УДК 681.3

В.А. Артамонов, Е.В. Артамонова

МЕТОДИЧЕСКИЕ АСПЕКТЫ ВЫБОРА ЗАТРАТ НА ОРГАНИЗАЦИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

ЧАСТЬ 1: МЕТОДИКА ОЦЕНКИ СОВОКУПНОЙ СТОИМОСТИ ВЛАДЕНИЙ

Многие руководители служб автоматизации ***(CIO)*** и служб информационной безопасности ***(CISO)*** наверняка задавались вопросами: Как оценить эффективность планируемой или существующей корпоративной системы защиты информации? Как оценить эффективность инвестиционного бюджета на информационную безопасность (ИБ) компании? В какие сроки окупятся затраты компании на ИБ? Как экономически эффективно планировать бюджет компании на ИБ и управлять им? Попробуем найти возможные ответы на эти вопросы.

Определение эффективности организации режима ИБ в компании предполагает некоторую оценку затрат на ИБ, а также достигаемого при этом эффекта. Действительно, сравнение этих оценок позволяет получить представление о том, как возвращаются инвестиции на ИБ, а также экономически корректно планировать бюджет предприятия на ИБ и управлять им.

На практике многие решения в области защиты информации часто принимаются на интуитивно-понятийном уровне, без каких-либо экономических расчетов и обоснований. В результате только те начальники служб ИБ, сумевшие заявить и отстоять потребность в защите информации, смогли как-то повлиять на планирование выделения бюджетных средств компании на ИБ. Однако современные требования бизнеса, предъявляемые к организации режима ИБ компании, настоятельно рекомендуют обращаться к более обоснованным технико-экономическим методам и средствам, позволяющим количественно измерять уровень защищенности компании, а также определять экономическую эффективность затрат на ИБ.

Сегодня оценивать эффективности корпоративной системы защиты информации рекомендуется с помощью некоторых критериев эффективности, например показателей *совокупной стоимости владения* ***(TCO)****, экономической эффективности бизнеса, коэффициентов возврата инвестиций на ИБ* ***(ROI)*** и др. [1].

В частности, известная методика совокупной стоимости владения была изначально предложена аналитической компанией Gartner Group для оценки затрат на информационные технологии [2].

В контексте информационной безопасности методика ***TCO*** может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она

позволяет руководителям служб информационной безопасности обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы ИБ. Кроме того, поскольку оценка экономической эффективности корпоративной системы защиты информации становится «измеримой», появляется возможность оперативно решать задачи контроля и коррекции показателей экономической эффективности, в частности показателя ***TCO***. Таким образом, этот показатель может послужить инструментом оптимизации расходов на обеспечение требуемого уровня защищенности КИС и обоснование бюджета на ИБ. При этом компании такие работы могут выполнять самостоятельно с привлечением системных интеграторов в области защиты информации или совместно с интегратором.

Отметим, что показатель ***TCO*** применим практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и помогает «навести порядок» в существующих и планируемых затратах на ИБ. С такой точки зрения данный показатель позволяет объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. При этом для объективности решения необходимо дополнительно учитывать состояние внешней и внутренней среды предприятия, например показатели технологического, управленческого, кадрового и финансового развития предприятия, поскольку не всегда наименьший показатель ***TCO*** корпоративной системы защиты информации оказывается оптимальным для предприятия.

Понятно, что при умелом управлении ***TCO*** удается рационально и экономно реализовывать средства бюджета на ИБ, достигая при этом приемлемого уровня защищенности компании, адекватного текущим целям и задачам бизнеса. Существенно, что сравнение определенного показателя ***TCO*** с аналогичными показателями ***TCO*** по отрасли (аналогичными компаниями) и с «лучшими в группе» позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто трудно или практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же «родственных» показателей ***TCO*** дает возможность убедиться, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения удобно проводить, пользуясь усредненными показателями ***TCO*** по отрасли, рассчитанными экспертами Gartner Group или собственными экспертами компании с помощью методов математической статистики и обработки наблюдений.

Таким образом, методика ***TCO*** Gartner Group позволяет ответить на следующие актуальные вопросы:

- какие ресурсы и денежные средства тратятся на ИБ;
- оптимальны ли затраты на ИБ для бизнеса компании;
- насколько эффективна работа службы ИБ компании по сравнению с другими компаниями;
- как сделать управление инвестированием в защиту информации эффективным;
- какие выбрать направления развития корпоративной системы защиты информации;
- как обосновать бюджет компании на ИБ;
- как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом;
- какова оптимальная структура службы ИБ компании;
- как правильно оценить сторонние услуги по сопровождению корпоративной системы защиты информации;
- как определить эффективность нового проекта в области защиты информации.

Сумма всех затрат на повышение уровня защищенности предприятия от угроз ИБ составляет общие затраты на безопасность.

Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия может быть представлена так, как это изображено на рис. 1.

Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма - общие затраты на безопасность. Мы не включаем в данном случае единовременные затраты на формирование политики ИБ предприятия, так как на любом действующем предприятии такая политика уже выработана.

Снижение общих затрат

Из примера, представленного на рис.1, видно, что достигаемый уровень защищенности измеряется в категориях «большой риск» и «риск отсутствует» (совершенная защита). Рассматривая левую сторону графика (большой риск), мы видим, что общие затраты на безопасность высоки в основном потому, что велики потери на компенсацию при нарушениях политики безопасности. Расходы же на обслуживание системы безопасности очень малы.

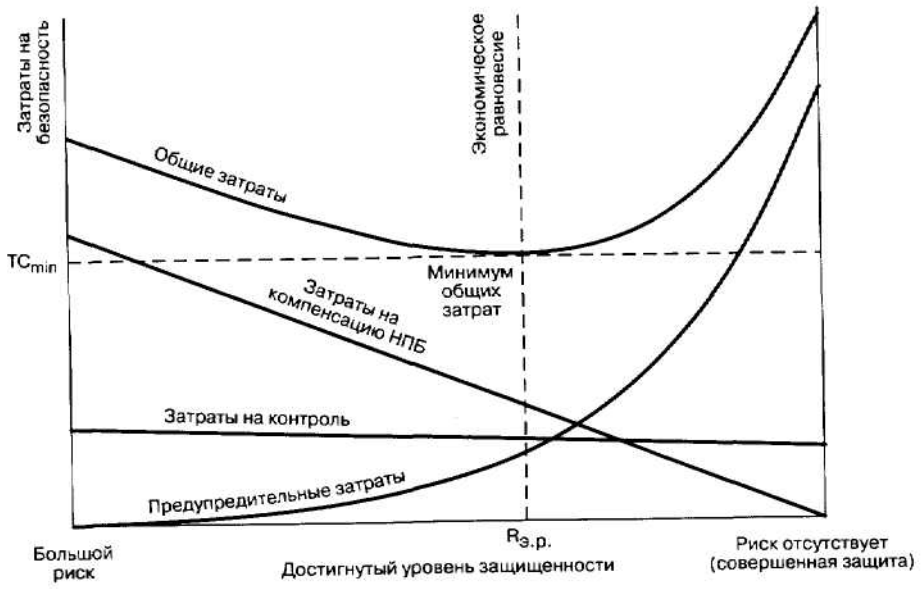

РИС.1 ВЗАИМОСВЯЗЬ МЕЖДУ ЗАТРАТАМИ НА БЕЗОПАСНОСТЬ И ДОСТИГАЕМЫМ УРОВНЕМ ЗАЩИЩЁННОСТИ

При движении по графику вправо достигаемый уровень защищенности возрастает (снижается информационный риск). Это происходит за счет увеличения объема предупредительных мероприятий, связанных с обслуживанием системы защиты. Расходы на компенсацию нарушений политики безопасности (НПБ) уменьшаются в результате предупредительных действий. Как показано на графике, на этой стадии расходы из-за потерь падают быстрее, нежели растут затраты на предупредительные мероприятия. В результате общие затраты на безопасность становятся меньше. Изменения объема затрат на контроль незначительны.

Увеличение общих затрат

Если двигаться по графику вправо, за точку экономического равновесия (то есть в область, где достигаемый уровень защищенности повышается), ситуация начинает меняться. Мы видим, что стремление добиться устойчивого снижения затрат на компенсацию нарушений политики безопасности приводит к более быстрому возрастанию затрат на предупредительные мероприятия. Получается, что ценой расходования значительного объема средств удается достичь сравнительно малого снижения уровня риска.

Экономическое равновесие

График на рис. 1 отражает только общий случай, так как построен с учетом некоторых допущений, не всегда отвечающих реальным ситуациям.

Первое допущение заключается в том, что предупредительная деятельность по техническому обслуживанию комплекса программно-технических средств защиты информации и предупреждению нарушений политики безопасности предприятия соответствует правилу Парето: в первую очередь рассматриваются те проблемы, решение которых дает наибольший эффект в части снижения информационного риска. Если не следовать этой модели, то вид графика станет совсем иным.

В соответствии со *вторым допущением* предполагается, что так называемое экономическое равновесие не изменяется во времени. В реальности все обстоит несколько иначе, поскольку на графике не учитываются два важных фактора:

- во-первых, предупредительная (превентивная) деятельность на практике - не просто порча бумаги, она позволяет не повторять допущенные ранее ошибки; но такая деятельность требует больших затрат, и экономический баланс может сдвигаться вправо по диаграмме;
- во-вторых, разработчики средств защиты не успевают за активностью злоумышленников, изыскивающих все новые и новые бреши в системах защиты. Кроме того, информатизация предприятия может породить новые проблемы, решение которых потребует дополнительных предупредительных затрат. Все это в состоянии сместить экономическое равновесие по направлению к левому краю диаграммы.

Опасность ошибочной интерпретации

Многие руководители служб безопасности (СБ) предприятий уверены в том, что они работают на уровне защищенности, отвечающем экономическому равновесию. Однако, как показывает практика, очень часто они не имеют веских доказательств для подтверждения этого предположения.

Рассматриваемый график - идеализированный, на нем уровень защищенности информационной среды предприятия от угроз безопасности представлен в терминах «высокий» и «низкий» и не соотносится с процентом возможного ущерба.

Руководитель службы безопасности, который не сомневается, что у него обеспечен базовый уровень защищенности, склонен считать, что это и есть экономическое равновесие, тогда как руководитель СБ, полагающий, что он поддерживает максимальный уровень защищенности, верит, что экономическое равновесие находится именно на этом уровне.

Приведенный график может внушить таким руководителям СБ уверенность в том, что повышение защищенности информационной среды на их предприятиях будет сопровождаться лишь увеличением затрат. В

результате никакой дополнительной предупредительной деятельности вестись не будет.

Нет совершенства

Если предупредительные мероприятия проводятся должным образом и являются эффективными, то достаточно трудно доказать, что на каком-либо предприятии общие затраты на безопасность выросли из-за увеличения расходов на эти нужды.

С другой стороны, если мы имеем дело с режимным объектом, обладающим очень низким уровнем риска, то есть теоретически возможны ситуации, при которых событие наступает, но случается это редко, а потенциальный ущерб сравнительно невелик, то на таком объекте общие затраты на безопасность незначительны.

Оба факта, взятые вместе, могут привести к заключению, что концепция экономического равновесия не подтверждается. Однако многие руководители предприятий уверены в правомочности этой концепции, но рассматривают ее как основание для того, чтобы не повышать уровень защищенности информационной среды.

Доля затрат на ИБ в обороте компании

Там, где затраты на безопасность должным образом учтены, они могут составлять до 20% и более от объема продаж (оборота). Эта оценкаполучена на основе анализа состояния защищенности информационной среды предприятий металлургической отрасли и связи [1].Типичное разделение затрат на информационную безопасность представлено в табл. 1

Таблица1. Распределение затрат на ИБ

Виды затрат	Расходы на безопасность
Затраты на потери (внешние и внутренние)	= 70% от общих затрат на безопасность
Затраты на контроль	= 25% от общих затрат на безопасность
Затраты на предупредительные мероприятия	= 5% от общих затрат на безопасность

Допустим, указанные затраты на безопасность составляют10% оборота. Далее предположим, что за счет увеличения объема предупредительных мероприятий и, следовательно, возрастания предупредительных затрат удалось снизить общие расходы на безопасность до 6% от оборота. Теперь распределение общих затрат на безопасность может быть таким, как описано в табл.2.

Таблица2. Распределение общих затрат на ИБ

Виды затрат	Расходы на безопасность
Затраты на потери (внешние и внутренние)	= 50% от новой величины общих затрат на безопасность

Затраты на контроль	=	25% от новой величины общих затрат на безопасность
Затраты на предупредительные мероприятия	=	25% от новой величины общих затрат на безопасность

Однако общие затраты на безопасность составили только 60% от их первоначальной величины.

Как новое их распределение выглядит по отношению к первоначальным общим затратам на безопасность, показано в табл.3.

Таблица3. Распределение затрат на ИБ

Виды затрат		Расходы на безопасность
Затраты на потери (внешние и внутренние)	$\frac{50\times60}{100}=$	30% от начальной величины общих затрат на безопасность
Затраты на контроль	$\frac{25\times60}{100}=$	25% от начальной величины общих затрат но безопасность
Затраты на предупредительные мероприятия	$\frac{25\times60}{100}=$	25% от начальной величины общих затрат на безопасность
Экономия	=	40% от начальной величины общих затрат на безопасность

Важным следствием рассуждений является вывод о том, что экономия расходов на безопасность невозможна без совершенствования системы защиты информации предприятия.

При оценке затрат на систему безопасности любого предприятия необходимо учитывать соотношение общих затрат на безопасность и общего объема продаж.

В целом методика ***TCO*** компании Gartner Group дает возможность:

- получить реалистичную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;
- сравнить подразделения службы ИБ компании как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;
- оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ***TCO***.

Литература

1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.: ил. - (Информационные технологии для инженеров).

2. www. Gartner.com /Gartner Security and Risk Management Summit 2012/.

МНОО «МАИТ», г. Минск