УДК 003.26

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАТРАТ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Синяк А. А., Губенко Н. Е.
Донецкий национальный технический университет
кафедра компьютерных наук и технологий
E-mail: bisikleta@mail.ru

Аннотация

Синяк А. А., Губенко Н. Е. Анализ методов оценки эффективности затрат в информационную безопасность. *Рассмотрены наиболее распространенные методы оценки эффективности вложений в информационную безопасность. Определены их преимущества и недостатки, выделены лучшие методы*

Общая постановка проблемы

На сегодняшний день в условиях рынка компания сосредоточена на поддержании своей конкурентоспособности – продуктов и услуг, конкурентоспособности компании в целом. В таких условиях качество и эффективность информационной системы влияют на конечные финансовые показатели через качество бизнес-процессов. В проигрыше оказываются те компании, где финансирование защиты информации ведется по остаточному принципу.

К вложениям в информационную безопасность (ИБ) можно относиться как к затратам или как к инвестициям. Отношение к вложениям в ИБ как к затратам отдаляет компанию от решения стратегической задачи, связанной с повышением ее адаптивности к рынку. Если у компании есть долгосрочная стратегия развития, она рассматривает вложения в ИБ как инвестиции

Основной экономический эффект, к которому стремится компания, создавая систему защиты информации, - это существенное уменьшение материального ущерба вследствие реализации существующих угроз информационной безопасности [1]

Исследования

Выделим наиболее известные методы оценки эффективности затрат в ИБ:

ROI (Return On Investments - коэффициент возврата инвестиций). Данный коэффициент показывает, какую прибыль получит компания от вложения денег в различные мероприятия. Наиболее распространенный метод вычисления ROI – дерево принятия решений. Суть анализа заключается в следующем: потенциальный доход от инвестиций умножается на вероятность получения этого дохода. В результате получаем «цену решения». Сопоставив пары "сумма инвестиций - цена решения" можем найти оптимальный вариант, когда вложенные деньги принесут максимальный эффект.

Следует заметить, что руководители служб безопасности, использующие ROI для оценки будущих затрат столкнуться с проблемой подсчета дохода от внедрения системы. Использование метода дерева принятия решения дает приблизительный результат. Обычно параметр ROI используют для оценки маркетинговых мероприятий. ИБ имеет свои особенности, которые делают распространенные способы расчета ROI неэффективными

BCP (Business Continuity Management - планирование непрерывности бизнеса). Планирование непрерывности бизнеса – это комплекс мероприятий, направленных на снижение рисков прерывания бизнеса и их негативных последствий. Наиболее

вероятные потенциальные опасности – это компьютерные угрозы. Эти угрозы имеют критический характер (вирус, поразивший бухгалтерию, наносит больший ущерб, чем пожар на складе).

Оценка эффективности затрат основывается на статистических данных. При этом учитываются вероятность возникновения опасной ситуации и потери, которые понесет компания в этом случае. Использование принципов BCP доступно для крупных компаний, которые могут себе позволить значительные затраты, связанные с введением их в действие[3]

LE (Loss Expectancy - метод ожидаемых потерь). Подход основывается на том, что вычисляются потери от нарушений политики безопасности, с которыми может столкнуться компания, и эти потери сравниваются с инвестициями в безопасность, направленными на предотвращение нарушений. Метод основан на эмпирическом опыте организаций и сведений о вторжениях, о потерях от вирусов, об отражении сервисных нападений. Чтобы определить эффект от внедрения системы ИБ, нужно вычислить показатель ожидаемых потерь (Annualised Loss Expectancy – ALE).

$$AS = ALE * E - AC, \quad (1)$$

где:

- AS – ежегодные сбережения (Annual Saving),
- E – эффективность системы защиты (около 85%),
- AC – ежегодные затраты на безопасность (Annual Cost)

SAEM (Security Attribute Evaluation Method - метод оценки свойств системы безопасности). Метод был разработан в Carnegie Melon University, основан на сравнении архитектур систем ИБ для получения стоимостных результатов оценки выгод от внедрения системы ИБ. Объединив вероятность события и ранжировав воздействие окружающей среды, можно предложить проекты по ИБ с многовариантным влиянием окружающей среды на относительные затраты. Недостаток метода в том, что специалисты по ИБ редко имеют точные данные относительно выгод, приносимых технологией, поэтому они полагаются на опыт и интуицию

FTA (Fault Tree Analysis – анализ дерева ошибок). Этот метод оценки выгод является не очень известным инструментом на сегодняшний день. Цель применения этого метода состоит в том, чтобы показать, в чем заключаются причины нарушений политики безопасности и какие сглаживающие контрмеры могут быть применены. Дерево ошибок – это графическое средство, которое позволяет свести систему возможных нарушений к логическим отношениям «и» – «или» компонентов этой системы. Если доступны данные по нормам отказа критических компонентов системы, то дерево ошибок позволяет определить ожидаемую вероятность отказа всей системы. На сегодняшний день данный метод еще не в полной мере адаптирован к области информационной безопасности и требует дальнейшего внимательного и глубокого изучения [4]

TCO (Total Cost Of Ownership - совокупная стоимость владения). Методика была предложена аналитической компанией Gartner Group. В этой модели затраты делятся на две категории: прямые и косвенные. Косвенные затраты – это скрытые расходы, возникающие при эксплуатации системы защиты информации (СЗИ). Под прямыми затратами понимают капитальные затраты и трудовые затраты.

Методика TCO компании Gartner Group позволяет:

1. Получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной СЗИ;

2. Сравнить подразделения службы ИБ компании между собой и с аналогичными подразделениями других предприятий в данной отрасли;
3. Оптимизировать инвестиции на ИБ компании с учетом реального значения показателя TCO

TCO не только отражает “стоимость владения” отдельных элементов и связей корпоративной системы защиты информации в течение их жизненного цикла. “Овладение методикой” TCO помогает службе ИБ лучше измерять, управлять и снижать затраты и улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании

Подход к оценке TCO основывается на результатах аудита структуры и поведения корпоративной системы защиты информации и компьютерной информационной системы (КИС) в целом, включая действия сотрудников служб автоматизации, ИБ, пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения с аналогичными компаниями по отрасли. [2]

Одно из преимуществ этого показателя состоит в том, что он позволяет сделать выводы о целесообразности реализации проекта в области ИБ на основании оценки только затрат. Другим преимуществом является то, что модель расчета TCO предполагает оценку не только первоначальных затрат на создание СЗИ, но и затрат, которые могут возникнуть на различных этапах жизненного цикла системы [1]

Таблица 1 Сравнительная характеристика методов оценки эффективности затрат

	ROI	BCP	LE	SAEM	TCO
Высокая стоимость проведения	-	+	-	-	-
Приблизительный результат	+	-	-	-	-
Простота реализации метода	+	-	+	±	±
«Стат. показатель»	+	-	-	-	+

Вывод

Оценка затрат на построение системы ИБ на сегодняшний день – это очень важная задача, без решения которой невозможно построение надежных систем защиты коммерческой информации. На сегодняшний день существует множества методов оценки эффективности затрат в информационную безопасность, среди которых выделяют ROI, BCP, LE, SAEM, TCO. На основе анализа можно сделать вывод, что метод ожидаемых потерь (LE) и метод оценки свойств системы безопасности (SAEM) являются более предпочтительными

Список литературы

1. Ясенев В.Н. Информационная безопасность в экономических системах: Учебное пособие – Н. Новгород: Изд-во ННГУ, 2006

2. Оценка затрат компании на Информационную безопасность. Электронный ресурс. Режим доступа: http://citforum.ru/security/articles/ocenka_zatrat/

3. Оценка затрат компании на ИБ. Электронный ресурс. Режим доступа: http://www.getinfo.ru/article682.html

4. Материал из CA – ежемесяного журнала. Электронный ресурс. Режим доступа: http://samag.ru/blog/art/No_number/16