

1 Основы экономики информационной безопасности

Управление информационной безопасностью, так же, как и управление во многих других сферах деятельности, предполагает периодическое принятие различных управленческих решений, заключающихся, как правило, в выборе определенных альтернатив (отборе одной из возможных организационных схем или одного из доступных технических решений) или определении некоторых параметров отдельных организационных и/или технических систем и подсистем. Одним из возможных подходов к выбору альтернатив в ситуации принятия управленческого решения является т.н. «волевой» подход, когда решение по тем или иным причинам принимается интуитивно, и формально обоснованная причинно-следственная взаимосвязь между определенными исходными предпосылками и конкретным принятым решением не может быть установлена. Очевидно, что альтернативой «волевому» подходу становится принятие решений, основанное на определенных формальных процедурах и последовательном анализе.

Основой такого анализа и последующего принятия решений является экономический анализ, предполагающий изучение всех (или хотя бы основных) факторов, под влиянием которых происходит развитие анализируемых систем, закономерностей их поведения, динамики изменения, а также использование универсальной денежной оценки. Именно на основе адекватно построенных экономических моделей и осуществляемого с их помощью экономического анализа должны приниматься решения, касающиеся как общей стратегии развития, так и отдельных организационных и технических мероприятий, как на уровне государств, регионов и отраслей, так и на уровне отдельных предприятий, подразделений и информационных систем.

При этом, так же как и экономика любой отрасли деятельности имеет свои особенности, экономика информационной безопасности, рассматриваемая как относительно самостоятельная дисциплина, с одной стороны, базируется на некоторых общих экономических законах и методах анализа, а с другой – нуждается в индивидуальном понимании, развитии специфических подходов к

анализу, накоплении статистических данных, специфичных для этой сферы, формировании устойчивых представлений о факторах, под влиянием которых функционируют информационные системы и средства защиты информации.

Сложность задач экономического анализа практически во всех областях деятельности, как правило, обуславливается тем, что многие ключевые параметры экономических моделей невозможно достоверно оценить, и они носят вероятностный характер (такие как, например, показатели потребительского спроса). Анализ усложняется также тем, что даже небольшие колебания (корректировка оценок) таких параметров могут серьезно повлиять на значения целевой функции и, соответственно, на решения, принимаемые по результатам анализа. Таким образом, для обеспечения как можно большей достоверности расчетов в процессе проведения экономического анализа и принятия решений необходимо организовать комплекс работ по сбору исходной информации, расчету прогнозных значений, опросу экспертов в различных областях и обработке всех данных. При этом в процессе проведения такого анализа необходимо уделять особое внимание промежуточным решениям, касающимся оценок тех или иных параметров, входящих в общую модель. Необходимо также учитывать то обстоятельство, что сам по себе такой анализ может оказаться достаточно ресурсоемкой процедурой и потребовать привлечения дополнительных специалистов и сторонних консультантов, а также усилий со стороны различных специалистов (экспертов), работающих на самом предприятии, – все эти затраты, в конечном счете, должны быть оправданы.

Особая сложность экономического анализа в такой сфере, как информационная безопасность, обуславливается такими специфическими факторами, как:

- быстрое развитие информационных технологий и методик, используемых в этой сфере (как средств и методов защиты, так и средств, и методов нападения);

Тема 2.11 – Экономика планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- невозможность достоверно предугадать все возможные сценарии нападения на информационные системы и модели поведения нападающих;

- невозможность дать достоверную, достаточно точную оценку стоимости информационных ресурсов, а также оценить последствия различных нарушений в денежном выражении.

Это требует дополнительных усилий по организации процесса экономического анализа, а также зачастую приводит к тому, что многие принимаемые решения, относящиеся к обеспечению информационной безопасности, могут оказаться неадекватными. Примерами ситуаций, в которых недостаточная развитость методологии экономического анализа негативно влияет на состояние информационной безопасности, могут быть случаи, когда:

- руководство предприятия может принять неадекватные решения относительно инвестиций в средства защиты информации, что, в свою очередь, может привести к убыткам, которых можно было избежать;

- руководство предприятия может принять определенные решения относительно организации бизнес-процессов и процессов обработки информации на предприятии, исходя из стремления сократить текущие затраты и уменьшить нагрузку на персонал, при этом не принимая во внимание экономические последствия недостаточной защищенности информационных ресурсов;

- страхователь и страховщик могут не заключить договор о страховании информационных рисков или установить неадекватные параметры такого договора ввиду того, что отсутствуют модели и методы оценки экономических параметров сделки.

2 Анализ вложений в средства защиты информации

В процессе текущей деятельности предприятиям постоянно приходится сталкиваться с теми или иными изменениями: уточняются бизнес-процессы, меняется конъюнктура рынков сбыта и рынков потребляемых материальных ресурсов и услуг, появляются новые технологии, изменяют свое поведение конкуренты и контрагенты, меняется законодательство и политика государства и т.д. В этих условиях менеджерам (в том числе и руководителям, отвечающим за обеспечение информационной безопасности) приходится постоянно анализировать происходящие изменения и адаптировать свою работу к постоянно меняющейся ситуации. Конкретные формы, в которых проявляется реакция руководителей, могут быть различными. Это может быть смена маркетинговой политики, реорганизация бизнес-процессов, изменение технологий, изменение производимого продукта, слияние с конкурентами или их поглощение и пр. Однако при всем разнообразии возможных моделей поведения в меняющейся среде почти всех их объединяет один важный общий для них методологический элемент: в большинстве случаев реакция бизнеса на новые угрозы и новые возможности предполагает осуществление новых более или менее долгосрочных и ресурсоемких вложений (инвестиций) в определенные организационные и/или технические мероприятия, которые, с одной стороны, предполагают расходование ресурсов (денежных средств), а с другой – дают возможность получить новые выгоды, выражающиеся в увеличении дохода или сокращении некоторых текущих расходов.

Таким образом, в ситуации, когда необходимо осуществить некоторые новые организационные или технические мероприятия (реализовать проект), основной задачей лиц, отвечающих за эффективную организацию информационной безопасности, является четкое соотнесение затрат, которые придется понести в связи с реализацией этого мероприятия (как единовременные, так и постоянные текущие), и дополнительных (новых) денежных потоков, которые будут получены. В данном случае под денежным

потоком может пониматься экономия затрат, предотвращение убытков, а также дополнительный доход предприятия.

В качестве основного показателя, отражающего это соотношение, в экономической практике принято использовать функцию отдачи от инвестиций – Return on Investment, ROI .

$$ROI = NPV(R, d) + NPV(C, d)$$

где:

R – дополнительный денежный поток, создаваемый в результате реализации проекта;

C – затраты, связанные с реализацией проекта (расход ресурсов, отрицательная величина);

d – ставка дисконтирования;

NPV – функция дисконтирования.

Функция дисконтирования используется при анализе инвестиционных вложений для учета влияния фактора времени и приведения разновременных затрат к одному моменту (обычно моменту начала реализации проекта). Ставка дисконтирования в этом случае позволяет учесть изменение стоимости денег с течением времени.

Модель отдачи от инвестиций наглядно демонстрирует, какие две основные задачи необходимо решить при анализе любого инвестиционного проекта и, в частности, проекта по реализации мероприятий в сфере информационной безопасности: расчет затрат, связанных с проектом, и расчет дополнительного денежного потока. Если методология расчета совокупных затрат (C) за последние 10-15 лет в целом достаточно полно сформировалась (в виде концепции «Total Cost of Ownership», TCO – Совокупная стоимость владения, ССВ) и активно используется на практике применительно к различным видам информационных систем и элементам информационной инфраструктуры, то расчет дополнительного денежного потока (R), получаемого в результате инвестиций в средства защиты информации, как

правило, вызывает серьезные затруднения. Одним из наиболее перспективных подходов к расчету этого показателя является методика, которая опирается на количественную (денежную) оценку рисков ущерба для информационных ресурсов и оценку уменьшения этих рисков, связанного с реализацией дополнительных мероприятий по защите информации.

Таким образом, в целом состав методологии анализа целесообразности вложений средств в проекты, направленные на обеспечение информационной безопасности, схематично представлен на Рисунке 1.



Рисунок 1 – Структура методологии анализа эффективности вложений в проекты по УИБ

Анализ затрат, связанных с реализацией проекта, хотя и является относительно более простой задачей, все же может вызвать определенные затруднения. Так же как и для многих других проектов в сфере информационных технологий, анализ затрат на реализацию проектов в сфере информационной безопасности целесообразно осуществлять, опираясь на известную базовую методологию «Total Cost of Ownership» – ТСО (Совокупная стоимость владения – ССВ), введенную консалтинговой компанией «Gartner Group» в 1987 году применительно к персональным компьютерам. В целом, эта методика ориентирована на обеспечение полноты анализа издержек (как прямых, так и косвенных), связанных с информационными технологиями и информационными системами, в ситуациях, когда необходимо оценить экономические последствия внедрения и использования таких систем: при оценке эффективности инвестиций, сравнении альтернативных технологий, составлении капитальных и текущих бюджетов и пр.

В общем случае суммарная величина ССВ включает в себя:

- затраты на проектирование информационной системы;
- затраты на приобретение аппаратных и программных средств: вычислительная техника, сетевое оборудование, программное обеспечение (с учетом используемых способов лицензирования), а также лизинговые платежи;
- затраты на разработку программного обеспечения и его документирование, а также на исправление ошибок в нем и доработку в течение периода эксплуатации;
- затраты на текущее администрирование информационных систем (включая оплату услуг сторонних организаций, которым эти функции переданы на аутсорсинг);
- затраты на техническую поддержку и сервисное обслуживание;
- затраты на расходные материалы;
- затраты на телекоммуникационные услуги (доступ в Интернет, выделенные и коммутируемые каналы связи и пр.);

– затраты на обучение пользователей, а также сотрудников ИТ-подразделений и департамента информационной безопасности;

– косвенные затраты – издержки предприятия, связанные с потерей времени пользователями в случае сбоев в работе информационных систем.

Также в расчет затрат на повышение уровня информационной безопасности необходимо включить расходы на реорганизацию бизнес-процессов и информационную работу с персоналом: оплата услуг бизнес-консультантов и консультантов по вопросам информационной безопасности, расходы на разработку организационной документации, расходы на проведение аудитов состояния информационной безопасности и пр. Кроме того, при анализе расходов необходимо также учесть то обстоятельство, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала предприятия и необходимость осуществления дополнительных операций при работе с информационными системами. Это обуславливает некоторое снижение производительности труда сотрудников предприятия и, соответственно, может вызвать дополнительные расходы.

Значение ССВ в каждом конкретном случае необходимо определять индивидуально с учетом особенностей проекта, который предстоит реализовать: основной востребованной функциональности, существующей инфраструктуры, количества пользователей и других факторов. В общем виде ССВ для анализа эффективности и целесообразности вложений в реализацию проектов по повышению уровня защищенности информации определяется как сумма всех элементов затрат, скорректированная с учетом фактора времени:

$$NPV(C, d) = \sum_{t=0}^T \frac{\sum_{n=1}^N C_{tn}}{(1+d)^t}$$

где:

T – предполагаемый жизненный цикл проекта (информационной и/или организационной системы), лет;

N – количество видов затрат, принимаемых в расчет;

C_{nt} – затраты n -ого вида, понесенные в t -ом периоде, руб.

Таким образом, в целом могут быть определены затраты, связанные с реализацией мероприятий по обеспечению информационной безопасности. Однако наибольшую сложность представляет определение положительного эффекта от внедрения средств защиты информации. Как правило, эффект от внедрения информационных систем (ERP-систем, систем автоматизации бухгалтерского и управленческого учета, CAD/CAM-систем и пр.) определяется тем, что они обеспечивают автоматизацию и ускорение различных бизнес-операций, а это, в свою очередь, позволяет сократить затраты ручного труда, приобрести конкурентные преимущества и, таким образом, повысить общую эффективность хозяйственной деятельности. Однако внедрение средств защиты информации само по себе, как правило, не обеспечивает сокращения затрат (хотя в отдельных случаях может и обеспечить) – достижение положительного эффекта от их использования зависит от множества трудно контролируемых факторов как внутри предприятия, так и вне его. Более того, как уже было отмечено, реализация мероприятий, связанных с обеспечением информационной безопасности, может привести к дополнительным нагрузкам на персонал предприятия и, соответственно, к снижению производительности труда.

В связи с этим одним из немногих способов, которые могли бы помочь предприятию определить эффект от осуществления мероприятий в сфере защиты информации, является денежная оценка (хотя бы приблизительная) того ущерба, который может быть нанесен информационным ресурсам предприятия и который может быть предотвращен в результате реализации предлагаемых мероприятий. Таким образом, предполагаемый

предотвращенный ущерб (разница между предполагаемым ущербом в случае отказа от реализации мероприятий и ущербом в случае их реализации) будет составлять полученный экономический эффект – дополнительный денежный поток.

Очевидно, что при таком подходе большинство расчетов могут быть только оценочными и носить приблизительный характер. Это связано с тем, что активность злоумышленников, являющихся источниками угроз для информационной безопасности, практически непредсказуема: невозможно достоверно предсказать стратегии нападения, квалификацию нападающих, их конкретные намерения и ресурсы (финансовые, технические, организационные), которые будут задействованы для совершения тех или иных действий, а также намерения в отношении украденной информации (если целью атаки будет похищение конфиденциальных сведений). Соответственно, для осуществления всех необходимых расчетов необходимо сделать множество допущений и экспертных оценок в контексте деятельности данного конкретного предприятия, а также по возможности изучить статистическую информацию, касающуюся атак на информационные ресурсы, аналогичные защищаемым.

Таким образом, экономическая оценка эффективности мер по защите информации предполагает:

- оценку существующих угроз для информационных активов, которых коснется реализация защитных мер;
- оценку вероятности реализации каждой из выявленных угроз;
- экономическую оценку последствий реализации угроз.

Для осуществления такого анализа, как правило, используются следующие базовые понятия.

1) Оценочная величина единовременных потерь (Single Loss Expectancy, SLE_i) – предполагаемая средняя оценочная сумма ущерба в результате одного нарушения информационной безопасности i -го типа. Она может быть

определена как произведение общей стоимости защищаемых информационного активов (AV) на коэффициент их разрушения вследствие нарушения информационной безопасности (подверженности нападению), который обозначается EF_i (Exposure Factor).

2) Количество нарушений информационной безопасности за год (Annualized Rate of Occurrence, ARO_i) – оценочная частота, с которой в течение года происходят нарушения информационной безопасности (реализуются угрозы) i -го типа.

3) Оценочная величина среднегодовых потерь (Annualized Loss Expectancy, ALE_i) – суммарный размер потерь от нарушений информационной безопасности (реализации рисков) i -го типа в течение года.

$$ALE_i = SLE_i \times ARO_i = (AV \times EF_i) \times ARO_i$$

Непосредственный эффект от реализации мероприятий по повышению уровня информационной безопасности будет проявляться в том, что:

– негативные последствия каждого нарушения (каждой реализованной угрозы) после реализации мероприятий (EF'_i) будут меньше, чем были до их реализации: $EF_i > EF'_i$;

– частота нарушений информационной безопасности уменьшится после реализации мероприятий $ARO_i > ARO'_i$.

В результате уменьшенная величина ALE'_i будет составлять:

$$ALE'_i = SLE_i \times ARO'_i = (AV_i EF'_i) \times ARO'_i$$

Таким образом, суммарный годовой эффект от реализации мероприятия будет определяться как:

$$R = \Delta ALE_i = ALE_i - ALE'_i$$

Исходя из этого, общий денежный поток от реализации мероприятия определяется по следующей формуле:

$$NPV(R, d) = \sum_{t=0}^T \frac{\sum_{i=1}^I (ALE_{it} - ALE'_{it})}{(1 + d)^t}$$

На основе всех этих данных в соответствии с формулой может быть определен суммарный эффект от реализации мероприятий в сфере информационной безопасности и продемонстрировано, насколько оправданными и целесообразными являются вложения в те или иные средства защиты информации в условиях конкретного предприятия с учетом всех особенностей его функционирования (а также с учетом принятых допущений и сделанных предположений).

И хотя с математической точки зрения все расчеты в описанной рамочной модели оценки ROI являются предельно простыми, определение отдельных параметров (прогнозных частот нарушений и размеров потерь, а также предполагаемого срока использования программных и аппаратных средств и организационных моделей) может вызвать значительные затруднения на практике. Проведение таких расчетов, так же как и проведение аудитов информационной безопасности, может потребовать привлечения сторонних консультантов, однако квалификация и профессиональная специализация таких консультантов может существенно отличаться от квалификации консультантов, специализирующихся, например, на проведении аудитов и внедрении технических средств защиты информации. Причем если оценку вероятностей атак, а также оценку того, насколько эти атаки могут быть успешными, предпочтительно доверить внешним консультантам по информационной безопасности, то оценку стоимости информации и экономических последствий утраты контроля над информационными активами, скорее всего, целесообразно осуществлять самим специалистам, работающим на предприятии (экономистам, маркетологам и пр.), а также привлекать для этого сторонних специалистов из соответствующих сфер деятельности (маркетинга, финансов, торговли и пр.).

Несмотря на все трудности процесса оценки целесообразности внедрения средств защиты, описанная методология позволяет менеджерам и специалистам

по защите информации получать обоснованные оценки и делать формализованные выводы относительно того, насколько оправданными являются вложения в определенные средства защиты информации, а также определить основные приоритеты расходования средств, предусмотренных в бюджете на обеспечение информационной безопасности (если предприятие практикует выделение фиксированных сумм на эти цели). При этом достаточно высокий уровень достоверности таких оценок достигается за счет того, что вся работа по проведению оценки и подготовке инвестиционных решений раскладывается на несколько относительно более простых и «прозрачных» задач, решение каждой из которых может быть закреплено за специалистами в определенной сфере. В результате общая оценка складывается на основе полученных решений нескольких отдельных задач, каждое из которых может быть проконтролировано и при необходимости дополнительно уточнено. В этих условиях общее качество получаемой аналитической оценки и, соответственно, формулируемого решения зависит от квалификации всех экспертов, аналитиков и специалистов, участвующих в работе. А значит, одной из основных задач руководителей предприятия и менеджеров, отвечающих за обеспечение информационной безопасности и принятие решений в этой сфере, является подбор наиболее квалифицированных и опытных специалистов, ибо от качества их работы будет зависеть не просто безопасность отдельных элементов информационных активов в определенные моменты времени, а эффективность всей системы защиты информации в среднесрочной, а иногда и в долгосрочной перспективе.