3.5. ВЫБОР МЕТОДОВ И СРЕДСТВ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ ПРЕДПРИЯТИЯ

Завгородний В.И., к.т.н., доцент кафедры «Информационные технологии»

Финансовая академия при Правительстве Российской Федерации

В статье раскрывается сущность информационных рисков и основные стратегии управления информационными рисками предприятия. Предлагаются алгоритмы выбора методов и средств управления информационными рисками. Алгоритмы позволяют сократить общие расходы на управление информационными рисками.

ВВЕДЕНИЕ

Проблема управления информационными рисками по мере развития информационных технологий приобретает особую остроту. Объясняется это постоянно увеличивающейся величиной расходов на управление информационными рисками, которые складываются из ущерба от информационных рисков и затрат предприятий на противодействие таким рискам. В этих условиях руководство предприятием уже не может возлагать решение этой проблемы только на службу безопасности и отдел информационных технологий. В управлении информационными рисками необходимо участвовать менеджерам всех уровней во главе с руководством предприятия.

Для этого они должны владеть знаниями и навыками управления информационными рисками. Им требуется, прежде всего, умение использовать все доступные финансовые и организационные методы управления информационными рисками.

Управление информационными рисками становится одним из основных направлений риск-менеджмента предприятия и направлено на достижение наивысшей экономической эффективности и стабильности функционирования предприятия.

СТРАТЕГИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

В мировой экономической науке существует две теории относительно сущности рисков. Классический подход к пониманию риска трактует его как возможное событие, приводящее к ущербу. В рамках неоклассической теории рассматриваются спекулятивные риски, которые предполагают наличие случайных событий, приводящих как к потерям, так и к получению положительных результатов, превышающих ожидаемые результаты предпринимательской деятельности. В области безопасности общепринятым является классический подход к пониманию рисков, который и используется в отношении информационных рисков.

С позиций высшего менеджмента предприятия сущность информационных рисков необходимо рассматривать следующим образом. Информационный риск – это возможность наступления случайного события, приводящего к нарушениям функционирования информационной системы предприятия и снижению качества информации, а также к неправомерному использованию, распространению или противодействию распространения информации во внешней среде, в результате которых наносится ущерб предприятию.

Понятие «информационная система» включает в себя все ресурсы предприятия, которые используются для получения, хранения, обработки, передачи и применения информации, а также информационные ресурсы. В состав информационных систем входят следующие компоненты:

- компьютерные системы;
- системы передачи информации;
- оргтехника;
- базы данных и файлы компьютерных систем;
- документы в печатной форме;
- аудио и видеоинформация на носителях различной физической природы.

В качестве одного из основных ресурсов информационной системы рассматривается специалист, имеющий отношение к использованию или эксплуатации информационной системы.

К компьютерным системам относятся компьютеры различного назначения, вычислительные системы и комплексы, вычислительные сети. В качестве компьютерных систем рассматриваются также блоки и узлы, входящие в состав других устройств и реализующие программный принцип управления для обработки информации. К таким системам относятся, прежде всего, блоки управления станками, транспортными средствами, средствами автоматизированного доступа на объекты, средствами связи и тому подобными устройствами.

Понятие «информационный риск» включает в себя все возможные события, которые могут воздействовать на любые ресурсы информационной системы и наносить ущерб предприятию.

Важное место в определении информационного риска занимает положение о том, что причиной ущерба может служить снижение качества информации. Качество информации характеризуется следующими показателями:

- достоверность;
- актуальность;
- конфиденциальность;
- полнота;
- своевременность получения;
- форма представления;
- избыточность.

Использование категории «качество информации» в определении информационного риска позволяет существенно расширить рамки рисковых событий. В результате этого учитываются события, влияющие на все показатели качества информации на всех этапах ее использования на предприятии, во всех звеньях информационной технологической цепи, включая работу с документами на бумажных носителях, видео- и аудио-информацией.

Наиболее полное определение информационного риска в широком смысле вводится с применением понятия «информационная сфера предприятия». При этом под информационной сферой предприятия будем понимать информационные ресурсы, средства и субъекты информационных процессов, а также систему регулирования отношений субъектов информационных процессов во внутренней и внешней среде предприятия.

Тогда информационный риск в широком смысле – это возможность наступления случайного события в информационной сфере предприятия, в результате которого предприятию будет нанесен ущерб.

Для достижения эффективности и стабильности предприятия информационными рисками необходимо управлять. Под управлением информационными рисками будем понимать систему согласованных мер, мероприятий и процедур, осуществляемых персоналом предприятия с целью минимизации расходов на противодействие информационным рискам и устранение их последствий.

Минимизация расходов на управление информационными рисками выбрана в качестве цели исходя из классического подхода к пониманию информационных рисков. Учитывается также, что безопасность и качество информации обеспечивают эффективность всех бизнес-процессов. Сокращение общих расходов на управление информационными рисками позволяет повысить эффективность производственных процессов в целом.

Расходы на управление информационными рисками складываются из затрат на создание, эксплуатацию и модернизацию системы управления информационными рисками, а также ущерба, который несет предприятие в результате реализации рисковых событий.

В отношении информационных рисков могут приниматься следующие стратегии управления:

- принятие риска;
- предотвращение риска;
- снижение возможного ущерба от риска;
- предотвращение риска и снижение возможного ущерба от него.

Принятие риска означает, что в отношении соответствующего риска не применяются никакие механизмы предотвращения информационного риска и минимизации ущерба от его реализации. Под механизмами управления информационными рисками понимаются все возможные методы и средства, используемые для снижения расходов предприятия, связанных с этими рисками. Стратегия принятия риска выбирается в отношении информационных рисков, ожидаемый ущерб от которых незначителен, а также при очень малой вероятности рискового события и ожидаемом ущербе, который не относится к категории катастрофических для предприятия.

Стратегия предотвращения информационных рисков предполагает воздействие на источники рисков с целью снижения вероятности наступления рискового события. Эта стратегия требует также устранения факторов, способствующих реализации рисков.

Величина ущерба от информационного риска может быть снижена, если в информационную систему заблаговременно внедряются и применяются специальные механизмы. Суть принимаемых мер в соответствии с третьей стратегией заключается в придании устойчивости предприятия к воздействию информационных рисков. Основу такой стратегии составляют адаптивная система управления и необходимые резервные ресурсы. В качестве резервов используются аппаратные, программные, информационные и финансовые ресурсы.

Для управления информационными рисками применяются два финансовых механизма управления:

- создание финансовых резервов;
- страхование рисков.

Финансовые резервы должны создаваться во всех системах управления информационными рисками. Эти резервы используются для оперативного устранения последствий рисковых событий. Зарезервированные финансовые ресурсы используются, прежде всего, на блокирование распространения негативного влияния рискового события на информационную систему и бизнес-процессы. а также на обеспечение применения других механизмов устранения последствий рисковых событий.

Страхование информационных рисков, в силу целого ряда причин, пока еще не нашло широкого применения в российской практике управления информационными рисками. Этот перспективный вид финансовых механизмов управления информационными рисками применим для определенных рисков и выбирается на основе анализа рисков.

Наиболее совершенной является стратегия, которая предполагает использование, как механизмов предотвращения информационных рисков, так и механизмов снижения ущерба от информационных рисков.

ОПТИМИЗАЦИЯ РАСХОДОВ НА УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Чтобы минимизировать общие расходы на управление информационными рисками, руководству предприятия приходится решать оптимизационную задачу о распределении финансовых средств, которые следует направлять на создание и развитие тех или иных механизмов защиты от информационных рисков. Причем возможны два варианта решения такой задачи:

- без ограничения на привлекаемые средства;
- средства на управление информационными рисками лимитированы.

Независимо от выбранной стратегии управления информационным риском, необходимо определить минимальный объем собственных резервных ресурсов, которые следует создать для оперативного реагирования в случае наступления ***i***-го рискового события. Объем собственных резервов определяется после анализа всех рисков. Он выбирается равным величине резервных ресурсов, необходимых для оперативного парирования риска с максимальным ожидаемым ущербом.

Предварительный выбор стратегии осуществляется на основании анализа информационных рисков. Например, если риск может привести к серьезному ущербу, а действенных нефинансовых механизмов противодействия ему не существует, то единственной приемлемой стратегией является страхование.

Окончательный выбор конкретной стратегии и соотношения различных механизмов защиты от риска осуществляется путем анализа расходов на управление этим риском.

A. Оптимизация расходов на управление информационным риском без ограничения затрат

Пусть затраты на управление информационными рисками не ограничены. Если для парирования риска применяется только страхование, то расходы предприятия на управление ***i***-м риском F_i могут быть представлены следующим образом:

$$F_i = V_i + P_i U_i - P_i H_i ,$$

где

V_i – страховой взнос;

P_i – вероятность наступления ***i***-го рискового события;

U_i – ожидаемый ущерб от ***i***-го рискового события;

H_i – страховая сумма.

Известно, что страховая сумма с позиций страховщика всегда должна быть меньше предполагаемого ущерба. В противном случае у страхователя отсутствует мотивация противодействия риску. Если величину франшизы обозначить ΔU_i , то расходы страхователя на управление ***i***-м риском можно представить в следующем виде:

$$F_i = V_i + P_i \Delta U_i .$$

Интересы страхователя заключаются в минимизации величины F_i. Страховщик стремится установить франшизу на уровне, который побуждал бы страхователя не допустить наступления рискового события. Для этого он устанавливает, например, уровень франшизы в диапазоне 5% – 10% от суммы ожидаемого ущерба.

С позиций страховщика размер страхового взноса каждого страхователя должен быть таким, чтобы в сумме все взносы покрывали возможные выплаты страховых сумм всем страхователям *i*-го информационного риска. За счет страхового взноса должны покрываться накладные расходы на обслуживание договора о страховании. Часть страхового взноса направляется на получение прибыли страховщиком. Страховой взнос может быть определен следующим образом:

$$V_i = P_i H_i + V_i^{'},$$

где $V_i^{'}$ – часть страхового взноса, обеспечивающая покрытие расходов страхования и получение прибыли от страхования i – го информационного риска.

Страховые компании обычно вычисляют сумму страхового взноса с использованием страхового тарифа γ, который представляет собой определенный процент от страховой суммы:

$$V_i = \gamma H_i .$$

Тогда страховой тариф определяется из выражения:

$$\gamma = \frac{P_i H_i + V_i^{'}}{H_i} .$$

Наибольшее распространение имеет стратегия совместного использования противодействия информационным рискам и страхования. Для этой стратегии полные расходы на управление *i*-м информационным риском предприятия определяются следующим образом:

$$F_i(a_i, b_i) = a_i + b_i + V(a_i, b_i)_i + P(a_i)_i \Delta U(a_i, b_i), \qquad (1)$$

где a_i – затраты на предотвращение *i*-го информационного риска;

b_i – затраты на снижение ущерба от *i*-го информационного риска.

Если величина страхового тарифа и процент франшизы установлены, то расходы предприятия на управление *i*-м информационным риском зависят только от затрат на его предотвращение и снижение ущерба от этого риска. Ожидаемые значения вероятности наступления *i*-го рискового события и ущерба от этого риска зависят от затрат на нефинансовые механизмы противодействия риску. Эти величины должны быть получены на этапе анализа рисков одним из рассмотренных способов.

Величины a_i и b_i являются дискретными. Они определены соответственно на подмножествах механизмов

$$m_a^i = \{m_{a1}^i, m_{a2}^i, ..., m_{aA}^i\} \ u \ m_b^i = \{m_{b1}^i, m_{b2}^i, ..., m_{bB}^i\}.$$

В свою очередь

$$m_a^i \subset M_a \ u \ m_b^i \subset M_b ,$$

где M_a и M_b – соответственно множество механизмов предотвращения информационных рисков и множество механизмов снижения ущерба от этих рисков.

Оптимизация затрат на управление *i*-м информационным риском сводится таким образом к выбору таких подмножеств m_a^{i*} и m_b^{i*}, которые обеспечивают F_i^{min}. Возможны два варианта исходного состояния системы, определяющих алгоритм поиска решения:

- нефинансовые механизмы не использовались ранее;
- в систему уже введены механизмы предотвращения *i*-го риска и / или снижения ущерба от этого риска.

При анализе возможных вариантов сочетаний механизмов необходимо учитывать совместимость механизмов.

Для принятия решения о включении нового подмножества механизмов или замене старого подмножества новым используется критерий. В качестве критерия может быть выбрано неравенство

$$F_i - F_i^{'} \geq k , \qquad (2)$$

где F_i – значение целевой функции для исходного подмножества или подмножества, полученного на предыдущем шаге;

$F_i^{'}$ – значение целевой функции для проверяемого подмножества;

k – пороговое значение разности, при превышении которого имеет экономический смысл рассматривать в качестве текущего оптимального подмножества механизмов очередное проверяемое подмножество. Пороговое значения должно, по крайней мере, превышать границу точности метода.

При оптимизации управления только *i*-м информационным риском независимо от других рисков множества m_a^{i*} и m_b^{i*} могут быть определены путем полного перебора. Алгоритм получения оптимального решения в этом случае может быть представлен следующей последовательностью шагов.

- Шаг 1. Если для управления *i*-м информационным риском применялись нефинансовые механизмы, то они принимаются за текущие оптимальные множества m_{at}^{i*}, m_{bt}^{i*} и вычисляется значение функции F_i (выражение (1)). Переход к шагу 2.
- Шаг 2. Проверка возможности генерации подмножеств m_{at}^i и m_{bt}^i. Если проверены не все комбинации механизмов, то – переход к шагу 3, иначе – к шагу 5.
- Шаг 3. Генерация новых текущих подмножеств m_{at}^i и m_{bt}^i. Проверка совместимости механизмов. Если механизмы совместимы, то – переход к шагу 4, иначе – переход к шагу 2.
- Шаг 4. Вычисление значения функции $F_i^{'}$ (1). Если подмножества m_{at}^{i*} и m_{bt}^{i*} не пусты, то проверяется критерий (2). Если критерий выполняется или подмножества m_{at}^{i*} и m_{bt}^{i*} пусты, то текущие подмножества считаются оптимальными текущими $m_{at}^{i*} := m_{at}^i$, $m_{bt}^{i*} := m_{bt}^i$ и запоминается оптимальное текущее значение функции $F_i := F_i^{'}$. Переход к шагу 2.[1]
- Шаг 5. Запоминание результатов $m_a^{i*} := m_{at}^{i*}$, $m_b^{i*} := m_{bt}^{i*}$ и $F_i^{min} := F_i^{'}$. Окончание алгоритма.

B. Оптимизация расходов на управление информационными рисками в условиях лимита на затраты

На практике руководители часто ограничены в средствах, которые они могут направить на управление информационными рисками. Пусть предприятие имеет возможность использовать на управление информаци-

[1] Знак := означает, что величина, стоящая слева от знака, становится равной величине, записанной справа от знака.

онными рисками часть полученной прибыли, из которой на управление ***i***-м риском может быть израсходована сумма C_i. Тогда целевая функция (1) примет вид:

$$F_i(\alpha_i,\beta_i)=\alpha_i C_i+\beta_i C_i+V(\alpha_i,\beta_i)_i+P(\alpha_i)_i\Delta U(\alpha_i,\beta_i),$$

при ограничении

$$\alpha_i C_i+\beta_i C_i+V(\alpha_i,\beta_i)\le C_i,$$

где

α_i и β_i – коэффициенты, определяющие распределение средств между механизмами соответственно предотвращающих ***i***-е рисковое событие и снижающих ущерб от этого риска.

Алгоритм поиска оптимального распределения ресурсов на управление информационным риском в условиях ограничения на затраты незначительно отличается от рассмотренного алгоритма без ограничений. На шаге 3 необходимо проводить дополнительную проверку получаемых подмножеств. Стоимость подмножеств механизмов m^i_{at} и m^i_{bt}. в сумме не должна превышать значение $C_i - V(\alpha_i,\beta_i)$.

Следует отметить целесообразность сравнения результатов определения оптимальных расходов на управление ***i***-м информационным риском без ограничений и с ограничениями расходов. Сопоставив значения предполагаемых расходов и затрат на управление риском, руководство предприятия может пересмотреть лимит средств, выделяемых на управление риском. Если по результатам расчетов окажется, что незначительное увеличение затрат C_i приведет к ожидаемому значительному уменьшению расходов на управление риском, то руководство может принять оптимальный план вложения средств в управление этим риском.

Для принятия решения о выборе механизмов противодействия конкретному информационному риску необходимо также сравнить данные расчетов расходов с применением страхования и без страхования. Окончательный выбор должен выполняться с учетом приоритета механизмов предотвращения информационных рисков по сравнению с механизмами снижения ущерба от рисков.

C. Оптимальное управление всеми значимыми информационными рисками с использованием страхования

Рассмотренные алгоритмы оптимизации расходов на управление отдельным информационным риском не позволяют получить оптимальное решение для всех значимых рисков в комплексе. То есть композиция оптимальных частных решений не дает в общем случае оптимальное решение для всех рассматриваемых рисков в целом. Это объясняется тем, что отдельные механизмы противодействия информационным рискам используются для парирования нескольких рисков.

Оптимизация расходов на управление отдельными информационными рисками имеет самостоятельное практическое значение в следующих случаях:

- при появлении одного нового информационного риска;
- при существенном изменении статистики по определенному риску, без заметных изменений по всем остальным рискам.

Комплексная оптимизация расходов на управление всеми информационными рисками осуществляется во всех остальных случаях.

Целевую функцию управления всеми значимыми информационными рисками с использованием страхования и без ограничений на сумму расходов можно представить следующим образом:

$$C=\sum_K P_k U_k+\mu+\sum_I (V_i+P_i\Delta U_i)+$$
$$+\sum_J (a_j+b_j+P(a_j)U(b_j))+$$
$$+\sum_Z (a_z+b_z+V(a_z,b_z)+P(a_z)\Delta U(a_z,b_z)), \qquad (3)$$

где

K – подмножество принимаемых информационных рисков;

μ – потери от создания собственных резервов для оперативного снижения ущерба;

I – подмножество рисков, которые управляются только с помощью страхования;

J – подмножество рисков, в отношении которых применяются только нефинансовые механизмы регулирования;

Z – подмножество рисков, которые регулируются с помощью нефинансовых механизмов и страхования, остальные обозначения введены выше.

Задача оптимизации управления всеми значимыми информационными рисками заключается в выборе для каждого риска стратегии управления и определении соответствующих подмножеств механизмов защиты от рисков с целью минимизации общих затрат на механизмы противодействия и общий ущерб от рисков.

Точное решение такой задачи возможно только путем полного перебора всех возможных вариантов выбора стратегий и механизмов противодействия. При наличии десятков механизмов противодействия информационным рискам и различных стратегий их комбинирования реализация полного перебора на практике затруднена. Целесообразно использовать методы целенаправленного перебора, таких как метод ветвей и границ. Для упрощения алгоритма возможно ограничение вариантов за счет предварительного анализа и отказа уже на этом этапе от заранее неоптимальных решений.

На этапе анализа информационных рисков могут быть определены общий ущерб от принимаемых рисков $\sum_K P_k U_k$ и финансовые потери μ, связанные с созданием и обслуживанием собственных резервов. Эти два слагаемых не учитываются в процессе поиска оптимального сочетания стратегий и механизмов защиты. Они используются для определения окончательного значения расходов на управление информационными рисками. Тогда целевая функция несколько упростится:

$$C=\sum_I (V_i+P_i\Delta U_i)+\sum_J (a_j+b_j+P(a_j)U(a_j,b_j))+$$
$$+\sum_Z (a_z+b_z+V(a_z,b_z)+P(a_z)\Delta U(a_z,b_z)). \qquad (4).$$

До начала реализации алгоритма поиска оптимальной стратегии и выбора механизмов противодействия в отношении каждого информационного риска необходимо получить целый ряд данных:

- подмножество информационных рисков $R_N \subset R$, в отношении которых используются механизмы противодействия;
- множество вероятностей наступления рисковых событий $P=\{P_1,P_2,...,P_N\}$, при условии, что в отношении этих рисков не принимается никаких механизмов противодействия;
- множество ожидаемых ущербов от рисков $U=\{U_1,U_2,...,U_N\}$, при условии, что в отношении этих

рисков не принимается никаких механизмов снижения ущерба;

- множество механизмов предотвращения информационных рисков $A=\{a_1, a_2, ..., a_L\}$;
- множество механизмов снижения ущерба от информационных рисков $B=\{b_1, b_2, ..., b_Q\}$;
- бинарная матрица совместимости механизмов противодействия $M=\|m_{ij}\|$;
- множество коэффициентов эффективности механизмов предотвращения информационных рисков $K=\{K_1, K_2, ..., K_L\}$;
- множество коэффициентов эффективности механизмов снижения ущерба от информационных рисков $Y=\{Y_1, Y_2, ..., Y_Q\}$;
- подмножество затрат на каждый механизм $S=\{s_1, s_2, ..., s_D\}$;
- бинарная матрица применимости механизмов предотвращения к определенным рискам $G=\|g_{ij}\|$;
- бинарная матрица применимости механизмов снижения ущерба от определенных рисков $W=\|w_{ij}\|$.

Матрица M имеет размерность

$$E \times E, \text{ где } E = L+Q,$$

где L – количество механизмов предотвращения информационных рисков;

Q – количество механизмов снижения ущерба от информационных рисков.

Если элемент матрицы M $m_{ij}=1$, то i-й и j-й механизмы противодействия могут использоваться совместно в системе управления информационными рисками. При несовместимости механизмов соответствующий им элемент матрицы M равен 0. Матрица позволяет контролировать совместимость всех нефинансовых механизмов противодействия информационным рискам. Совместимыми являются механизмы, которые не дублируют, а дополняют друг друга, и допускают совместное использование в рамках одной организационно-технической системы.

Механизм противодействия может воздействовать сразу на несколько информационных рисков. Поэтому множество коэффициентов эффективности механизмов предотвращения рисков и множество коэффициентов эффективности снижения ущерба состоят из подмножеств. Подмножество ($K_i=\{k_\alpha^i, k_\beta^i, ..., k_\omega^i\}$) состоит из коэффициентов, причем коэффициент (k_j^i) позволяет скорректировать вероятность наступления j-го рискового события при использовании i-го механизма. Для каждого механизма i мощность подмножества K_i различна. Тогда, если для парирования i-го рискового события используются, например, механизмы предотвращения δ, λ и μ, то вероятность этого события будет определяться следующим образом:

$$P(a_i)=k_i^\delta\, k_i^\lambda\, k_i^\mu\, P_i.$$

Причем, затраты a_i определяются как сумма затрат на каждый механизм предотвращения i-го рискового события:

$$a_i=s_\delta+s_\lambda+s_\mu.$$

Множество коэффициентов $Y=\{Y_1, Y_2, ..., Y_Q\}$ предназначено для корректировки величин ущерба от введенных механизмов снижения ущерба. Подмножество ($Y_j=\{y_\varphi^j, y_\nu^j, ..., y_\gamma^j\}$) образуют коэффициенты, которые позволяют определить величину ущерба от информационных рисков φ, ν и т.д. после применения j-го механизма снижения ущерба. Если, например, для снижения ущерба от j-го риска применяются механизмы φ, ν и γ, то сумма ущерба от этого риска может быть определена таким образом:

$$U(b_j)=U_j-y_j^\varphi U_j-y_j^\nu U_j-y_j^\gamma U_j=$$
$$=U_j(1-(y_j^\varphi+y_j^\delta+y_j^\gamma)),$$

причем

$$y_j^\varphi+y_j^\nu+y_j^\gamma<1 \;u\; b_j=s_\varphi+s_\nu+s_\gamma.$$

Бинарные матрицы G и W позволяют определить нефинансовые механизмы противодействия информационным рискам, которые могут использоваться для управления тем или иным риском. Если $g_{ij}=1$ и $w_{ij}=1$, то i-й механизм может использоваться для управления j-м информационным риском, иначе – i-й механизм не применяется для управления j-м риском.

Сущность алгоритма выбора оптимального набора механизмов управления информационными рисками состоит в следующем. Осуществляется направленный перебор допустимых сочетаний механизмов по всем информационным рискам и подсчет целевой функции (4) после включения очередного механизма. Полученное на каждом шаге значение функции сравнивается с текущим оптимальным значением целевой функции, подсчитанным для всех N рисков. Если функция на определенном шаге принимает значение, превышающее текущее оптимальное значение функции, то дальнейший анализ ветви не производится, осуществляется шаг назад и просмотр следующей ветви.

Для сокращения числа проверок целесообразно анализировать возможные варианты, начиная с наиболее предпочтительных стратегий управления информационными рисками. Такой стратегией для большинства рисков является стратегия совместного использования нефинансовых механизмов противодействия информационным рискам и страхования рисков. Число проверок сокращается также в случае ограничения средств, выделяемых на управление информационными рисками.

Наиболее сложной задачей оптимизации управления информационными рисками является генерация вариантов сочетания механизмов управления для всех выбранных стратегий управления.

Укрупненный алгоритм выбора оптимального подмножества механизмов управления информационными рисками может быть представлен следующей последовательностью шагов.

- Шаг 1. Выбор стратегии управления. Если все стратегии просмотрены, то – переход к шагу 6.
- Шаг 2. Генерация набора совместимых механизмов.
- Шаг 3. Вычисление текущей целевой функции C_t. При первом вычислении функции запоминаются текущая сумма расходов в качестве оптимальной текущей функции $C_t^* := C_t$, а также наборы соответствующих механизмов, $M_{at}^* := M_{at}$, $M_{bt}^* := M_{bt}$.
- Шаг 4. Проверяется условие $C_t \geq C_t^*$. Если условие не выполняется, то запоминаются результаты в качестве оптимальных текущих значений $C_t^* := C_t$, $M_{at}^* := M_{at}$, $M_{bt}^* := M_{bt}$.

- Шаг 5. Проверка условия окончания генерации наборов механизмов для текущей стратегии. Если условие выполняется, то – переход к шагу 1, иначе – к шагу 2.
- Шаг 6. Запоминаются значения оптимального выбора механизмов противодействия информационным рискам $C^* := C_t^*$, $M_a^* := M_{at}^*$, $M_b^* := M_{bt}^*$. Работа алгоритма завершается.

Представленный алгоритм не раскрывает подробно порядок перебора механизмов, стратегий и рисков. Он показывает лишь общую последовательность выбора оптимального варианта подмножеств механизмов предотвращения и механизмов снижения ущерба от предполагаемых рисков, включая и страхование. Более подробно алгоритм изложен в [1].

D. Неформальный подход к распределению денежных средств на управление информационными рисками

В рассмотренных формальных методах оптимизации распределения сложно учесть приоритеты различных направлений противодействия информационным рискам и особенности конкретных рисков.

Так, механизмы предотвращения рисков предпочтительнее механизмов снижения ущерба, вызванного наступлением рискового события. Информационный риск всегда приводит к ущербу, который невозможно полностью покрыть заблаговременно созданными механизмами. К тому же реальные последствия наступления рискового события могут значительно превышать ожидаемые.

Формальные методы не учитывают всех особенностей рисков. Например, ожидаемый суммарный ущерб от частых рисковых событий с незначительным ущербом может быть равен ожидаемому ущербу от рискового события с очень большим ущербом и очень малой вероятностью наступления этого события. С формальных позиций такие риски не различаются по последствиям. Однако для управления ими, очевидно, необходимы разные подходы.

Приведенные доводы приводят к мысли о необходимости проведения дополнительного анализа результатов, полученных с помощью формальных методов оптимизации. Такой анализ проводится с использованием правил нестрогого предпочтения, учета особенностей информационных рисков и механизмов защиты от них, в том числе и уже применяемых в системе механизмов защиты.

На предварительных этапах анализа возможно решать задачу о выборе вида механизма защиты от информационных рисков, а затем уже отбирать конкретный механизм защиты. При выборе вида механизма защиты могут использоваться либо средние, либо наилучшие показатели эффективности механизмов каждого вида.

Эффективность i-го механизма защиты от информационного риска может оцениваться с помощью интегрированного показателя эффективности механизма K_i:

$$K_i = \frac{\nabla U}{C_i},$$

где ∇U – величина суммы денежных средств, на которую уменьшается ущерб за счет применения i-го механизма защиты за определенный период времени t;

C_i – полные затраты на i-й механизм защиты, приведенные к временному периоду t.

Принятие предварительного решения о целесообразности использования определенного механизма защиты может осуществляться на основе анализа графика зависимости ущерба от затрат на применение механизмов защиты (см. рис. 1).

Анализ графика показывает, что начиная с определенного значения затрат на механизмы защиты от информационного риска дополнительные затраты на механизмы защиты не покрываются снижением ущерба. То есть если системе управления информационными рисками по анализируемому риску соответствует точка равновесия на графике, в которой $C = U$, то дальнейшее наращивание возможностей по противодействию этому риску экономически не целесообразно.

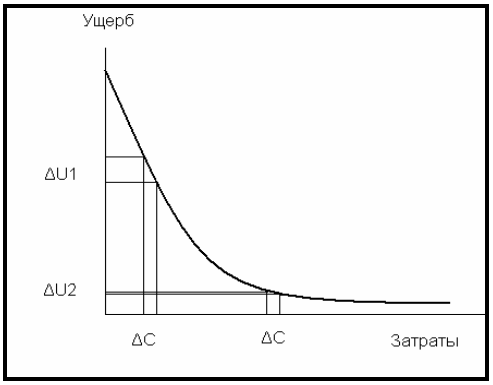

Рис. 1. Ущерб от определенного информационного риска как функция от затрат на механизмы защиты от этого риска

ЗАКЛЮЧЕНИЕ

В статье раскрывается сущность информационных рисков и основные стратегии управления информационными рисками предприятия. Предлагаются алгоритмы, позволяющие осуществлять выбор методов и средств воздействия на причины и факторы информационных рисков с целью минимизации общих расходов на управление информационными рисками.

Литература

1. Завгородний В.И. Методика выбора механизмов управления информационными рисками. / Вестник Финансовой академии. №3, 2006, с. 137-148.

Завгородний Виктор Иванович

РЕЦЕНЗИЯ

Управление информационными рисками, создание и модернизация системы управления информационными рисками становится одной из центральных задач руководства предприятия. В процессе решения этой задачи приходится осуществлять выбор методов и средств управления информационными рисками. Целью такого выбора является достижение минимальных расходов на управление информационными рисками, которые включают в себя затраты на создание и эксплуатацию системы управления и суммарный ущерб от информационных рисков.

Автор предлагает формальную постановку задачи выбора механизмов управления информационными рисками и алгоритмы решения этой задачи с применением страхования рисков. Задача рассматривается для одного информационного риска и для всех значимых информационных рисков, при безлимитном финансировании и в условиях ограничения финансовых средств. При этом учитывается совместимость методов и средств управления информационными рисками.

Следует отметить, что предлагаемые алгоритмы могут быть достаточно просто реализованы в автоматизированной системе выбора механизмов управления. Единственной сложностью остается получение исходных данных. Впрочем, эти сложности характерны для всех задач, связанных с управлением рисками, и информационными рисками прежде всего.

Статья выполнена на актуальную тему, содержит новые научные результаты и достойна опубликования в научном журнале.

Чистов Д.В., д.э.н., профессор

3.5. SAMPLING OF METHODS AND CONTROL MEANS INFORMATIONAL MARKS OF THE FACTORY

V.I. Zavgorodniy the Lecturer of Chair
«Information Technologies»

Financial academy at the Government of the Russian Federation

The essence of information risks and the basic strategy of management by information risks of the enterprise are described in article. Algorithms of a choice of methods and means's of control by information risks are offered. Algorithms allow to cut down the general expenses on management of information risks.