УДК 004.056:005 + 004.056:330.133

МЕТОДИКИ ОЦЕНКИ СТОИМОСТИ ВЛАДЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

А.Н. Шиховцев, Л.В. Астахова

В данной статье описаны методики оценки стоимости владения СУИБ и выявлены их достоинства и недостатки.

Ключевые слова: управление информационной безопасностью, оценка, стоимость, методика.

В настоящее время проблема оценки стоимости владения системой управления информационной безопасностью (СУИБ) становится более актуальной по причине того, что автоматизированные системы стали важным элементом эффективного выполнения бизнес-процессов предприятий. Согласно статистике, с каждым годом все больше компаний подвергаются кибератакам с общим ущербом более триллиона долларов, что и заставляет руководство компаний задумываться о создании СУИБ.

Анализ литературы показал, что конкретная методика оценки стоимости СУИБ нормативно не закреплена. На практике свое применение в этом вопросе нашли методики оценки затрат на ИТ-системы. В данной работе будут рассмотрены различные методики оценки затрат, а также их пригодность использования в сфере информационной безопасности (ИБ).

Директор любой компании, прежде всего, задается вопросом о стоимости создания СУИБ, а также о цене ее обслуживания. Как уже было сказано, на сегодняшний день нет конкретной методики, которая позволила бы провести эффективную оценку затрат именно в сфере ИБ. Однако в этом случае можно обратиться к методикам оценки затрат на ИТ-системы. Стоить отметить, что на данный момент их существует большое множество, но не каждую можно использовать при оценке СУИБ. После изучения литературы и других источников мы можем обратиться к классификации, которую описал в своей статье С.В. Разумников [1]. Он выделил три основные группы методик: финансовые, качественные и вероятностные. К финансовым относятся следующие методики: совокупная стоимость владения (Total Cost of Ownership, TCO) и экономическая добавленная стоимость (Economic Value Added, EVA). К качественным: система сбалансированных показателей (Balanced Scorecard, BSC), совокупный экономический эффект (Total Economic Impact, TEI), быстрое экономическое обоснование (Rapid Economic Justification, REJ), информационная экономика (Information Economics, IE). Вероятностные методики: справедливая цена опционов (Real Options Valuation, ROV) и прикладная информационная экономика (Applied Information Economics, AIE).

Рассмотрим группу *финансовых методик*.

Совокупная стоимость владения (Total Cost of Ownership, TCO) – методика, созданная компанией Gartner Group в конце 80-х годов. Первоначально разработанная для оценки затрат на ИТ-системы, данная методика, претерпев некоторые изменения, нашла свое применение и сфере ИБ. Совокупная стоимость владения для СУИБ складывается из следующих показателей: аудит ИБ на предприятии, стоимость проектных работ, стоимость закупки и настройки программно-технических средств защиты, затраты на обеспечение физической безопасности, обучение персонала, а также управления, поддержки и модернизации СУИБ [2]. Согласно [3], все затраты можно разделить на две категории – прямые и косвенные. Под косвенными затратами подразумевают скрытые расходы, которые возникают в процессе эксплуатации СУИБ. Прямые затраты – это непосредственно основные расходы на создание системы, которые составляют обычно около 25 % от всех расходов [3]. Расчет затрат по данной методике производится по следующей формуле:

$$TCO = TCOp + TCA,$$

где *TCO* – совокупная стоимость владения, *TCOp* – стоимость использования системы, *TCA* – прямые затраты на систему.

Стоит отметить, что параметр TCOp включает в себя расходы на так называемые человеческие ресурсы – начиная с затрат на обучение персонала и заканчивая заработной платой. Очень часто этот нюанс упускается из расчета стоимости СУИБ, несмотря на его важность. Ведь не смотря на введенную СУИБ, более 70 % утечек и утрат защищаемой информации в организациях происходит именно по вине персонала. Л.В. Астахова описывает несколько методик. Например, метод анализа влияния человеческого фактора – Human Reliability Assessment (HRA), который может быть использован не только в качественном, но и в количественном виде. Благодаря этой методике, есть возможность идентифицировать ошибки работников при работе с СУИБ, учитывая которые система будет показывать лучший результат. Кроме того, автор рассматривает вопрос рисков, связанных с культурным капиталом, обосновывает авторскую методику оценки культурного капитала – Assessment of cultural capital (ACC) организации [4], которая также может быть использована как методика количественной оценки стоимости владения УИБ. Полагаем, что ACC или HRA и другие методики оценки человеческого или культурного капитала организации в совокупности с TCO дадут более полную картину об оценке стоимости владения СУИБ.

Экономическая добавленная стоимость (Economic Value Added, EVA). Методика предложена компанией Stern Stewart & Co. Ее суть достаточно проста – вычисляется разница между чистой операционной прибы-

лью предприятия и всеми затратами, понесенными предприятием на создание ИТ-системы. В статье А.А. Гусева [5] используется следующая формула расчета:

$$EVA = NOPAT - K * CC,$$

где *EVA* – экономическая добавленная стоимость, *NOPAT* – прибыль от операционной деятельности компании, *K* – капитал, вложенный в активы, которые служат для обеспечения оперативной деятельности компании, *CC* – средневзвешенная стоимость капитала. Из всего этого следует факт, что данная методика не может использоваться в ИБ, так как экономическая добавленная стоимость связана с доходом компании от введения системы в работу. В нашем случае СУИБ, как на коммерческом, так и на государственном предприятии не принесет дохода, а лишь обезопасит выполнение бизнес-процессов и информационные потоки.

Качественные методики оценки затрат

Система сбалансированных показателей (Balanced Scorecard, BSC) – методика, разработанная профессорами Гарвардского университета Робертом Капланом и Дэвидом Нортоном. Данная методика пользуется большим спросом среди компаний, как малыми, так и промышленными, и государственными. Основной упор системы сбалансированных показателей делается на формализацию целей ИТ-системы в привязке к бизнес-процессам компании, а также на планы стратегического развития. Успешную попытку использования этой методики в сфере ИБ можно увидеть в работе А.В. Лукацкого [6]. В своей статье он описывает возможные пути использования данной методики при создании СУИБ на предприятии. Он говорит о том, что данную методику лучше применять тогда, когда она уже используется на предприятии относительно других проектов. Однако стоит помнить, что методика BSC, в первую очередь, направлена на управление активами и ресурсами [7], а не на оценку финансирования СУИБ.

Совокупный экономический эффект (Total Economic Impact, TEI). Это методика, разработанная компанией Forrester Research, позволяющая оценить проект внедрения какого-либо компонента информационной системы на предприятии. Главной отличительной чертой является применение трех показателей: стоимости, гибкости и преимущества. Показатель стоимости рассчитывается путем использования методики совокупной стоимости владения (TCO). Показатель гибкости указывает на сложность процессов внедрения какого-либо компонента информационной системы (начиная с затрат на введение и заканчивая адаптацией персонала). А показатель преимущества отражает возможности, которые могут появиться при введении системы в действие. После расчета показателей идет анализ рисков, которые могут возникнуть в ходе внедрения и функционирования системы. Однако данная методика имеет узкий спектр применения, поэтому используется чаще для введения отдельных компонентов системы. Если

рассматривать СУИБ, то речь идет о таких компонентах, как выбор защитного средства для рабочих мест или определенной криптосистемы.

Быстрое экономическое обоснование (Rapid Economic Justification, REJ). Эта методика, которая была разработана компанией Microsoft, основывается на методике TCO. Быстрое экономическое обоснование конкретизируется на установлении соответствий между расходами на ИТ-системы и приоритетами компании, ее бизнес-процессами. REJ разрабатывалась как методика, с помощью которой ИТ-специалисты могут проанализировать экономическую выгоду инвестиций в ИТ-систему. Стоит отметить, что, несмотря на заявленную простоту методики, она является сложной и затратной ввиду большого объема данных, которые необходимо собрать для анализа. REJ направлена на установление подсчета затрат введения ИТ-системы, а также определение получаемой выгоды от ее создания. Однако последнее не является приоритетом для оценки СУИБ, так как целью создания такой системы является не достижение выгоды компанией, а защита ее сведений и безопасность информационного оборота на предприятии.

Информационная экономика (Information Economics, IE). Методика, которую описал в 1976 году Марк Порат, является качественным методом оценки затрат на ИТ-проект. В его основе лежит принцип формирования списка критериев оценки эффективности проекта, а также анализ потенциальных выгод от введения ИТ-системы. Методика подразумевает выбор нескольких факторов, которые определяют эффективность данного проекта и рассматриваются со стороны значимости каждого из них для бизнес-процессов, а также рассмотрение рисков, связанных с вводом системы в строй. Применение этой методики в сфере ИБ неоднозначно потому, что методика позволяет рассмотреть положительные и отрицательные стороны введения СУИБ или же отдельных компонентов, однако другие аспекты – такие, как вычисление прибыли от введения СУИБ, – не рассматриваются.

Вероятностные методики

Справедливая цена опционов (Real Options Valuation, ROV). Данная методика была разработана в 1997 году Робертом Мертоном, Майроном Шоулзом и Фишером Блэком. Стоит сразу отметить, что эта методика не предназначена именно для ИТ-систем и ее использование крайне трудоемкий процесс. ROV рассматривает СУИБ с точки зрения ее управляемости в процессе создания. Выделяются несколько параметров, такие как выручка от создания системы, сложность, расходы на ее создание и функционирование и т.д. Следующим этапом является оценка управляемости данными параметрами – чем больше вероятность управления ими, т.е. понижение расходов и сложности создания проекта, тем выше будет оценка самого проекта. В целом методику можно использовать, как в ИТ-сфере, так и

в сфере ИБ, однако стоит учесть, что ее практически не используют в данных сферах. Ее применение вызовет сложности, поскольку сам метод очень затратный в плане ресурсов и времени [8].

Прикладная информационная экономика (Applied Information Economics, AIE). В основе данного метода лежит методика информационной экономики. Суть его проста – к каждой цели проекта создания СУИБ определяется вероятность ее достижения, а также вероятность улучшения функционирования бизнес-процессов компании от нововведений [8]. Чем выше полученные результаты, тем создание информационной системы будет выгоднее. Но стоит отметить, что данный метод не является методикой как таковой, и его можно применить только на ранних этапах создания системы. Однако есть другие методики, которые смогут более полно ответить на вопрос о затратах на создание и функционирование СУИБ.

Таким образом, в данной работе было рассмотрено несколько методик оценки затрат на ИТ-системы с учетом их применения для оценки стоимости СУИБ. Анализ показал, что не все методики могут быть применимы в сфере ИБ. В плане оценки стоимости лучше всего подходит методика совокупной стоимости владения (TCO), которая поможет рассчитать все затраты, связанные с внедрением СУИБ, включая стоимость управления человеческим и культурным капиталом организации в процессе управления ее ИБ. К тому же эта методика уже не один год используется в сфере ИБ, что облегчит ее использование на практике. При оценке стоимости СУИБ также возможно использование методики системы сбалансированных показателей (BSC). На практике она используется гораздо реже методики TCO, однако при грамотном подходе к ней, ее привязка к ИБ может оказаться весьма полезным инструментом в руках специалистов.

Важно также помнить, что любая методика – это набор математических формул и логических выражений. Поэтому решение о создании и инвестировании СУИБ на предприятии зависит, в первую очередь, от качества исходных данных, на основе которых будут применяться методики и приниматься соответствующие решения [3].

Библиографический список

1. Разумников, С.В. Анализ существующих методов оценки эффективности информационных технологий для облачных ИТ-сервисов / С.В. Разумников. // Современные проблемы науки и образования. – 2013. – № 3.

2. Ажмухамедов, И.М. Оценка экономической эффективности мер по обеспечению информационной безопасности / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика». – 2011. – № 1.

3. Милославская, Н.Г. Проверка деятельности по управлению информационной безопасностью / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой // Вопросы управления информационной безопасностью. Вып. 5. – М.: Горячая линия-Телеком, 2012. – С. 89–92.

4. Астахова, Л.В. Информационная безопасность: риски, связанные с культурным капиталом персонала / А.В. Астахова // Научно-техническая информация. Серия 1: «Организация и методика информационной работы». – 2015. – № 4.

5. Гусев, А.А. Концепция EVA и оценка деятельности компании / А.А. Гусев // Финансовый менеджмент. – 2005. – № 1.

6. Лукацкий, А.В. BSC и информационная безопасность / А.В. Лукацкий // Директор информационной службы. – 2009. – № 1.

7. Kádárová J. Balanced Scorecard as an Issue Taught in the Field of Industrial Engineering / J. Kádárová, M. Durkáčová, L. Kalafusová // Procedia – Social and Behavioral Sciences. – 2014. – Vol. 143. – Pp. 174–179.

8. Галкин, Г. Методы определения экономического эффекта от ИТ-проекта. Ч. 2. Качественные и вероятностные методы / Г. Галкин // Intelligent Enterprise. – 2005. – № 24 (133).

К содержанию