ОЦЕНКА ЗАТРАТ КОРПОРАТИВНЫХ СИСТЕМ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Галушка Е.В., Чигринская В. С., Губенко Н.Е.
Донецкий национальный технический университет

Большинство руководителей служб автоматизации (CIO) и служб информационной безопасности (CISO) отечественных компаний часто задаются вопросами: «Как оценить эффективность планируемой или существующей корпоративной системы защиты информации? Как оценить эффективность инвестиционного бюджета на информационную безопасность (ИБ) компании? В какие сроки окупаются затраты компании на ИБ? Как экономически эффективно планировать и управлять бюджетом компании на ИБ?». Данный доклад посвящен рассмотрению этой проблеме. Оценка эффективности организации режима ИБ в компании предполагает оценку затрат на ИБ, а также оценку достигаемого при этом эффекта. Сопоставление этих оценок позволяет, оценит возврат инвестиций на ИБ, а также экономически корректно планировать и управлять бюджетом компании на ИБ.

На практике многие компании работают на уровне фольклора, поэтому решение в области защиты информации часто принимаются на интуитивно-понятийном уровне, без каких-либо экономических расчетов и обоснований. В результате только те начальники служб ИБ (CISO), которые за счет своей „энергетики" смогли заявить и отстоять потребности в защите информации могли как-то повлиять на планирование бюджета компании на ИБ. Однако современные требования бизнеса, предъявляемые к организации режима ИБ компании, диктуют настоятельную необходимость использовать в своей работе более обоснованные технико-экономические методы и средства, позволяющие количественно измерять уровень защищенности компании, а также оценивать экономическую эффективность затрат на ИБ.

Как показано в ряде работ [1], сегодня для оценки эффективности корпоративной системы защиты информации рекомендуется использовать показатели эффективности, например показатели: совокупной стоимости владения(TCO), экономической эффективности бизнеса и непрерывности бизнеса (BCP), коэффициенты возврата инвестиций на ИБ (ROI) и другие.

В частности, известная методика совокупной стоимости владения (TCO) была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987) для оценки затрат на информационные технологии. методика Gartner Group позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Сегодня методика TCO может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности (CISO) обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников служб ИБ. Показатель TCO может применяться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и позволяет «навести порядок» в существующих и планируемых затратах на ИБ. С этой точки зрения показатель TCO 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 и состояние внешней и внутренней среды предприятия, например показатель технологического, кадрового и финансового развития предприятия. Умелое управление TCO позволяет рационально и экономно реализовывать средства бюджета на ИБ, достигая при этом приемлемого уровня защищенности компании, адекватного текущим целям и задачам бизнеса. В целом методика TCO компании Gartner Group позволяет:

- получить адекватную 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;

- оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ТСО.

Под показателем ТСО понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течении года. ТСО может рассматриваться как ключевой количественный показатель эффективности организации ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

Известно, что в методике ТСО в качестве базы для сравнения используются данные и показатели ТСО для западных компаний. Однако данная методика способна учитывать специфику украинских компаний с помощью так называемых поправочных коэффициентов. В качестве примера использования методики ТСО для обоснования инвестиций на ИБ в данном докладе будет рассмотрен проект создания корпоративной системы защиты информации от вирусов и враждебных апплетов, интегрированной с системой контроля и управления доступом на объекте.

Используя методику оценки субъективной вероятности для предприятия базового уровня защиты условно определили три возможных степени готовности корпоративной системы защиты от вирусов и враждебных апплетов, а именно: базовую, среднюю и высокую. Также условно выделим три степени готовности системы контроля и управления доступом: базовая, средняя, высокая.

Проект по созданию корпоративной системы защиты информации от вирусов предполагает определенной развитие и переход от некоторого базового уровня (0 уровень) к более высокому (10 уровню согласно лучшей практики). Также будут приведены характеристики процесса развития корпоративной системы защиты информации на выделенных уровнях защиты, статьи расходов базового и повышенного уровня защиты, показан уровень расходов при переходе на более высокий уровень защищенности КИС (переход с 0-ого уровня на 10-й). Полученные данные о снижении ТСО в среднем на 230 тыс. долл. в год позволяет обосновать инвестиции в размере около 600 тыс. долл. на защиту от вирусов. При этом период окупаемости составляет не более 3 лет.

Таким образом, применение методики ТСО для обоснования инвестиций в проекты обеспечения информационной безопасности на предприятии вполне обоснованно и имеет право на существование. При этом выбор конкретной методики оценки затрат на ИБ находится в сфере ответственности руководителей соответствующих служб и отделов информации.

Литература

[1] www.Citforum.ru