**Лекция 6 (Продолжение)**

**Соотношение эффективности и рентабельности систем информационной безопасности**

Часто оказывается довольно трудно или практически невозможно оценить прямой экономический эффект от затрат на ИБ. Тем не менее современные требования бизнеса, предъявляемые к информационной безопасности, диктуют настоятельную необходимость использовать обоснованные технико-экономические методы и средства, позволяющие количественно измерять уровень защищенности компании, а также оценивать экономическую эффективность затрат на ИБ.

Можно использовать, например, следующие показатели: экономическую эффективность и непрерывность бизнеса (Business Continuity and Productivity — BCP), общую величину затрат на внедрение системы ИБ (Net Present Value — NPV), совокупную стоимость владения системой ИБ (Тotal Сost of Оwnership — TCO), коэффициент возврата инвестиций в ИБ (Return on Investment — ROI) и другие. В целом эти показатели позволяют:

* 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 в данной отрасли;
* оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ТСО.

Количественно показатель ТСО выражается суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации. ТСО может рассматриваться как ключевой количественный показатель эффективности ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

Прямые затраты включают как капитальные компоненты затрат (элементы Software/Hardware, телекоммуникации, разработка, внедрение, эксплуатация, сопровождение, совершенствование непосредственно системы ИБ, административное управление), так и трудозатраты, которые учитываются в категориях производственных операций и административного управления. Сюда же относят затраты на обучение и повышение квалификации персонала, консалтинг по ИБ, услуги удаленных пользователей, аутсорсинг и др., связанные с поддержкой деятельности системы ИБ и организации в целом.

Косвенные затраты отражаются в составе затрат посредством таких измеримых показателей как простои, сбои в работе и отказы корпоративной системы защиты информации и КИС в целом, как затраты на операции и поддержку (не относящиеся к прямым затратам). Часто косвенные затраты играют значительную роль, так как они обычно изначально не видны и не отражаются в бюджете на ИБ, а выявляются при анализе затрат в последствии — это в конечном счете приводит к росту "скрытых" затрат компании на ИБ, не учитываемых в совокупной стоимости продукта компании.

В ходе работ по организации ИБ проводится сбор информации и расчет показателей ТСО, BCP и ROI организации по следующим параметрам:

* расходы на существующие компоненты КИС и информационные активы компании (базы данных, хранилища знаний, сетевые устройства, серверы и клиентские места, периферийные устройства);
* расходы на организацию ИБ в компании (разработку концепции и политики безопасности, планирование и управление процессами защиты информации, обслуживание средств защиты информации и данных, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, и пр.);
* расходы на аппаратные и программные средства защиты информации, персонал (приобретение, внедрение, эксплуатация, расходные материалы, амортизация, зарплата);
* расходы на организационные меры защиты информации, включая подготовку персонала;
* существующие косвенные расходы на организацию ИБ в компании и в частности обеспечение непрерывности или устойчивости бизнеса компании;
* экономию средств и ресурсов, внутренние и внешние доходы от оказания услуг в области обеспечения ИБ.

Анализ собранных показателей позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, например: "сейчас мы тратим на ИБ столько-то, если будем тратить столько-то по конкретным направлениям ИБ, то получим такой-то реальный экономический эффект".

В целом, определение затрат компании на ИБ подразумевает решение следующих трех задач [Петренко С,. 2006]:

* оценку текущего уровня ТСО корпоративной системы защиты информации и КИС в целом;
* аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня ТСО;
* формирование целевой модели ТСО.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ТСО. В ходе работ по оценке ТСО проводится сбор информации и расчет показателей ТСО организации по следующим направлениям:

* существующие компоненты КИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);
* существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация);
* существующие расходы на организацию ИБ в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.);
* существующие расходы на организационные меры защиты информации;
* существующие косвенные расходы на организацию ИБ в компании и в частности обеспечение непрерывности или устойчивости бизнеса компании.

Аудит ИБ компании. По результатам собеседования с менеджерами компании и проведения инструментальных проверок уровня защищенности организации выполняется анализ следующих основных аспектов:

* политики безопасности;
* надёжности организации защиты;
* классификации и управления информационными ресурсами;
* подготовленности персонала;
* физической безопасности;
* администрирования компьютерных систем и сетей;
* управления доступом к системам;
* разработки и сопровождения систем;
* планирования бесперебойной работы организации;
* проверки всей системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

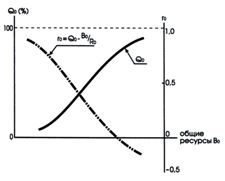
Сравнение текущего показателя ТСО проверяемой компании с модельным значением показателя ТСО позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение "узких" мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

Формирование целевой модели ТСО. По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку. Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Проиллюстрируем сказанное на примере определения оптимальной величины соотношения "эффективность-рентабельность" [Астахов А.Н., 2002]. Эффективные системы защиты стоят дорого, и поэтому при формировании контрмер, комплектовании отделов ИБ и выборе соответствующих программно-аппаратных средств необходимо учитывать рентабельность средств защиты.

На [рис. 4.21](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=4#image.4.21) показано уменьшение относительного ущерба вследствие применения средств защиты информации. Здесь величина Q_0 - мера общей эффективности защиты, R_0 - величина максимального ущерба. Чем больше Q_0, тем меньший ущерб создадут угрозы. Таким образом, мерой риска является величина (1 - Q_0). Стремление обеспечить высокоэффективную защиту, когда Q_0 близко к 1 (или 100%), приводит к значительным расходам на ресурсы.

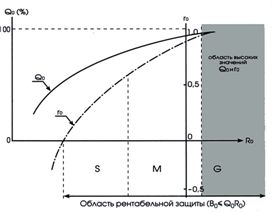


**Рис. 4.21.**Зависимость эффективности и рентабельности системы защиты от величины общих ресурсов

Чем выше совокупные ассигнования B_0 на ресурсы, тем на большую эффективность защиты можно рассчитывать ([рис. 4.21](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=4#image.4.21), сплошная кривая). Однако чрезмерные расходы на собственную безопасность не всегда оправданы экономически.

Можно столкнуться с ситуацией, когда стоимость защиты B_0 превысит уровень максимального ущерба от реализации угроз. В этом случае возникает опасность угрозы "разорения" от защиты. Её уровень также можно оценить, к примеру, величиной r_0 разности относительного "защищенности" Q_0 и относительных затрат В_0/R_0 на ресурсы. Назовем эту величину рентабельностью защиты. Если она положительная (т. е. В_0 \le R_0*Q_0), то защита рентабельна. В отличие от эффективности, чем больше затраты B_0, тем меньше рентабельность. Эта противоположность создает неоднозначную ситуацию в выборе стратегии защиты, которую необходимо заранее планировать, чтобы защита не привела к значительным убыткам.

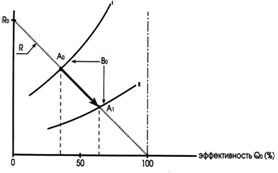
На [рис. 4.22](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=4#image.4.22) представлена типовая зависимость эффективности защиты Q_0 и ее рентабельности r_0 от максимального ущерба R_0. По сути, это является мерой масштабности бизнеса. Легко видеть, что сделать защиту одновременно и высокоэффективной, и высокорентабельной под силу лишь крупным коммерческим структурам (область G), для которых характерны большие величины максимального ущерба.



**Рис. 4.22.**Зависимость эффективности и рентабельности защиты от величины максимального ущерба

Достаточно, например, чтобы B_0 соотносилось с R_0(1–Q_0). Тогда при Q_0 \to1 получим r_0 \to1. В худшем положении оказываются интересы среднего (область М) и малого (область S) бизнеса, поскольку из-за ограниченности ресурсов выбор стратегии защиты более сложен. Рекомендации просты: надо обеспечить максимально возможную эффективность при положительном показателе рентабельности защиты. А это означает, что в первую очередь следует противодействовать наиболее вероятным и опасным угрозам. Малые и средние компании должны разумно сочетать необходимую защиту и экономию ресурсов.

[Рис. 4.23](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=4#image.4.23) показывает, какую выгоду могут обеспечить кооперативные формы обеспечения ИБ. Здесь представлены характерные зависимости величины риска R=R_0*(1-Q_0) и общих затрат на ресурсы B_0 от эффективности автономной (I) и кооперативной (II) защиты. Точка пересечения А0 зависимостей R(Q) и B(Q) для автономной защиты соответствует примерно области минимальных общих потерь R_0(1–Q_0)+B_0.



**Рис. 4.23.**Зависимости риска R и расходов на ресурсы В0 от эффективности защиты Q0

Экономия ресурсов выразится в том, что исходная зависимость (I) окажется "выше" новой зависимости (II), которая отображает кооперацию в использовании ресурсов. Соответственно новая точка пересечения кривых А_1 окажется правее прежней А_0. Практически это означает, что при сохранении рентабельности защиты увеличивается ее эффективность. Причем выигрыш тем существенней, чем больше экономия.

На практике в основном кооперируются по двум формам - материально-техническим и кадровым ресурсам, которые и являются составными частями общего механизма обеспечения ИБ.

Приобретение и поддержка средств защиты - это не бесполезная трата финансовых средств. Это инвестиции, которые при правильном вложении окупятся с лихвой и позволят вывести бизнес на желаемую высоту!