ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Экономические модели и аналитические аспекты информационной безопасности

Выполнила студентка 3 курса
механико-математического факультета
специальности компьютерная безопасность
Семенихина В. С.
e-mail: svarya@mail.ru
Научный руководитель
заместитель декана по учебной части
доцент Никитина Е. Ю.
e-mail: neyu@psu.ru

Пермь, 2009 г.

Оглавление

Введение

Ушедший 2008 год был ознаменован началом очередного кризиса, принявшего масштабы мирового. Столкнувшись с финансовыми проблемами, организации различных масштабов занялись оптимизацией своих расходов, в том числе и расходов на ИТ. По результатом исследования Intelligent Enterprise «ИТ в условиях кризиса» только 10% компаний не будут сворачивать активность использования компьютерных технологий на предприятиях. Из оставшейся части 80% заявили, что у них будут сокращаться капитальные вложения. Лидерство этого направления вполне ожидаемо, но отметим, что его обозначили не 100% компаний, сокращающих свою активность. Значит надо полагать, что кое-где капитальные вложения все-таки еще идут. Кризис одинаково равномерно влияет на такие направления развития, как выход на новые рынки и территориальная экспансия (более трети опрошенных компаний).

Сокращение активности и затрат компаний выливается прежде всего в урезание ИТ-бюджета, поэтому в исследование был включен вопрос: «Какое сокращение ИТ-бюджета вы прогнозируете в 2009 году?». Лишь чуть более четверти ИТ-директоров прогнозируют сохранение ИТ-бюжета на уровне 2008 года. А более 60% заявили о его сокращении, причем 39% — на 20% и более. Это разительно отличается от результатов предыдущих исследований, в том числе и весенних данных 2008 года.

В то же время, процесс повышения сложности информационных систем не прекращен, стало быть и затраты на ИТ будут расти. Сокращение же расходов возможно в случае оптимизации и тщательного учета всех статей расходов. Сегодня на предприятиях России нужно инициировать миграцию от существующей простой, но бесперспективной модели общей стоимости компьютерной и программной собственности к сложной и трудоемкой, но прогрессивной методике детального анализа всех составляющих расходов на информационные технологии. Это позволит управлять IT-затратами, тем самым увеличивая выгоду от использования информационных технологий на предприятии.

"В нынешнихусловиях структуризация процессов и упорядочение того, что уже существует для управления процессом обеспечения информационной безопасности в больших компаниях, выходит на первый план", говорит Евгений Дружинин, ведущий системный инженер компании "Крок".

Практический опыт этого крупнейшего отечественного интегратора говорит о том, что сейчас наиболее распространены два сценария развития событий – эволюционное развитие ИБ (в случае органического роста бизнеса) и интеграция компаний с разным уровнем зрелости в плане обеспечения ИБ (в случае строительства холдингов и сделок по слиянию-поглощению).

Первый вариант отличается необходимостью формализации и улучшения процессов обеспечения и управления ИБ. Во втором случае стоят другие задачи – формирование единого управляющего каркаса (поскольку в каждой компании могут существовать свои собственные схемы управления и несения ответственности за ИБ), а также упорядочение и выравнивание нормативно-технической документации в этой области.

Но общим для обоих вариантов, по мнению экспертов "Крок", является то, что необходима структуризация процессов ИБ. Что это дает? Во-первых, устраняются противоречия в управленческих и организационных составляющих процессов обеспечения ИБ. Во-вторых, достигается полнота в нормативно-методических документах (НМД). В-третьих, улучшаются механизмы обеспечения ИБ в свете постоянного появления новых угроз.

Исходя из теории, можно достичь полной безопасности только при условии неработоспособности решения в целом, и наоборот. В реальности существует некий компромисс, найти который с каждым годом становится все труднее.
И это не теоретические изыскания, а реалии сегодняшнего дня, когда обеспечение ИБ становится все большим тормозом при внедрении новых информационных систем. Вывод, который можно сделать на основе всего этого, - это необходимость использование менеджмента для оценки эффективности внедрения той или иной информационной системы в целом и подсистемы ее безопасности в частности. Тому, чем руководствоваться и какие критерии являются критически важными при управлении совокупной стоимостью владения, посвящена часть моей работы.

Безусловно, на стоимость защиты предприятий напрямую влияют риски, поэтому их оценку и план по обеспечению информационной безопасности целесообразно вести еще на начальных этапах проектирования будущей информационной системы предприятия. И продолжать данные мероприятия на всех этапах жизненного цикла предприятия. Даже если информационная система уже существует, необходимо произвести оценку целесообразности затрат при имеющемся наборе рисков и угроз.

Риски, вызванные постоянным развитием бизнеса во всем мире, эволюционируют так быстро, что специалисты по ИТ-безопасности не успевает адекватно отреагировать на них. Эксперты компании Ernst&Young посчитали эту тенденцию настолько важной, что даже включили слова "Отчет о расширяющейся пропасти" ("Report on Widening Gap") в название своего ещё в исследования 2005 года. В ходе изучения вопроса оценки рисков, я узнала о многообразии подходов и различиях в них. Факт взаимосвязи рисков и затрат на ИБ не вызывает ни у кого сомнения, по этому часть моей работы посвящена процессу анализа рисков.

Классификация предприятий с точки зрения ИБ

Для определения принадлежности предприятия к какому либо из классов, проводится анализ соответствия по следующим характеристикам для каждого типа:

- Использование ИТ в бизнес процессе – степень с которой предприятия используют ИТ в критичных бизнес процессах
- Технологический профиль – типы технологий используемых предприятием, ранжируя их от автономных персональных компьютеров (ПК) до универсальных ЭВМ (mainframe).
- Установление доверия – процесс, используемый предприятием для налаживания отношений со своим деловым партнером, т.е. “Знаю Ваш Клиент”
- Информационная ценность актива вне предприятия, или “Значение для Хакера” – ценность для хакера/внешней стороны, по отношению к предприятию, информационных активов если
- Покрытие ИБ – персонал и управление в месте, необходимые чтобы защитить информационные активы предприятия
- Удар при прорыве безопасности – воздействие на предприятие, в случае если безопасности была нарушена

Gartner Group выделяет 4 уровня зрелости компании с точки зрения обеспечения информационной безопасности (ИБ):

0 уровень	ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ; Финансирование отсутствует; ИБ реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам).
1 уровень	ИБ рассматривается руководством как чисто "техническая" проблема, отсутствует единая программа (концепция, политика) развития системы обеспечения информационной безопасности (СОИБ) компании; Финансирование ведется в рамках общего ИТ-бюджета; ИБ реализуется средствами нулевого уровня + средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (традиционные средства защиты).
2 уровень	ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для производственных процессов, есть утвержденная руководством программа развития СОИБ компании; Финансирование ведется в рамках отдельного бюджета; ИБ реализуется средствами первого уровня + средства усиленной

	аутентификации, средства анализа почтовых сообщений и web-контента, IDS (системы обнаружения вторжений), средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, положения, процедуры, регламенты и руководства).
3 уровень	ИБ является частью корпоративной культуры, назначен CISA (старший офицер по вопросам обеспечения ИБ); Финансирование ведется в рамках отдельного бюджета; ИБ реализуется средствами второго уровня + системы управления ИБ, CSIRT (группа реагирования на инциденты нарушения ИБ), SLA (соглашение об уровне сервиса).

По информации Gartner Group процентное соотношение компаний применительно к описанным 4 уровням выглядит следующим образом:

2001 год	2005 год	2008 год
0 уровень - 30% 1 уровень - 55% 2 уровень - 10 % 3 уровень - 5 %	0 уровень - 20% 1 уровень - 35% 2 уровень - 30 % 3 уровень - 15 %	0 уровень – 5 % 1 уровень – 40 % 2 уровень – 35 % 3 уровень – 20 %

Существующие методики оценки эффективности ИС

Достижение максимальных выгод от использования на предприятии информационной системы напрямую зависит от уровня управления затратами на информационные технологии на протяжении всего жизненного цикла системы. В понятие управления IT-затратами входят процессы их планирования, учета, анализа и контроля, а его целью является снижение показателей, характеризующих расходы и издержки. В момент снижения объемов финансирования, приоритетными задачами становятся оптимизация. Любое предприятие с помощью автоматизации стремится повысить эффективность ведения своего бизнеса. Оценка эффективности этих нововведений, как правило, и ложиться в основу изменений в управлении затратами на ИБ.

На сегодня существует три основные группы методов оценки эффективности ИС:

1. Финансовые методы.

- Экономическая добавленная стоимость (Economic Value Added, EVA)
- Полная стоимость владения (Total Cost of Ownership, TCO)
- Совокупный экономический эффект (Total Economic Impact, TEI)
- Быстрое экономическое обоснование (Rapid Economic Justification, REJ)

2. Качественные методы.

- Система сбалансированных показателей (Balanced Scorecard)
- Информационная экономика (Information Economics, IE)
- Управление портфелем активов (Portfolio Management)
- Система показателей ИТ (IT Scorecard)

3. Вероятностные методы.

- Справедливая цена опционов (Real Options Valuation, ROV)
- Прикладная информационная экономика (Applied Information Economics, AIE)

Опишем кратко каждый из приведенных методов.

Вероятностные методы

Во многих стандартах говорится о необходимости оценивать и отслеживать риски информационной безопасности. Однако как правильно это делать и, самое главное, как доказать руководству, что полученный результат действительно отражает действительность, а не является просто формальным умозаключением?

Отношение к риск-менеджменту и оценке рисков ИБ среди российских ИТ и ИБ-специалистов иначе как скептическим назвать сложно, и это отношение сложилось не на пустом месте. Традиционно ИБ находится либо в ведении ИТ-отдела, либо под крылом службы безопасности. При этом только в немногих компаниях вопросы ИБ находили поддержку и понимание руководителей высшего звена. Неумение специалистов по ИТ объясниться с высшим руководством, а порой и слабое знание предметной области не позволило им донести до руководителей правильное понимание необходимости оценки и мониторинга рисков, связанных с ИБ.

Сейчас уже ясно, что аудит, оценка рисков, оценка уязвимости, тесты на проникновение – это все совершенно разные вещи. Аудит есть не что иное, как проверка какого-либо объекта на соответствие заданным критериям, либо в более широком смысле – независимая проверка и подтверждение истинности заявлений руководства организации. Оценка уязвимости и тест на проникновение вообще относятся к проверкам, направленным скорее на определение состояния ИБ с технической точки зрения. Оценка рисков же имеет четко выраженную бизнес-направленность и проводится с целью определения необходимых мер защиты исходя из тех рисков, которым подвергаются наиболее ценные активы компании. Только она позволяет дать ответ на вопрос, почему здесь должно быть установлено именно это средство защиты, в такой конфигурации и в этой точке информационной системы.

Требования ИТ контроля устанавливаются таким образом что бы предприятие могло защитить себя от уязвимостей используемых технических и программных средств. Воздействия уязвимостей при эксплуатации могут быть классифицированы на пять типов угроз:

1. Нарушение границ – нарушение условия невмешательства
2. Обнаружение – нарушение конфиденциальности, авторизации и секретности
3. Изменение – нарушение целостности
4. Отказ от обязательств – нарушение условия невозможности отказа. Отказ в связи с отклонением действительности транзакции
5. Отказ в обслуживании – нарушение пригодности

Существует множество различных рисков ИТ-безопасности, в зависимости от специфики предприятия, соответственно необходимый уровень защиты также будет различаться. Факторы, влияющие на различие рисков:

- Культура управления – менеджеры желающие принять на себя более высокие бизнес-риски нуждаются в большем количестве информации об этих рисках.
- Классификация актива – планы по приобретению и слиянию, электронные активы, защищаемые законодательством о секретности и финансовые активы подвержены более высокому уровню угроз информационной безопасности, так как эта информация является наиболее желанной для недобросовестных сотрудников.
- Технологическая среда – предприятие не имеющие связи с Интернетом не нуждается в брандмауэре; большее количество автоматизированных процессов и сетевых соединений создают большее количество точек доступа подлежащих защите от несанкционированного доступа/вторжения.
- Внутренняя информация – техническая экспертиза не всегда может быть преобразована к аудиту информационной безопасности. Предприятие, возможно, не знает обо всей гамме угроз, которым оно подвержено и осуществление внешнего аудита может быть необходимым для полной защиты его среды.

Риск может быть измерен в зависимости от уровня воздействия (низкий, средний, высокий) для следующих типов потерь:

- Финансовых
- Конкурентного преимущества
- Юридических/Регулирующих
- Операционных/Отказа в обслуживании
- Репутации на рынке

В описанных ниже методах используются статистические и математические модели, позволяющие оценить вероятность возникновения риска. Анализ рисков предприятия.

Справедливая цена опционов (Real Options Valuation, ROV)

Методология ROV, созданная на основе удостоенной Нобелевской премии модели оценки опционов Блэка-Шоулза, направлена на определение количественных параметров гибкости. Данная технология позволяет оценить эффективность аренды, слияния, покупки и производства. Ее часто используют в качестве альтернативы стандартным процедурам составления бюджета и плана капиталовложений в условиях неопределенного состояния рынка и экономики, когда на передний план выступают параметры гибкости. Большинство компаний используют методологию ROV в качестве одного из элементов построения привычной всем системы финансовых показателей и показателей эффективности.

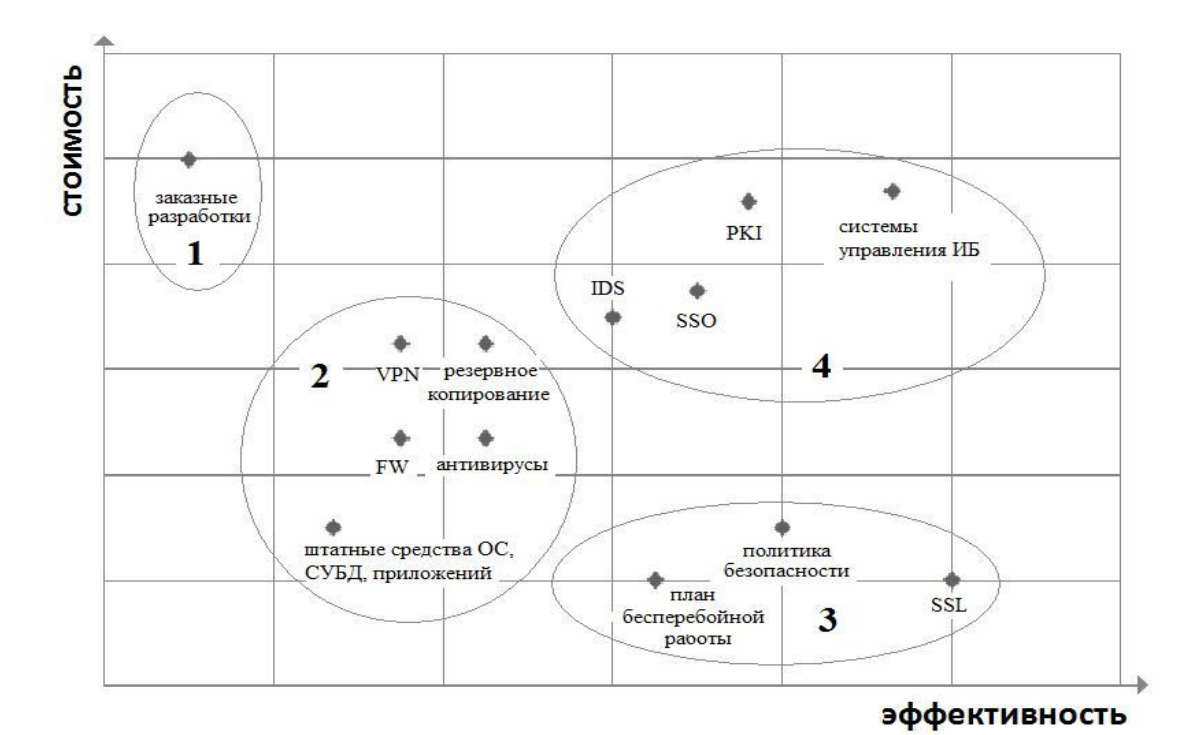
Прикладная информационная экономика (Applied Information Economics, AIE)

Этот метод хорошо подойдет тем, кто не доверяет скользящей шкале «эвристического» анализа риска методологии TEI, неуютно чувствует себя с однобокими рекомендациями модели TCO и не хочет делать ставку исключительно на модель Balanced Scorecard. Если вам нужна качественная, статистически верная методика анализа рисков, которая обезопасит руководителей, недостаточно хорошо владеющих предметом, то AIE - наилучший выход.

Эта методология объединяет достижения теории опционов, современной теории управления портфелем активов, традиционных бухгалтерских подходов (к которым относятся прежде всего NPV, ROI и IRR) и подстраховочных статистических методов, с помощью которых можно выразить неопределенность в количественных оценках, построить кривую распределения ожидаемых результатов, оценить риск и возврат на инвестиции. Для этой методологии характерен большой объем расчетов, а многие скептически относятся к сложным вычислениям. Но главным критерием все же является конечный результат, и с этим не поспоришь. Для дорогостоящих проектов методология AIE является удобным и статистически верным способом анализа рисков.

Качественные методы

Стивен Росс, директор Deloitte&Touche, предлагает следующий подход для оценки эффективности отдельных мер и средств обеспечения ИБ.



Исходя из приведенного графика видно, что наиболее дорогими и наименее эффективными являются специализированные средства (собственные или заказные разработки).

Ко второй категории относятся штатные средства защиты ОС, СУБД и традиционные средства защиты (уровень 0 и 1 по Gartner Group).

Наиболее дорогими, но в тоже время наиболее эффективными являются средства защиты 4 категории (уровень 2 и 3 по Gartner Group). Для внедрения средств данной категории необходимо использовать процедуру анализа риска. Анализ риска в данном случае позволит гарантировать адекватность затрат на внедрение существующим угрозам нарушения ИБ.

К наиболее дешевым, однако имеющим высокий уровень эффективности, относятся организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, план бесперебойной работы, положения, процедуры, регламенты и руководства).

Внедрение дополнительных средств защиты (переход на уровни 2 и 3) требует существенных финансовых вложений и соответственно обоснования. Отсутствие единой программы развития СОИБ, одобренной и подписанной руководством, обостряет проблему обоснования вложений в безопасность.

Хочется отметить, важность применения средств защиты в комплексе и в соответствии с некоторой моделью безопасности, которая строится на анализе угроз безопасности.

В методах, называемых еще эвристическими, предпринята попытка дополнить количественные расчеты субъективными и качественными оценками, которые позволяют определить ценность персонала и процессов.

Система сбалансированных показателей (Balanced Scorecard)

В рамках этой методики традиционные показатели финансовых отчетов объединяются с операционными параметрами, что создает достаточно общую схему, позволяющую оценить нематериальные активы: уровень корпоративных инноваций, степень удовлетворенности сотрудников, эффективность приложений и т. д. В методе Balanced Scorecard эти параметры рассматриваются с четырех точек зрения - финансовой, удовлетворения потребностей клиентов, внутренних процессов, а также дальнейшего роста и обучения. Менеджеры должны сопоставить перспективы каждого из этих четырех направлений с общей стратегией развития бизнеса.

Поскольку методология Balanced Scorecard прежде всего является инструментом формирования стратегии управления, она редко работает без непосредственного участия руководящего звена высшего уровня. Если компания пропускает первоначальный этап планирования стратегии ведения бизнеса с четкими причинно-следственными связями, все может закончиться определением параметров, которые не имеют непосредственного отношения к эффективности бизнеса. Критики методологии предъявляют обвинения в том, что она часто используется для оправдания каких-либо действий, а не для проведения ощутимых преобразований.

Информационная экономика (Information Economics, IE)

Методология Information Economics ориентирована на объективную оценку портфеля проектов и предусматривает направление ресурсов туда, где они приносят наибольшую выгоду. Идея заключается в том, чтобы заставить информационную службу и бизнес-менеджеров расставить приоритеты и представить более объективные заключения о стратегической ценности отдельных проектов для бизнеса.

Руководителям ИТ-отделов и бизнес-менеджерам сначала необходимо составить список из 10 главных факторов, влияющих на процесс принятия решения, и оценить относительную значимость («плюсы») и риск («минусы») каждого из них для бизнеса. Для каждого предприятия факторы будут своими, причем они могут добавляться, удаляться или изменяться по мере смены приоритетов. Проекты в области информационных технологий оцениваются с точки зрения данных факторов. В результате получается

полный относительный рейтинг каждого проекта в портфеле информационной службы. Методология IE - быстрый способ определения приоритетов затрат и сопоставления ИТ-проектов с бизнес-целями. Анализ рисков если и субъективен, то в достаточной степени детализирован. Эта методология не предназначена для управления проектами, поэтому предварительно руководителям информационных служб и бизнес-менеджерам необходимо пересмотреть существующие модели планирования и адаптировать их к процессу.

Управление портфелем активов (Portfolio Management)

Методология управления портфелем активов вобрала в себя многие положительные черты других подходов к оценке эффективности. Для достижения конечной цели организациям следует рассматривать сотрудников информационной службы и ИТ-проекты не как затратную часть, а как активы, которые управляются по тем же самым принципам, что и любые другие инвестиции. Это означает, что директор информационной службы осуществляет постоянный контроль за капиталовложениями и оценивает новые инвестиции по критериям затрат, выгоды и риска. Он должен минимизировать риск, вкладывая деньги в разные технологические проекты.

Перейти на использование подобной методологии не так просто. Если организация не хочет менять процедуры управления и не готова исповедовать новую философию работы с активами, преимущества Portfolio Management окажутся бесполезными. Кроме того, некоторое время уйдет на то, чтобы перестроить менталитет сотрудников.

Система показателей ИТ (IT Scorecard)

По мнению ряда специалистов, причинно-следственные связи в чистой модели сбалансированных оценочных ведомостей не работают. Некоторые перспективные направления к ней неприменимы, например управление знаниями и ростом. Методология Balanced Scorecard в чистом виде требует стратегической схемы, но ИТ-организации в большинстве своем имеют тактический характер, хотят они того или нет.

В качестве альтернативы существует подход, ориентированный на информационные технологии и направленный на привлечение ИТ-ресурсов к решению стратегических задач. Вместо четырех классических основных направлений сбалансированных показателей определяются следующие направления: развитие бизнеса, производительность, качество (для ИТ - как с внутренней, так и с внешней точки зрения) и принятие решений. Эта программа, обладающая весьма специфичным, многоуровневым подходом, будет верой и правдой служить принявшим ее долгие годы.

Традиционные финансовые методы

Эти методологии используют традиционные финансовые расчеты с учетом специфики ИТ и необходимости оценивать риск.

Для каждой из них существует несколько широко известных и употребляемых для расчетов моделей, которые отвечают некоторым требованиях. Как правило, современные модели безопасности строятся на основании анализа, включающего в себя:

1) Предположение безопасности;
2) Угрозы безопасности;
3) Политики безопасности;
4) Требования к средствам и методам реализации политик;
5) Требования доверия;

Модель безопасности должна быть построена на следующих принципах:

1. обеспечение конфиденциальности;
2. обеспечения целостности;
3. обеспечение наличия;
4. обеспечение аутентификации;
5. обеспечение авторизации;
6. обеспечение невозможности отказа;
7. аудита;
8. использование шифрования.

Экономическая добавленная стоимость (Economic Value Added, EVA)

В качестве основной характеристики EVA использует чистую операционную прибыль, из которой вычитаются соответствующие денежные затраты. При оценке, например, новой системы ERP методология EVA требует учета всех инвестиций, в том числе первоначальных денежных вложений, расходов на поддержку, затрат на внутреннее и внешнее обучение и т. д. Все эти расходы считаются платой за предполагаемую выгоду, которая будет способствовать увеличению оборота и снижению издержек.

Использование месячных, квартальных или годовых оценок EVA для характеристики эффективности работы отдельных подразделений позволяет согласовать подчас противоречивые цели, такие как рост оборота, увеличение доли продаж на рынке или движение денежных средств, с помощью единого финансового показателя.

Несмотря на достоинства, для многих информационных служб очень сложно на основе такого обобщенного взгляда принять решение, скажем, о покупке нового сервера без проведения промежуточных расчетов. Поэтому компании гораздо более комфортно чувствуют себя, отводя методологии EVA роль

лишь одного из показателей, который применяется наряду с другими методологиями оценки.

Совокупный экономический эффект (Total Economic Impact, TEI)

Методология совокупного экономического эффекта (Total Economic Impact) предназначена для поддержки принятия решений, снижения рисков и обеспечения «гибкости», то есть ожидаемых или потенциальных преимуществ, остающихся за рамками анализа преимуществ и затрат (cost-benefit analysis).

При оценке затрат руководители информационных служб оперируют тремя основными параметрами - стоимостью, преимуществами и гибкостью. Для каждого из них определяется свой уровень риска. Анализ стоимости обычно осуществляется по методу TCO. Оценка преимуществ должна проводиться с точки зрения стоимости проекта и стратегических вложений, выходящих за рамки информационных технологий. Гибкость определяется с использованием методологий расчетов фьючерсов и опционов, например моделей Блэка-Шоулза, или оценки справедливой цены опционов (Real Options Valuation). Для инвестиций в информационные технологии анализ рисков должен предусматривать доступность и устойчивость параметров производителей, продуктов, архитектуры, корпоративной культуры, объема и временных рамок реализации проекта.

Методология TEI нагляднее работает при анализе двух различных сценариев (например: разработка своими силами или покупка, продукты Oracle или продукты Sybase) особенно если два эти варианта сопряжены с построением инфраструктуры или реализацией других корпоративных проектов, чьи преимущества и недостатки оценить сложно.

Быстрое экономическое обоснование (Rapid Economic Justification, REJ)

Подобно TEI, методология Rapid Economic Justification, предложенная корпорацией Microsoft, предусматривает конкретизацию модели TCO за счет установления соответствия между расходами на ИТ и приоритетами бизнеса. Пятиступенчатый процесс требует: разработки бизнес-плана, отражающего мнение всех заинтересованных сторон и учитывающего основные факторы успеха и ключевые параметры эффективности; совместной проработки влияния технологии на факторы успеха; анализа критериев стоимости/эффективности; определения потенциальных рисков с указанием вероятности возникновения и воздействия каждого из них; вычисления стандартных финансовых показателей.

Методология REJ лучше подходит для управления отдельными проектами, а не их портфелем. Аналитикам и пользователям нравится оценка бизнеса, предусмотренная в REJ, ее базирующаяся на TCO платформа и наличие анализа рисков (хотя и субъективного). Однако, несмотря на «быстроту»,

присутствующую в названии, процедура REJ может оказаться достаточно продолжительной. Кроме того, многие организации не доверяют цифрам, которые оплачиваются производителем.

Совокупная стоимость владения (Total Cost of Ownership, TCO)

TCO - эффективный подход к определению наилучшего соотношения цена/качество для предприятий сферы услуг на основе рассмотрения таких ключевых бизнес-процессов, как восстановление после сбоев, управление модернизацией и техническая поддержка.

В рамках данного подхода предполагается оценка стоимости приобретения, администрирования, установки, перемещения и модернизации, технической поддержки и сопровождения, вынужденных простоев и других скрытых затрат. Сегодня данный подход приобрел достаточно широкое распространение. Подсчет полной стоимости владения стал стилем жизни многих руководителей технических подразделений, отдающих предпочтение беспристрастному анализу новых продуктов и обновлений. Производители оборудования могут заметно увеличить объемы продаж, если наделят продукцию возможностями снижения TCO.

Методология TCO очень хорошо подходит для подсчета текущих стоимостных параметров, с ее помощью можно достаточно полно проанализировать эффективность выполнения каких-то отдельных функций или набора функций. В сочетании с другими параметрами, применяемыми на практике, она позволяет получить удачную схему учета и контроля расходов на информационные технологии. Однако методология TCO не учитывает риски и не позволяет соотнести технологию со стратегическими целями дальнейшего развития бизнеса и решением задачи повышения конкурентоспособности.

В настоящее время специалисты компании Gartner, предложившей этот подход, работают над созданием более широкой версии TCO - совокупной оценки возможностей (Total Value of Opportunity, TVO), которая должна оказать более заметное влияние на эффективность капиталовложений.

Как показывает практика, именно данная методология получила максимальное распространение среди ИТ-менеджеров. Методология используется для анализа привлекательности информационных технологий, как объекта инвестиций. И просто для оценки одной из статей корпоративных расходов. Для того, чтобы понять мотивацию такого частого использования, необходимо изучить подробно преимущества данной методологии и конкретных моделей, применяемых на практике.

Модели подсчета ТСО

Кроме выявления избыточных статей затрат, целью подсчета совокупной стоимости владения является оценка возможности возврата вложенных в IT средств — анализ привлекательности информационных технологий как объекта для инвестиций. Кроме того, IT-менеджер сможет составить реальный, обоснованный IT-бюджет, который будет базироваться на количественных показателях. И наконец, совокупной стоимости владения может (и должна) использоваться в качестве одной из составляющих для финансовой оценки корпоративных затрат.

Однако следует отметить, что подсчет ТСО показывает только расходную, но никак не доходную часть. Если на предприятии уже функционирует информационная система, основанная на современных технологиях, или ее создание запланировано, то IT-менеджер должен быть "готов" сам и "подготовить" руководство к затратам, связанным с владением информационной системой. IT-затраты будут — и никто не в силах это изменить. Повлиять можно только на их структуру, избавившись от нецелесообразных и избыточных статей расходов. Данная задача должна ложиться именно на IT-менеджеров, которые обязаны реализовывать целевые корпоративные программы по оптимизации совокупной стоимости владения и постоянно вести работы по снижению IT-затрат.

Достичь оптимизации ТСО можно лишь за счет непрерывного управления IT-затратами. Большинство же компаний производят модернизацию существующих систем или начинают проекты по построению новых. И этот факт говорит о важности такого инструмента управления IT-затратами, как планирование совокупной стоимости владения.

Впервые вопросами подсчета стоимости владения (в упрощенном виде) занялась Gartner Group еще в 1987 году. Тогдашняя методика высокой точностью не отличалась и особого успеха не имела изза своего основного недостатка: отсутствия дифференциации между аппаратными платформами, операционными системами и сетями.

Образованной в 1994 г. фирме Interpose удалось за небольшой срок создать принципиально новую модель анализа финансовой стороны ИТ. Большой объем работы выполнила и Gartner Group, осуществившая трудоемкие анкетирования и исследования рынка, которые потом использовались для совершенствования модели.

Сейчас происходит миграция от бесперспективной модели общей стоимости компьютерной собственности к значительно более сложной и трудоемкой методике детального анализа стоимости всех составляющих затрат на информационные технологии. Это вызвано резким повышением сложности и

увеличением размеров корпоративных систем, что зачастую приводит к непрогнозируемому росту дополнительных затрат, вызванных широким спектром используемых технологий, а также существенно возросла и роль человеческого фактора.

Увеличения количества пользователей данной методикой управления затратами на ИТ и оценки эффективности ИС повлекло и развитие практической части. На ряду с моделью Garther Group, компания Microsoft создала собственную модель подсчета TCO. Для того чтобы понять какие принципиальные отличия этих методик, рассмотрим их поочередно.

Модель Microsoft

IT-затраты в TCO, разработанная компанией Microsoft совместно с Interpose, разбиваются на две категории:

- Прямые затраты — те, которые обычно учитываются при бюджетном планировании. У многих украинских предприятий нет возможности управлять своим IT-бюджетом, поскольку зачастую система бюджетного управления отсутствует как таковая. Прямые затраты, как правило, предусматриваются в бюджетах центрального IT-департамента, а также рабочих или проектных групп по поддержке и внедрению информационных технологий внутри производственных и административных подразделений. К ним относятся затраты:

    1) на аппаратное и программное обеспечение (покупка или аренда, новая установка или обновление и т. д.);
    2) на управление (сетевое и системное администрирование, проектирование);
    3) на поддержку (служба технической поддержки, обучение, контракты на поддержку и сопровождение);
    4) на разработку (постановка задачи и разработка приложений, документации, тестирование и сопровождение);
    5) на телекоммуникации (каналы связи и их обслуживание).

- Косвенные затраты — те, которые не поддаются планированию и часто даже не учитываются. Согласно исследованиям Interpose, они составляют свыше 50% средних расходов организаций на информационные технологии (см. диаграмму). К ним можно отнести:

    1) пользовательские затраты (персональная поддержка, неформальное обучение, ошибки и просчеты);

2) простои (потеря производительности из-за выхода из строя оборудования или профилактические плановые остановки работы).

Модель Garther Group

Каждая модель ТСО компании Gartner Group состоит из двух основных компонент:

1. Учетная карта предприятия
2. Технический сценарий

Модель ТСО для ИБ отличается от традиционной модели ТСО тем, что в ней есть третий компонент – сценарий безопасности.

Учетная карта ТСО для ИБ предприятия состоит из пяти основных разделов:

- Техническая часть
- Персонал
- Программное обеспечение
- Внешние службы
- Физическая безопасность

В свою очередь эти пять разделов подразделяются на следующие действия по безопасности – аутентификация, авторизация, защита кода и поддержка, реакция на Кибер-инциденты, мониторинг контента, управление цифровыми правами, кодирование, брандмауэры, программа информационной безопасности, фильтрация и мониторинг интернет контента, обнаружение вторжения, соответствие лицензии, регистрация, сообщение и аудит; Управление Враждебным Программным Кодом, Целостность Сообщения, Управление секретностью, Инфраструктура Открытых Ключей, Сортировка Записей и Хранение, Удаленный Доступ, Оценка Рисков, Управление Безопасностью, Архитектура Безопасности, Сертификация Стандартов,

Управление Операционными Инцидентами, Уязвимости, Оценка и Управление.

Технический сценарий – это номенклатура производимых предприятием товаров и услуг. Включает в себя:

1. Корпоративное резюме
    - Первичное географическое месторасположение
    - Производство
    - Суммарный доход компании
    - Совокупность конечных пользователей
    - Мобильный персонал
2. ИТ профиль
    - Используемая прикладная архитектура (например, клиент-сервер)
    - Используемый протокол для электронного обмена данными (EDI)
    - Способ подключения удаленных пользователей
    - Способ подключения индивидуальных удаленных пользователей
    - Используемые операционные системы
    - Техническая среда

Сценарий безопасности состоит из двух действий в рамках безопасности – это организация команды реагирования на Кибер-инциденты (КРКИ) и мониторинг контента.
Команда реагирования на Кибер-инциденты
Расходы на создание КРКИ включают:

- Технические средства
- Персонал
    - Фаза 1: Планирование
    - Фаза 2: Приобретение
    - Фаза 3: Внедрение
    - Фаза 4: Администрирование и управление стабилизацией цен
    - Фаза 5: Усовершенствование
    - Фаза 6: Отставка (КРКИ не будет устранена в течение, например 5-ти лет)
- Программное обеспечение
- Обучение
- Телекоммуникации

В сокращенной модели (чаще применяемой для подсчета ТСО) учитываются следующие IT-затраты: фиксированные, или, как их еще называют, капитальные вложения, и текущие. Их условно разносят по временной шкале: капитальные вложения осуществляются на этапе построения ИС, текущие затраты — на этапе функционирования. По методике Gartner Group к фиксированным следует относить следующие затраты:

- стоимость разработки и внедрения проекта;
- привлечение внешних консультантов;

- первоначальные закупки основного ПО;
- первоначальные закупки дополнительного ПО;
- первоначальные закупки аппаратного обеспечения.

Фиксированными эти затраты называются потому, что делаются, как правило, один раз, на начальных этапах создания ИС. При этом выбор той или иной стратегии, аппаратной и программной платформ весьма существенно влияет на последующие текущие затраты.

В свою очередь, текущие затраты состоят из трех статей:

- стоимость обновления и модернизации системы;
- затраты на управление системой в целом;

  Под "затратами на управление системой" подразумеваются расходы, связанные с управлением и администрированием компонентов ИС. В этой статье затрат можно выделить некоторые подкатегории:

  1) обучение административного персонала и конечных пользователей;
  2) заработная плата;
  3) привлечение внешних консультантов;
  4) аутсорсинг;
  5) учебные курсы и сертификация;
  6) техническое и организационное администрирование и сервис.
- затраты, вызванные активностью пользователей ИС ("активность пользователя");

  Стоимость обеспечения работы пользователя отражена в понятии "активность пользователя". Эта статья затрат, по данным Gartner Group, имеет наиболее значимый вес в совокупной стоимости ИС. В ней выделяют следующие подстатьи затрат:

  1) прямая помощь и дополнительные настройки;
  2) формальное обучение;
  3) разработка приложений;
  4) работа с данными;
  5) неформальное обучение;
  6) futz-фактор (параметр, определяющий объем затрат, связанных с последствиями некомпетентных действий пользователя).

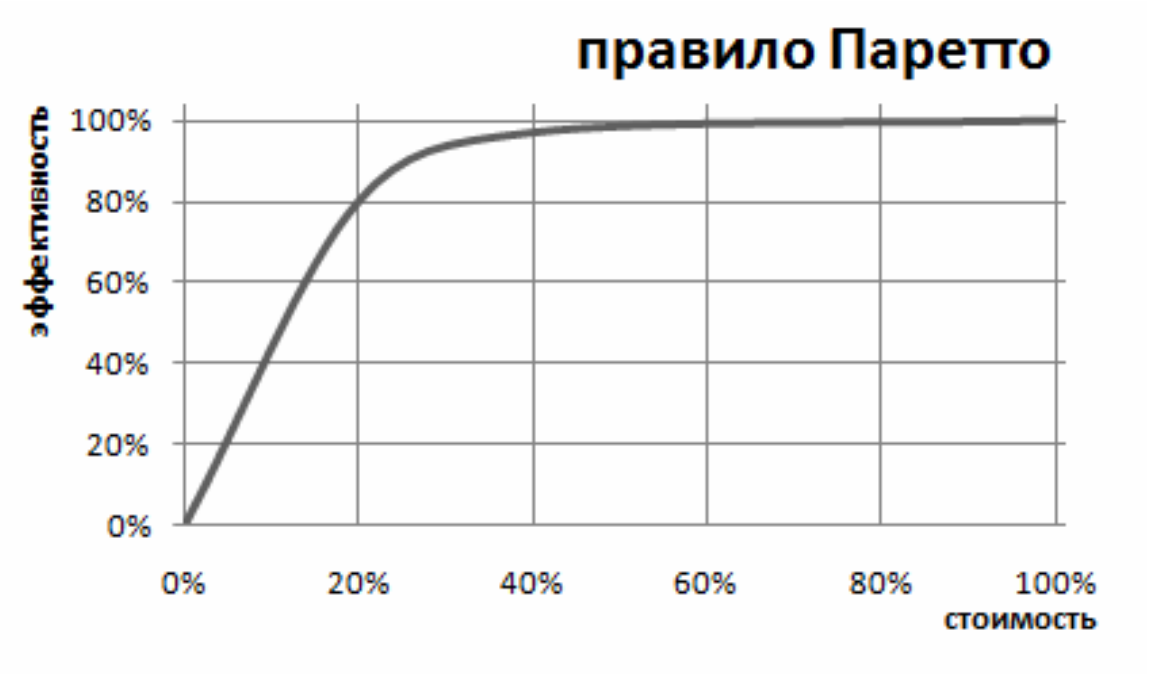
  Эти затраты связаны, например, с участием администратора в настройке рабочей станции, с оказанием помощи пользователю или с консультациями. По данным аналитических компаний, основные факторы, влияющие на итоговую стоимость владения информационными технологиями, на 75% обусловлены проблемами конечного пользователя.

Альтернативные варианты подсчетов ТСО

Несмотря на то, что уж существует несколько работающих моделей ТСО, было бы неверным сказать, что работа над созданием новых моделей не ведется. Не смотря на то, что существующие модели способны удовлетворить существующие потребности ИТ-менеджеров, поиск новых более удобных, рациональных и практичных методов не прекращен. Не редки статьи в СМИ с новой точкой зрения специалистов в области ИБ и экономики, с предложениями по изменениям концепции, подхода к подсчетам ТСО. В своей работе мне хотелось поделиться мыслями по поводу тому, какую пользу может оказать изменение угла обзора на подсчеты ТСО. К сожалению, данные подходы не имеют под собой реализованных моделей и базируются скорее на умозаключениях, чем на практическом применении.

Безопасность жизненного цикла информации в АС

Модель ТСО компании Garther Group, как было сказано ранее, имеет две части расходов. Их условно разносят по временной шкале: капитальные вложения осуществляются на этапе построения ИС, текущие затраты — на этапе функционирования. Можно расширить эту модель, и рассматривать затраты на всех этапах жизненного цикла. Выделение создания ИС оправданно, так как это этот этап обеспечивает эффективность всей системы. Если применить правило Паретто, то получим что 20% процентов затрат на ИС обеспечивают её эффективность на 80 %. В соответствии с тем, что взаимосвязь затрат на создание ИС и её эффективность однозначно и доказуема, стало быть что эффективность затрат можно оценивать по стремлению к изображенному графику.



Здесь затраты, понесенные при создании АС обеспечивают защищенность предприятия на 80 %.

Кроме этого стоит выделять такую часть как инвестиции, в котором стоит учитывать амортизационные отчисления на обновление материальной базы. Размер этой части определяет политику компании – количественные параметры инвестиций говорят о желании компании изменения класса имеющейся АС или же о том, что предприятие не заинтересованно в развитии, стараясь лишь поддерживать систему в работоспособном состоянии.

Самой затратной частью ИС всегда является поддержка, так как её размер зависит от человеческого фактора. Предотвращение рисков и угроз от человеческого фактора занимает огромное количество времени и усилий ИТ-специалистов, что сложно учесть при оценке совокупной стоимости владения. Эффективность обеспечения работоспособности и защищенности от этих затрат минимален, поэтому на мой взгляд целесообразнее инвестировать денежные средства в повышения уровня квалификации пользователей АС, чем увеличивать персонал, занимающийся поддержкой пользователей. Рост штата не ведет роста уровня навыков, а в случае повышения квалификации количество нежелательных событий в АС, совершенных по неосторожности ли не знанию, снижается, что имеет в перспективе больший экономический эффект.

Зависимость класс АС – расходы на ИБ

В соответствии с РД «АС. Защита от НСД. Классификация АС и требования по защите информации», определено 9 классов защищенности АС от НСД к информации и три группы, в которые объединены классы в соответствии с особенностями обработки информации классами в группе. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. На основании этого внутри группы можно выбрать так называемый базовый класс, имеющий некоторую стоимость владения. Остальные классы в группе будут являться расширенными видами базового класса, так как наряду с его требованиями к ним будут выдвинуты дополнительные. Таким образом, возможно определение стоимости перехода от одного класса к другому путем подсчета затрат на обеспечение дополнительных требований.

Критически важными остаются такие параметры как размеры предприятия, его территориальная разрозненность и класс АС. Обладая этими сведениями, уже возможно предопределить порядок финансовых затрат, относящихся к ТСО. Кроме этого, возможным становится контролировать объем средств, приходящихся на соблюдение того или иного требования. Имея отчеты о нарушениях или утечках информации и соотнеся их расходами на выполнения требований, возможно определить, насколько эффективными являются вложения в данное направление. В случае, когда объем инвестиций

и без того велик, что никаким образом не сказывается на соблюдении одного из требований и политик безопасности, однозначным является вывод о нерациональном использовании денежных средств и неэффективности принятых мер. Это может послужить первым сигналом к перестроению системы безопасности предприятия, или о принятии решения о пересмотре методов выполнения требования. Кроме этого стоит обратить внимание на расходы, если совокупная стоимость владения базового класса в группы предприятия выше, чем расширенного. В таком случае имеет смысл говорить о недостаточной оснащенности АС расширенного класса или о избыточных расходах на АС базового класса.

Рассмотрение расходов на ИБ как страховку

Последние несколько лет в сфере информационной безопасности наблюдается общая тенденция к отнесению затрат на безопасность в категорию инвестиций. В западной прессе даже придумали специальный термин - ROSI (Return on Security Investment), то есть прибыль на инвестированный в информационную безопасность капитал. Данный термин был образован в качестве производной от термина из финансовой сферы ROI (Return on Investment), обозначающего отношение среднего увеличения прибыли к объёму инвестиций. Ключевым в данном определении является слово "прибыль".

Все же описывать затраты на информационную безопасность как инвестиции означает неправильно истолковать значение инвестиций. Невозможно получить прибыль в ответ на затраты в сфере информационной безопасности, можно лишь сэкономить часть денег. В результате ROSI - искусственный, некорректный термин, использование данного подхода является попыткой обратиться к желанию руководителей извлечь прибыль из инвестиций. Затраты на информационную безопасность - это именно "затраты".

Противники последнего утверждения обычно приводят в качестве аргумента то, что "возврат" инвестиций происходит за счет предотвращения возможных потерь. У подобного подхода существуют фундаментальные проблемы - невозможно рассчитать финансовые потери, которые были предотвращены, предотвращение потерь не равносильно созданию прибыли.

Как оценить финансовый результат того, что не было потеряно? Можно провести сложный, комплексный анализ и описать сценарии того, что могло бы произойти, возможные потери, и как меры информационной безопасности, внедренные (или предлагаемые), помогли предотвратить потери. Однако в нашем меняющемся мире, в условиях появления все новых и новых типов атак это было бы крайне затруднительно. А деньги, выделяемые на информационную безопасность - не создают новых денег.

Намного лучше относить затраты на информационную безопасность в другую финансовую категорию, куда они действительно подходят - страховку. Это особая сфера перераспределительных отношений по поводу формирования и использования целевых фондов денежных средств для защиты имущественных интересов физических и юридических лиц и возмещения им материального ущерба при наступлении неблагоприятных явлений и событий, именуемых страховыми случаями.

Страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий) (ст. 2 закона РФ "Об организации страхового дела в Российской Федерации").

Специалисты в области ИБ отвечают за защиту ресурсов организации, что очень хорошо подходит под определение страховки. Единственная разница, что по сравнению с существующим страхованием от потерь не обязательно передается третьей стороне.

Рассмотрим данный подход подробнее. Информационная безопасность, также как и страховка, начинается с управления рисками. Первый этап в управлении рисками - идентификация и оценка ресурсов, которые следует защищать (страховать) от возможных потерь. Без знания о том, что мы хотим защищать и каковы угрозы, мы не узнаем какие защитные меры предусмотреть, что купить и внедрить. А без оценки стоимости защищаемого ресурса мы не будем знать приемлемое количество средств (страховую премию) которые можно потратить.

Поскольку после идентификации и оценки ресурсов мы уже знаем, что нам необходимо защищать, кроме того, мы знаем стоимость данных ресурсов, будь это база данных или центр обработки данных целиком. Значит, мы можем использовать методологию управления рисками для того, чтобы определить приемлемое количество денег, которые необходимо потратить (а не инвестировать) для защиты данных ресурсов.

Ни одна из указанных защитных мер не генерирует новые деньги; напротив - только потребляет их. Также как страховка автомобиля или квартиры. Тем не менее, для организаций подобная страховка в области информационной безопасности имеет определенную ценность, так как снижает риск возможных потерь.

Страховая премия, которую мы платим за эту страховку - это совокупная стоимость владения соответствующей технологией. Часть данной премии обычно платится сразу, оставшаяся часть относится к текущим расходам.

Возможное возражение, которое может быть высказано по отношению к приведенной страховой модели ИБ: когда мы теряем застрахованный ресурс, страховая компания выплачивает нам денежное возмещение. Если же мы имеем дело с нарушением информационной безопасности, мы не получаем никакой компенсации. Однако в случае нарушения требований безопасности начнет работать группа по расследованию происшествия, которая в свою очередь является очередной мерой информационной безопасности. Если данная группа не сможет полностью прекратить нарушение безопасности, и мы продолжим нести потери, то можно будет применить "обычную" страховку как стандартную меру переноса рисков для покрытия убытков от потери ресурсов, прибыли и т.д. Полная цепочка защитных мер, начиная от физической и до технологической безопасности, фактически наша страховка от возможных потерь ресурсов компании.

Профессионалы в области информационной безопасности, работающие в больших организациях, могут счесть полезным привлечение профессиональных страховщиков к процессу управления рисками.

Вывод

Во времена благополучия, роста котировок, курсов и показателей доходности, вопросами оптимизации, достижения максимальной эффективности занимались скорее формально. В сложившейся же ситуации, когда большая часть компаний предполагает сокращение бюджетов на поддержание ИТ- средств на одну пятую (а то и больше), этот вопрос стоит максимально остро. Все больше риск-менеджеров обращается к таким показателям как TCO, TEI, и другие, в поисках способов максимально достоверно подсчитать все убытки, которые несут организации.

Кризис – время перемен, и самое подходящее время пристальнее взглянуть на то, куда и на что направляются денежные потоки. Сейчас, обращаясь к статьям расходов на ИТ в том числе, нужно понимать, что получишь в замен на эти расходы. Соотнесение рисков и той системы безопасности что существует – практический первый этап на пути оздоровления расходов на информационную безопасность. Что же в самом начале? Основой рассмотрения безопасности АС является анализ угроз и рисков.

В своей работе я рассмотрела, каковы угрозы и риски компаний в зависимости от зрелости их системы ИБ. Посмотрев на статистику Garther Group о процентном соотношении компаний различных уровней, радостным заключением стало то, что компании во времена бурного роста столь же активно развивали и свои ИТ-системы. И во времена суровой экономии на затратах, не являющихся основными при создании товара или услуги, многие будут довольствоваться лишь поддержанием существующей системы. Иногда этого будет достаточно, чтобы обеспечить безопасность информационной системы предприятия. И это прежде всего связанно с тем, что большее количество компаний (55%), имеют находятся на 2 и третьем уровне по уровню зрелости своих систем ИБ. Таким образом, эти компании смогут обеспечить прежнюю надежность системы даже при столь существенных сокращениях финансирования.

Но достижения какого-либо уровня безопасности предприятия не гарантируют сами по себе защищенности. Определяющим здесь является – соответствие мер с имеющимися угрозами. Если в ходе анализа было выявлено, что меры и затраты различаются, стоит задуматься о реструктуризации системы ИБ. Чем это чревато? В первую очередь, необходимо понять, какой объем денежных средств и на какие нужды необходим. Для этого существует несколько основных методологий подсчета различных показателей, от прикладной информационной экономики, помогающей при анализе рисков, до совокупной стоимости владения, которая позволяет оценить прямые и косвенные затраты, которые несет предприятие в связи с содержанием ИТ-системы.

Для удобства рассмотрения, эти методологии сгруппированы по целям назначения. Вероятностные методики приходят на помощь при анализе рисков, качественные – в случае необходимости оценки эффекта от затрат денежных средств на реализацию защиты от той или иной угрозы, и финансовые – при непосредственных денежных подсчетах. Хочется отметить, что качественные, позволяют являются очень наглядными для демонстрации какими методами и средствами нейтрализуются угрозы, и на сколько эти методы и средства являются оптимальными.

Не смотря на то, что подсчеты - весьма простая задача, но в случае информационной безопасности – это не так. Кроме прямых затрат, таких как расходы на приобретение технических и программных средств, имеются ещё такие расходы как простой и пользовательские затраты. Надеюсь, что в моей работе максимально доступно изложено что это за затраты и почему их необходимо учитывать. Кроме этого, вопрос подсчета затрат оказался не таким однобоким и простым, именно по этому существующие модели TCO обе имею право на жизнь и активно используются.

В ходе изучения существующих моделей и подходов компаний Garther Group и Microsoft, поняла, что они не отвечают всем потребностям и не отражают всех взглядов на вопросы безопасности. Предложенные мной три варианта угла рассмотрения этого вопроса должны пройти практические испытания, чтобы можно было сделать вывод о том, насколько они удобны в использовании и отвечают существующим потребностям в новых подходах.

Изученной и рассмотренный мной материал способен помочь на конечном этапе работы по анализу системы информационной безопасности, и рассмотренные мною модели и методы подхода к этому вопросы способны помочь упростить этап финансовых подсчетов. Разобравшись с ним, компании могут быть уверены, что расходы на ИТ не повредят их предприятиям, и смогут приносит только пользу в тяжелые времена финансовой нестабильности.

Литература

1) http://www.docflow.ru/analytic_full.asp?param=32184 –
2) http://www.citforum.ru/security/articles/ocenka_zatrat/www.citforum.ru - «Оценка затрат компании на Информационную безопасность», автор: Сергей Петренко;
3) http://www.ibusiness.ru/marcet/CIO/19102/ - «TCO: что это такое и как его считать», автор: Михаил Румянцев;
4) http://www.ibusiness.ru/marcet/CIO/19102/ ;
5) http://www.iemag.ru/researches/detail.php?ID=18230 - Исследование «ИТ в условиях кризиса». Снижение активности и сокращение ИТ-бюджетов, автор: Константин Зимин;
6) Зиндер Е. З. Архитектура предприятия в контексте бизнес-реинжиниринга. Часть 1 // Intelligent Enterprise, № 4/2008, с. 46.
7) www.fostas.ru/events/showdesc.php?id=79 – Зиндер Е. З. Архитектура предприятия на пространстве от политики и стратегии до тактики // Управленческий консультант. Киев: изд-во БУК, 2005. С. 44—71.
8) FEA Consolidated Reference Model Document. Version 2.3. October 2007.
9) www.opengroup.org/bookstore/catalog/i061.htm/ TOGAF — The Open Group Architecture Framework, Version 8.1.1 Enterprise Edition.
10) Аналитический банковский журнал 07 (158) июль 2008, «TCO, или Как управлять IT-затратами»;