УДК 519.876.5

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ СИСТЕМ СРЕДСТВАМИ И МЕТОДАМИ ВИЗУАЛЬНОГО МОДЕЛИРОВАНИЯ

Селина Н.В., Губенко Н.В.
Донецкий национальный технический университет г.Донецк
Кафедра компьютерных систем мониторинга
E-mail: gubenko@cs.donntu.edu.ua

Аннотация

Селина Н.В., Губенко Н.В. Исследование эффективности защищенности корпоративных систем средствами и методами визуального моделирования. *В статье рассматривается вопрос, как спроектировать экономически эффективную систему безопасности, адекватную угрозам бизнеса.*

Общая постановка проблемы. Как известно, первым этапом процесса организации защиты корпоративной вычислительной сети является анализ ее защищенности. Решение данной задачи предполагает сбор большого объема информации о структуре, элементах и активах корпоративной вычислительной сети, которая является сложным техническим объектом с распределенной структурой, состоящей из правового, организационного, программного и аппаратного уровней, В настоящее время анализ защищенности проводится с постоянным участием сетевых администраторов, при этом используются их знания о структуре различных уровней корпоративной вычислительной сети, особенностях применяемых методов и средств анализа защищенности. Автоматизация анализа защищенности, актуальность которой возрастает с увеличением количества узлов и сложности конфигурации корпоративной вычислительной сети, затруднена по следующим причинам: необходима разработка модели представления знаний о корпоративной вычислительной сети, требуется формализация процедуры анализа защищенности, а также концепция построения системы анализа защищенности. [1]

Анализ состояния методов и подходов к решению рассматриваемой задачи показал, что на сегодняшний день существует несколько направлений ее исследования. Можно выделить работы Петренко С.А., Симонова СВ. по построению экономически обоснованных систем обеспечения информационной безопасности, Мельникова А.З., по проблемам анализа защищенности информационных систем, Котенко ИЗ. по разработке интеллектуальных методов анализа уязвимостей корпоративной вычислительной сети, Васильева ВЛ, Городецкого В.И., Макаревича О.Б,, Медведовского И.Д., Шелупаиова А.А. и др, по проектированию интеллектуальных систем защиты информации.

Постановка задач исследования. Основным экономическим эффектом, к которому стремится компания, создавая СЗИ, является существенное уменьшение материального ущерба вследствие реализации каких-либо существующих угроз информационной безопасности. При этом, руководствуясь статистическими данными различных аналитических служб, можно сделать вывод о том, что ущерб этот вполне реален и измеряется в денежных единицах.

Обеспечение информационной безопасности компании имеет вполне конкретный экономический смысл. А достижение этой цели должно осуществляться экономически оправданными мерами. Принимать решение о финансировании проектов по ИБ целесообразно лишь в том случае, когда есть уверенность, что не просто увеличивается расходная часть бюджета, а производится инвестиции в развитие компании. При этом отдача от таких инвестиций должна быть вполне прогнозируемой.

Именно поэтому в основе большинства методов оценки эффективности вложений в информационную безопасность лежит сопоставление затрат, требуемых на создание СЗИ, и ущерба, который может быть причинен компании из-за отсутствия этой системы [2].

Целью данной работы является повышение эффективности моделирования процессов защищенности корпоративных систем.

Решение задачи и результаты исследований. Для решения поставленной задачи был проведен анализ всех методов оценки целесообразности затрат на систему информационной безопасности. Выбор осуществлялся на основе следующих целей:

1. Метод должен обеспечивать количественную оценку затрат на безопасность, используя качественные показатели оценки вероятностей событий и их последствий;

2. Метод должен быть прозрачен с точки зрения пользователя, и давать возможность вводить собственные эмпирические данные;

3. Метод должен быть универсален, то есть одинаково применим к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, затрат на перемещение персонала и обучение конечных пользователей и т. д.

4. Выбранный метод должен позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия.

Рассмотрим существующие методы.

Прикладной информационный анализ Applied Information Economics (AIE)

Методика AIE (компания Hubbard Ross) позволяет повысить точность показателя «действительная экономическая стоимость вложений в технологии безопасности за счет определения доходности инвестиций» (Return on Investment, ROI) до и после инвестирования. Применение AIE позволяет сократить неопределенность затрат, рисков и выгод, в том числе и неочевидных.

Потребительский индекс Customer Index (CI)

Метод предлагает оценивать степень влияния инвестиций в технологии безопасности на численность и состав потребителей. В процессе оценки предприятие или организация определяет экономические показатели своих потребителей за счет отслеживания доходов, затрат и прибылей по каждому заказчику в отдельности. Недостаток метода состоит в трудности формализации процесса установления прямой связи между инвестициями в технологии безопасности и сохранением или увеличением числа потребителей. Этот метод применяется в основном для оценки эффективности корпоративных систем защиты информации в компаниях, у которых число заказчиков непосредственно влияет на все аспекты бизнеса.

Добавленная экономическая стоимость Economic Value Added (EVA)

Методика EVA (консалтинговая компания Stern Stewart и Co.) предлагает рассматривать службу информационной безопасности как «государство в государстве», то есть специалисты службы безопасности продают свои услуги внутри компании по расценкам, примерно эквивалентным расценкам на внешнем рынке, что позволяет компании отследить доходы и расходы, связанные с технологиями безопасности. Таким образом, служба безопасности превращается в центр прибыли и появляется возможность четко определить, как расходуются активы, связанные с технологиями безопасности, и увеличиваются доходы акционеров.

Исходная экономическая стоимость Economic Value Sourced (EVS)

Методика EVS (компания META Group Consulting) основывается на количественном измерении возврата от инвестиций в технологии безопасности. Методика предполагает точный расчет всех возможных рисков и выгод для бизнеса, связанных с внедрением и функционированием корпоративной системы защиты информации. При этом расширяется

использование таких инструментальных средств оценки ИТ, как добавленная экономическая стоимость (EVA), внутренняя норма рентабельности (IRR) и возврат от инвестиций (ROI) за счет определения и вовлечения в оценочный процесс параметров времени и риска.

Управление портфелем активов Portfolio Management (PM)

Методика управления портфелем активов предполагает, что компании управляют технологиями безопасности так же, как управляли бы акционерным инвестиционным фондом с учетом объема, размера, срока, прибыльности и риска каждой инвестиции. Портфель активов технологий безопасности состоит из «статических» (апаратно-программные средства защиты информации, операционные системы и пакеты прикладных программ-ных продуктов, сетевое оборудование и программное обеспечение, данные и информацию, оказываемые услуги, человеческие ресурсы и пр.) и «динамичных» активов (различные проекты по расширению и обновлению всего портфеля активов, знания и опыт, интеллектуальный капитал и т. д.).

Оценка действительных возможностей Real Option Valuation (ROV)

Основу методики составляет ключевая концепция построения модели «гибких возможностей компании» в будущем. Методика рассматривает технологии безопасности в качестве набора возможностей с большой степенью их детализации. Правильное решение принимается после тщательного анализа широкого спектра показателей и рассмотрения множества результатов или вариантов будущих сценариев, которые в терминах методики именуются «динамическим планом выпуска» управляющих решений или гибкости, который поможет организациям лучше адаптировать или изменять свой курс в области информационной безопасности.

Метод жизненного цикла искусственных систем System Life Cycle Analysis (SLCA)

В основе метода жизненного цикла искусственных систем System Life Cycle Analysis (SLCA), предложенного в российским бизнес-аналитиком Игорем Холкиным, лежит измерение «идеальности» корпоративной системы защиты информации – соотношение ее полезных факторов к сумме вредных факторов и факторов расплаты за выполнение полезных функций. Оценку предваряет совместная работа аналитика и ведущих специалистов обследуемой компании по выработке реестра полезных, негативных и затратных факторов бизнес-системы без использования системы безопасности и присвоению им определенных весовых коэффициентов. Результатом работы является расчетная модель, описывающая состояние без системы безопасности. После этого в модель вводятся описанные факторы ожидаемых изменений и производится расчет уровня развития компании с корпоративной системой защиты информации. Таким образом, строятся традиционные модели «Как есть» и «Как будет» с учетом реестра полезных, негативных и затратных факторов бизнес-системы.

Совокупная стоимость владения Total Cost of Ownership (TCO)

TCO первоначально разрабатывалась как средство расчета стоимости владения компьютером. Но в последнее время благодаря усилиям компании Gartner Group эта методика стала основным инструментом подсчета совокупной стоимости владения корпоративных систем защиты информации. Основной целью расчета ССВ является выявление избыточных статей расхода и оценка возможности возврата инвестиций, вложенных в технологии безопасности. Таким образом, полученные данные по совокупной стоимости владения используются для выявления расходной части использования корпоративной системы защиты информации.

Анализ методов оценки эффективности инвестиций в корпоративные системы информационной безопасности показывает, что только метод совокупной стоимости владения (TCO) в явном виде позволяет рассчитать расходную часть на систему безопасности. Также метод TCO позволяет произвести наиболее адекватную экономическую оценку проекта. Основываясь на этом показателе, заказчик может выбрать исполнителя,

минимизируя стоимость реализации и сопровождения системы либо находя «золотую середину» между затратами и качеством На сегодняшний день аудит информационных систем по стандартам Gartner Group является одним из наиболее широко применяемых приемов, использующихся для выработки рекомендаций по оптимизации затрат на ИТ.

Даже однократная оценка совокупной стоимости владения ИТ-инфраструктурой может повысить эффективность управления затратами, тем самым увеличивая эффективность использования ИТ на предприятии. Если учет затрат на ИТ-инфраструктуру по методике ТСО будет проводиться на регулярной основе – это даст возможность не только оптимизировать затраты на содержание и развитие информационных систем, но и привести план развития ИТ-инфраструктуры в соответствие основным бизнес-целям фирмы.

Существует два наиболее наглядных варианта оценки проекта. Первый – сравнение ТСО уже реализованных аналогичных решений. Второй основан на сравнении ТСО решений, предлагаемых разными исполнителями или созданными на базе разных продуктов. Выбор конкретного способа оценки всегда остается за ИТ-руководителем или менеджером проекта. В обоих случаях следует по возможности сравнивать те решения, что развернуты на предприятиях той же отрасли, в которой работает заказчик проекта.

Первый способ позволяет доказать руководству компании, что предлагаемое решение имеет экономические показатели не хуже (или лучше), чем в среднем по отрасли. Этот подход требует довольно большого объема статистического материала, сбор которого является достаточно трудоемкой задачей.

Второй способ сравнения не требует такого объема необходимых статистических материалов, как в предыдущем случае, кроме того, данные могут быть получены из открытых источников, что позволяет применять этот способ практически всегда. Анализ результатов расчета может использоваться в качестве аргументации выбора исполнителя или варианта реализации информационной системы.

Приведем пример расчета ТСО. Клиент приступил к выбору исполнителя и остановил пока свой выбор на двух компаниях, специализирующихся в области информационной безопасности. Их известность на рынке примерно одинакова. Программные продукты, предлагаемые исполнителями, аналогичны и сертифицированы. В качестве источников информации используются прейскуранты или предложения исполнителей. Предполагается, что проект должен будет функционировать в течение 10 лет без дополнительной модернизации.

На начальном этапе оценки проекта ТСО для реализации с привлечением выбранного исполнителя будет оцениваться с использованием лишь прямых, обязательных расходов.

В принципе, возможны четыре результата анализа ТСО в разрезе единовременных и ежегодных расходов:

1) Ед1 > Ед2, Еж1 > Еж2, выбор клиента – исполнитель 2;

2) Ед1 < Ед2, Еж1 < Еж2, выбор клиента – исполнитель 1;

3) Ед1> Ед2, Еж1 > Еж2, выбор клиента требует уточнения;

4) Ед1< Ед2, Еж1 < Еж2, выбор клиента требует уточнения.

где Едn – единовременные расходы, которые понесет клиент при привлечении исполнителя n;

Ежn – ежегодные расходы, которые понесет клиент при привлечении исполнителя n.

Очевидно, что два первых варианта расчета ТСО однозначны и дополнительных уточнений для выбора исполнителя не требуется.

Рассмотрим более подробно третий и четвертый варианты. Поскольку варианты симметричны относительно исполнителей, рассмотрим один из них, а именно третий.

Результаты проведенного расчета (или представленного исполнителем или исполнителем) приведены на рисунке 1.

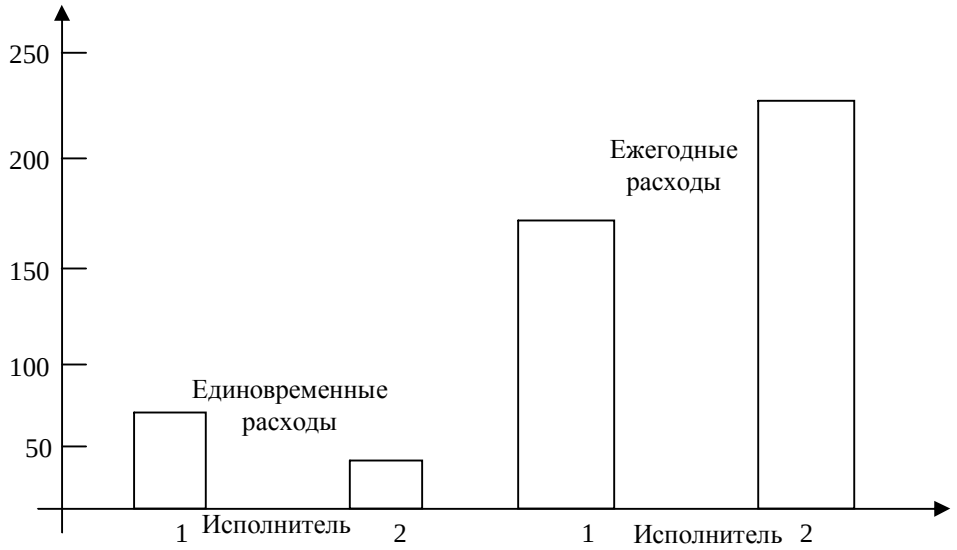

Рисунок 1 – Результаты проведенного расчета

Как видно, единовременные расходы на реализацию проекта с использованием продуктов исполнителя 1 превысят единовременные расходы на реализацию проекта с использованием продуктов исполнителя 2 (в первую очередь, за счет более высокой стоимости программного обеспечения). Однако применительно ко всему сроку функционирования проекта ТСО проекта с привлечением исполнителя 1 окажется ниже, чем ТСО проекта с привлечением исполнителя 2 за тот же период. Это обусловлено значительным превышением ежегодных расходов, в первую очередь за счет высокой стоимости сопровождения программного обеспечения исполнителем 2.

Данная ситуация требует дополнительного определения коэффициента сравнивания затрат. В приведенном примере он составит около двух лет, т.е. к концу второго года функционирования проекта клиент понесет одинаковые затраты, какого бы из исполнителей он ни выбрал. Но, как говорилось выше, предполагаемая продолжительность функционирования проекта – 10 лет. Следовательно, в течение восьми лет клиент будет нести большие расходы, если привлечет к реализации проекта исполнителя 2. Естественно, клиенту это не выгодно, и его выбор должен пасть на исполнителя 1.

Также из представленной ситуации и анализа результата видно, что если бы клиент сравнивал лишь прейскуранты без расчета ТСО в долгосрочной перспективе, то цены производителя 2 казались бы ему значительно привлекательней, чем цены исполнителя 1.

Выводы. В качестве инструмента для моделирования исследуемых процессов была выбрана система Arena фирмы System Modeling Corporation. Arena позволяет строить имитационные модели, проигрывать их и анализировать результаты такого проигрывания.

В целом система исключительно проста в использовании. В системе Arena удачно соединены интерфейсные возможности среды Windows и присущая Arena легкость иерархического построения модели и ее последовательного приближения к реальному объекту.

Список литературы

1. http://www.lib.ua-ru.net/diss/cont/169843.html

2. «Оценка затрат на защиту информации» С. А. Петренко, д. т. н., Е. М. Терехова Информационно-методический журнал «Inside. Защита информации», №1 январь-февраль 2005 год, http://www.inside-zi.ru/pages/1_2005/36.html