуг?

В случае положительного решения о передаче каких-либо функций управления безопасностью в аутсорсинг, необходимо подписать соглашение о конфиденциальности с поставщиком услуги. И помните, что в разглашении тайны прежде всего повинен тот, кто доверил ее другому.

В заключение выделим три ключевых фактора, от которых, на наш взгляд, зависит успех построения любой СОБИ. Во-первых, руководителям компании следует осознать проблемы защиты информации, а в идеале — и лично курировать выполнение проектов организации СОБИ. Во-вторых, нужно выделить отдельный бюджет для поддержки ИБ и контролировать его целевое использование. Руководство фирмы-заказчика должно воспринимать это как неотъемлемую часть процесса обеспечения ИБ. В-третьих, требуется создать рабочую группу, отвечающую за реализацию проекта создания СОБИ, члены которой обладают необходимой квалификацией и знаниями в области ИБ.
