Обзор рынка информационной безопасности Украины

Ткаченко Владимир
Валентин Сисоєв, CISM

План

1. Структура рынка информационной безопасности

Начнем с очевидных фактов – рынок информационной безопасности в Украине существует и развивается, несмотря на общую неблагоприятную рыночную обстановку. В нашем понимании участниками рынка информационной безопасности (ИБ) кроме потребителей и поставщиков услуг и решений, также выступают украинские и международные регуляторы. Еще участниками можно считать новый для Украины сегмент страхования рисков информационных технологий (услуга на Украине только начала развиваться). На Рисунок 1 приведена структура современного рынка ИБ Украины.

Рисунок 1. Структура участников рынка информационной безопасности Украины

1.1. Страхование рисков

Рассмотрим каждую группу игроков рынка более детально. Начнем с «темной лошадки» - страхования рисков информационных технологий (ИТ). В основу страхования ответственности за риски ИТ положены:

- нарушение прав интеллектуальной собственности на информацию;
- порча или утрата информационных активов ;
- предоставление некачественной и недостоверной информации;
- создание некачественных информационных систем или процессов и средств их обеспечения;
- нарушение процессов и правил формирования информационных активов;
- нарушение процессов и правил подготовки, предоставления и получения информационных продуктов и услуг, несвоевременное предоставление информации, или необоснованный отказ в предоставлении информации.

Страхователями информационных рисков при этом могут быть юридические и физические лица, имущественный интерес которых связан с владением, распространением, использованием и распоряжением информацией либо информационными активами.

К сожалению, на данный момент большинство этих услуг недоступно на украинском рынке (либо попытка найти поставщиков таких услуг превращается в детективную историю).

1.2 Регуляторы рынка

С регуляторами рынка ситуация более менее прозрачна, хотя мягко говоря неоднозначна. Любые работы, продукты или услуги в сфере информационной безопасности (в варианте украинского законодательства – сфера защиты информации) являются предметом лицензирования. Органом, выступающим регулятором в данной сфере и, соответственно, выдающим лицензии является Государственная служба специальной связи и защиты информации в Украине (www.dsszzi.gov.ua). Объектами лицензирования является деятельность в сфере технической и криптографической защиты информации. Данная организация больше ориентирована на регулирование защиты информации, составляющей государственную тайну, либо являющейся собственностью государства, поэтому сектор коммерческой и банковской тайны остается вне зоны внимания данного ведомства.
Вопросы обеспечения банковской тайны находятся в сфере регулирования Национального банка Украины, который на протяжении нескольких лет весьма последовательно и успешно внедряет международные подходы к обеспечению информационной безопасности. Единственным слабо отрегулированным участком остается коммерческая тайна предприятий. Также некоторое влияние на рынок ИБ в Украине оказывают международные регуляторы в лице Комитета по безопасности индустрии платежных карт PCI SSC, международные биржевые структуры (требующие соответствия нормативным актам SOX 404, Basel II или международным стандартам ISO 27001, PCI DSS и др.).

1.3 Поставщики услуг и решений ИБ

К поставщикам услуг и решений по ИБ отнесем все компании, специализирующиеся на продаже и интеграции продуктов информационной безопасности (программных и аппаратных), компании производящие продукты (программные и аппаратные) и аудиторские компании, осуществляющие аудит и консалтинг по вопросам ИБ. Для Украины характерной особенностью является тот факт, что пересчитать узкоспециализированные компании можно по пальцам руки. В основном компания интегратор, предлагает продукт или решение и аудит ИБ после его внедрения, что в корне неверно, так как в данном случае она является заинтересованной стороной. Также характерно, что поставщики услуг стремятся решить абсолютно все вопросы в сфере ИБ заказчика, например, проектируя систему обнаружения вторжений в сеть, внедряют систему видеонаблюдения за периметром и одновременно продают антивирусное программное обеспечение (ПО). После этого проводят аудит на соответствие стандартам информационной безопасности. Такая ситуация удобна для потребителя, так как управлять несколькими процессами с одним поставщиком на первый взгляд легче, но с другой стороны – отсутствие контроля и специализации приводит к некачественной реализации отдельных задач, повышенным затратам и затянутым срокам внедрения.
Существует также группа услуг по обучению или повышению квалификации персонала потребителей услуг ИБ. Услуги тренингов в основном предлагаются либо консалтинговыми специализированными компаниями, либо системными интеграторами, как дополнительная услуга в рамках внедрения решений по ИБ.

1.4 Потребители продуктов и услуг ИБ

Потребителей можем разделить по сегментам рынка следующим образом:

- государственный сектор (государственные предприятия и органы управления, военные формирования и др.);
- банковский сектор (банковские и другие финучреждения);
- коммерческий сектор (предприятия различных форм собственности и секторов экономики).

В коммерческом секторе необходимо выделить подгруппу телекоммуникационных компаний, так как их деятельность регулируется и лицензируется отдельной группой законодательных и нормативных актов,

которые зачастую содержат специфические требования по обеспечению ИБ. К телекоммуникационным компаниям следует отнести операторов сотовой и фиксированной связи, провайдеров Интернет, контент-провайдеров и другие компании, чья деятельность регулируется Национальной комиссией по вопросам регулирования связи Украины (НКРС).

1.5 Основные игроки рынка ИБ

Попытаемся теперь более детально рассмотреть основных игроков рынка ИБ на Рисунке 2.

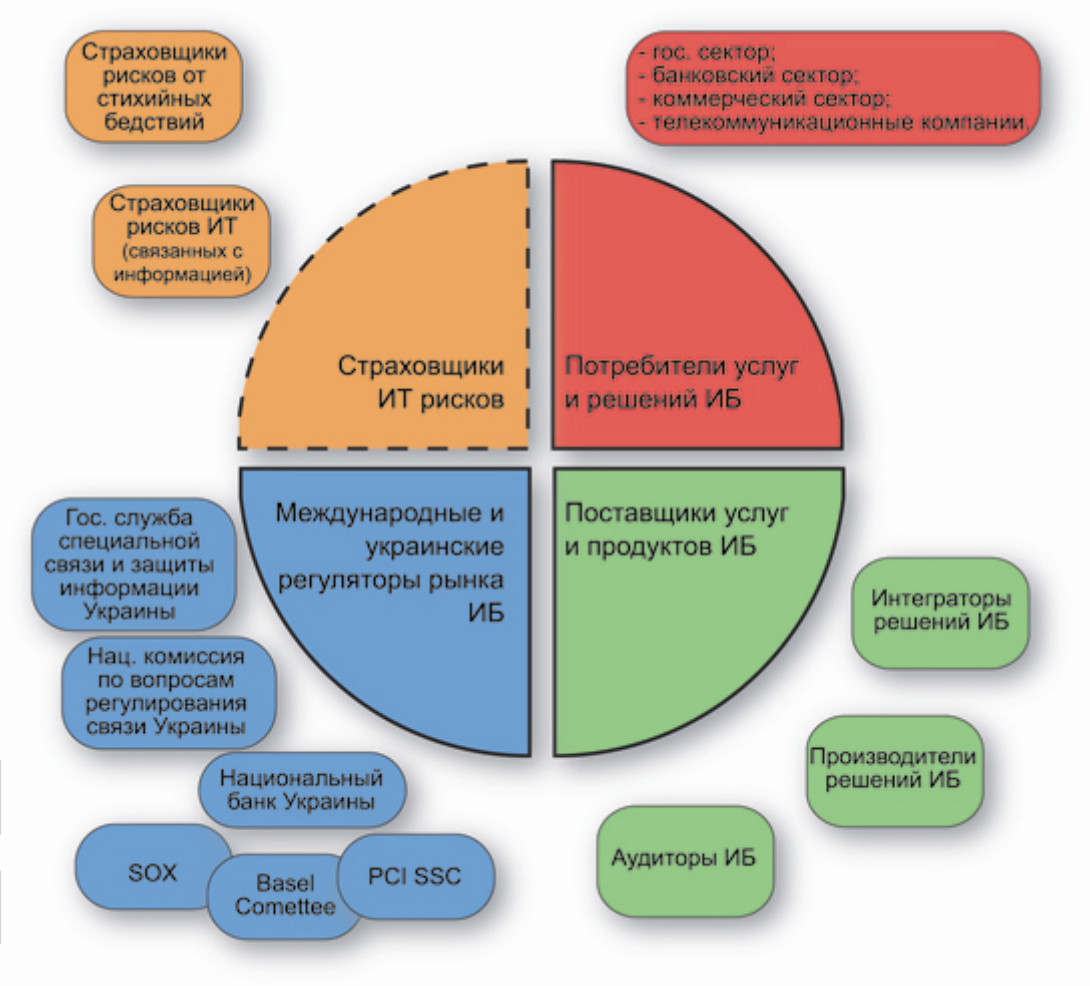

Рисунок 2. Участники рынка информационной безопасности Украины (вариант).

Итак, за исключением рынка страховщиков информационных рисков, в целом рынок ИБ в Украине в основном сформирован и достаточно успешно развивается.

2. Проблемные аспекты рынка информационной безопасности Украины

На наш взгляд основными проблемами для рынка информационной безопасности сегодня являются:

- отсталость законодательства в вопросах регулирования защиты информации составляющей коммерческую тайну;
- психологическая проблема менеджмента большинства компаний (сначала инцидент ИБ должен нанести ущерб и только после этого начинаются мероприятия по защите информации);
- отсутствие действенного механизма оценки бренда (неспособность оценить репутационные риски для компании);
- нечеткое сегментирование рынка ИБ и, как следствие, непрозрачное ценообразование.

Законодательная и нормативная база достаточно прозрачно регламентирует вопросы, относящиеся к государственной и банковской тайне. Оба регулятора разъяснили и внедрили действенные механизмы по защите информации в подотчетных учреждениях. На первый взгляд все просто – есть гостайна или конфиденциальная информация, которая является собственностью государства, будьте добры построить комплексную систему защиты информации. Если вы решили заняться банковским делом – Национальный банк через органы надзора также проверит соответствие вашей инфраструктуры его постановлениям. Нацкомиссия по регулированию связи также выдвигает некоторые требования, в основном по обеспечению, непрерывности услуг к своим подопечным операторам и провайдерам.

Однако картина не такая радужная, если посмотреть на нормативное поле Украины внимательнее. В переносном смысле это «поле» обильно усеяно «минами» законодательных ловушек и опутано «колючей проволокой» противоречий. Большинство нормативных актов, в том числе ГОСТов были приняты в конце 90х – начале 2000х годов и достаточно сложно применимы в современной многофункциональной среде, с которой имеют дело начальники департаментов и отделов ИБ или ИТ. Некоторые нормы остались неизменными со времен их утверждения Гостехкомиссией СССР. Стандарты по разработке и внедрению ИТ систем и систем ИБ применяются также без изменений со времен СССР. Некоторые компании-интеграторы просто игнорируют их требования, так как внедрение системы может затянуться на годы, а молодые специалисты – основные исполнители проектов по ИБ, даже не знают об их существовании. Международные стандарты носят в Украине рекомендательный характер, что в современных условиях означает - раз не требуется, значит не обязательно.

Здесь мы подошли вплотную к психологическому аспекту информационной безопасности. Он заключается в инертности менеджмента предприятий, так как основная задача любого бизнеса – зарабатывать деньги. Затраты на ИБ представляются в данном случае как инвестиции с неочевидным результатом (пока гром не грянет, мужик не перекрестится). Но после зарабатывания денег почти никто не вспоминает о том, что заработанное надо сохранить, а это и есть одна из основных задач ИБ. Поддержание требуемого уровня конфиденциальности, целостности и доступности информации для бизнес процессов – важнейшие задачи системы управления ИБ.

Также существует определенная степень заблуждения менеджмента относительно того, что внедрение проектов ИБ является дополнительной задачей ИТ департамента компании. На самом деле как проекты ИТ, так и проекты ИБ не могут реализовываться без вмешательства в систему управления компанией и/или бизнес процессами компании.

Также, спокойствие менеджмента, вероятней всего, основано на невозможности определить и количественно или качественно выразить репутационные риски компании связанные с потерей конфиденциальных данных или с простоями систем. Недавний пример с системой приема моментальных платежей iBox показывает, насколько разрушительным для репутации может оказаться перерыв в работе. Глядя на мировой тренд угроз информационной безопасности, следует задуматься, может не стоит ждать пока грянет гром?

(Источник Initial consolidated results. Information Security Forum Benchmark.)

И самой важной, на наш взгляд, проблемой является отсутствие сегментирования или классификации рынка ИБ. Сегодня на рынке работают несколько категорий компаний предлагающих услуги ИБ – это филиалы достаточно известных международных компаний в сфере ИБ, локальные компании с собственным капиталом и, отдельно стоит также выделить российские компании. Вследствие такого представительного состава цены на одни и те же услуги могут довольно сильно отличаться. С другой стороны большинство решений в сфере ИБ являются уникальными и невозможно перед реализацией проекта сказать точную сумму как на выходе из супермаркета. Однако во всем мире принята практика понятного и прозрачного ценообразования, исходя из различных факторов, что на Украине реализовать относительно проблематично, пока все компании действуют сами по себе без какой-либо координации со стороны регуляторов или профессионального союза.
Добавляет неразберихи и тот факт, что многие интеграторы ИТ или смежных областей реализуют продукты и услуги в сфере ИБ. При этом данный бизнес не является для них профильным, и качество реализации оставляет желать лучшего.

3. Перспективы развития рынка информационной безопасности

Как это ни странно звучит, но 2010 и 2011 годы являются переломными для нашего рынка именно в сфере информационной безопасности. Прежде всего, благодаря инициативе Национального банка Украины, который принял отраслевой стандарт, основанный на положениях международного стандарта по ИБ ISO 27001. Таким образом, банковский сектор получит еще более прозрачные правила игры, а поставщики услуг и продуктов ИБ новые возможности по реализации проектов. Кроме того, усиливается влияние мировых тенденций по нейтрализации угроз ИБ, так как Украина не может оставаться слабым звеном в мировом информационном сообществе. Ожидается, что иностранными инвесторами и международными институтами будет оказываться давление с целью снижения вероятности основных угроз ИБ.
Также очевидно, что реализация проектов в сфере ИБ будет в основном осуществляться профессиональными компаниями, специализирующимися на узкой области ИБ. Менеджеры и ИТ директоры компаний будут руководствоваться парадигмой: «оценка рисков – аудит ИБ – внедрение продуктов и мероприятий по результатам аудита – сертификация на соответствие стандарту». Надеемся, что формула «что-то надо делать, давайте купим файрвол (антивирус, UTM, спам-фильтр…) нужное почеркнуть» канет в лету.