УДК 330.46

СИСТЕМНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ. ВЫБОР МЕХАНИЗМОВ ЗАЩИТЫ

В.И. Завгородний

Управление информационными рисками рассмотрено на уровне управления всей информационной сферой предприятия, не ограничиваясь рамками обеспечения безопасности информации. Предложен метод оптимизации выбора механизмов защиты от информационных рисков.

Ключевые слова: информационные риски, системное управление информационными рисками, система управления информационными рисками, выбор механизмов защиты от информационных рисков.

ВВЕДЕНИЕ

Появление термина «информационный риск» более десяти лет назад означало признание значимости проблемы противодействия негативным явлениям в информационной сфере предприятия, однако рассматривалась лишь область обеспечения безопасности информации. Такой подход практически остается неизменным по настоящее время [1]. Информационный риск рассматривается как угроза безопасности информации. Изменения касаются только понимания результатов реализации таких угроз, учета экономических последствий информационных рисков в виде ущерба предприятия.

В рамках обеспечения информационной безопасности по-прежнему рассматриваются лишь три негативных исхода для информационных ресурсов — нарушение конфиденциальности, доступности и целостности. Не принимается в расчет возможность снижения качества информации в результате наступления событий, не связанных с нарушением безопасности информации. Качество информации с позиций ее потребителя определяется следующими характеристиками: достоверность, актуальность, полнота, избыточность, своевременность получения, форма представления, готовность к применению. Алгоритмические и программные ошибки, сбои и отказы технических средств, ошибки субъектов информационных процессов, использование недостоверных и неполных данных, другие причины могут не отражаться на безопасности информации, но приводить к снижению качества информации. В результате использования в бизнес-процессах информации низкого качества предприятию наносится экономический ущерб.

Значение информации в деятельности современных предприятий возросло настолько, что без системного управления всеми процессами получения, хранения, преобразования и передачи информации невозможно эффективное и устойчивое функционирование предприятий. В этой связи требуется, прежде всего, сместить акценты в политике управления информационными рисками. При рассмотрении информационных рисков необходимо учитывать проблемы обеспечения как безопасности информации, так и ее качества, тесно увязывая их решение с конечными целями функционирования предприятия.

Наряду с дальнейшим развитием информационных технологий следует существенно повысить уровень управления информационными процессами предприятий путем создания эффективных систем управления информационными рисками (СУИР), обеспечивающих комплексное применение механизмов управления.

1. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Рассмотрение вопросов управления информационными рисками целесообразно начать с определения или уточнения наиболее важных понятий, таких как информационная сфера и информационный риск. Понятие «информационная сфера предприятия» вводится в соответствии с методологией системного подхода. С позиций рассмотрения сущности информационных рисков предлагается выделить две системы: информационная система предприятия (внутренняя среда) и внешняя информационная среда. Объединение этих двух систем позволяет получить системный комплекс или мегасистему [2]. Такую мегасистему и предла-

гается рассматривать как информационную сферу предприятия. Информационная сфера предприятия не может быть представлена в виде системы из-за наличия иррационального взаимодействия между информационной системой предприятия и внешней средой. Понятие иррациональности вводится в работе [2], под которой понимается наличие неупорядоченности, нецелесообразности, неопознаваемости, непредсказуемости и парадоксальности во взаимодействии систем.

С позиций системного анализа информационная система предприятия представляет собой открытую систему, образуемую множеством взаимосвязанных информационных элементов, которые обеспечивают получение, обработку, хранение и передачу необходимой информации в целях эффективного функционирования предприятия. В качестве информационных элементов следует рассматривать субъекты и объекты информационных процессов. К субъектам информационных процессов относятся сотрудники предприятия, имеющие отношение к получению, обработке, хранению и передаче информации. Объектами выступают информационные ресурсы и материальные средства обеспечения информационного процесса предприятия.

Внешнюю информационную среду предприятия образуют объекты, субъекты, процессы и явления внешней среды, оказывающие влияние на элементы информационной системы предприятия и на информацию во внешней среде, имеющую отношение к предприятию, его бизнес-процессам.

На самом высоком уровне представления мегасистемы, с учетом целей исследования информационных рисков, понятие информационной сферы предприятия может быть сформулировано следующим образом. Под информационной сферой предприятия следует понимать взаимосвязанные элементы информационной системы предприятия и внешней информационной среды предприятия, а также систему регулирования отношений субъектов информационных процессов во внутренней и внешней среде предприятия. Таким образом, к информационной сфере предприятия относятся все элементы внутренней и внешней среды в их взаимодействии, имеющие отношение к получаемой, используемой, обрабатываемой, хранящейся и распространяемой информации, влияющей на бизнес-процессы предприятия, независимо от форм представления информации, видов объектов и субъектов, а также временных и пространственных рамок информационных процессов. В определении информационной сферы предприятия особо подчеркивается важность механизмов регулирования отношений субъектов информационных процессов для достижения целей бизнес-процессов.

Понятие информационного риска должно базироваться на понятии риска. Общепринятым традиционным является подход, базирующийся на понимании риска как возможной опасности, возможного убытка или неудачи [3]. В экономике под риском понимается возможное событие, в результате которого предприятие понесет убытки, а также размер возможного ущерба [4]. Реже рассматриваются спекулятивные риски, которые связывают с возможностью получения неожиданной прибыли [5]. Общепризнано также, что риски связаны с наступлением случайных событий [4, 5].

В последнее время рассматриваются и другие подходы к определению понятия «риск». Так, риск рассматривается как следствие принятого решения («риск решения»), а если причины ущерба находятся «вовне, т. е. вменяются окружающему миру», то речь может идти об опасности [6]. В работе [7] этот подход развивается, и риск трактуется как размер потерь от принятия решений. Такой подход позволяет логично определить управление рисками как управление решениями, подчеркнуть важность принятия решений.

Предложенное деление ущерба от негативных явлений на риски и опасности приводит к выводу, что в отношении опасностей не принимается управляющих решений, потому что они находятся вне сферы влияния лица, принимающего решение. Но ведь все значимые «опасности» учитываются в деятельности предприятий. Так, например, пока невозможно предотвратить землетрясение, но возможность его учитывается, и к этой опасности готовятся заблаговременно на основе принятого решения. Употребление термина «опасность» оправдано, по-видимому, по отношению к тем негативным событиям, которые ранее не происходили или по ним отсутствует какая-либо информация.

Проведенный анализ подходов к определению сущности информационных рисков с использованием дефиниции информационной сферы предприятия позволяет сформулировать понятие «информационный риск». Информационный риск — это возможность наступления случайного события в информационной сфере предприятия, в результате которого предприятию будет нанесен ущерб. Причем информационные риски рассматриваются как вероятные события во внутренней или внешней среде предприятия, оказывающие негативное влияние не только на безопасность информации, но и на ее качество; учитываются все события, которые могут произойти на всех этапах информационного процесса от получения информации до ее использования в бизнес-процессах.

Управление информационными рисками организуется в целях минимизации общей суммы ущерба от них и затрат на управление ими. Управление информационными рисками предполагает три стратегии управления, которые в различных сочетаниях могут применяться в отношении конкретных информационных рисков:

— воздействие на источники рисков для устранения причин рисковых событий;

— влияние на факторы рисков, способствующие реализации рисковых событий;

— создание условий для снижения ущерба от наступившего рискового события.

Устранение причин, порождающих отдельные риски, невозможно или неэффективно. В основном это относится к рискам, источник которых находится во внешней среде. Фактор риска характеризует уязвимость системы при воздействии этого риска. Факторы риска устраняются в основном на уровне информационной системы предприятия. Первые две стратегии применяются для предотвращения рисковых событий (существенного снижения вероятности их реализации). Третья стратегия предусматривает наличие механизмов управления, обеспечивающих минимизацию ущерба при реализации рисковых событий. Она направлена на локализацию негативного влияния риска, оперативное устранение ущерба, перехода к штатному режиму функционирования и возможную корректировку политики управления риском.

Для управления информационными рисками создается система управления, под СУИР понимается единый комплекс правовых норм, экономических и организационных мер, технических, программных и криптографических средств, а также информационных ресурсов, обеспечивающий минимальные суммарные расходы на компенсацию ущерба и затрат на управление информационными рисками.

Система управления информационными рисками входит как подсистема в информационную систему предприятия. Поэтому она должна создаваться на единых с информационной системой научно-методических принципах построения сложных человеко-машинных систем [8].

В процессе создания СУИР и ее модернизации решается задача оптимального выбора механизмов защиты от информационных рисков. Под механизмами защиты понимаются методы и средства, обеспечивающие управление информационными рисками.

2. ВЫБОР МЕХАНИЗМОВ ЗАЩИТЫ ОТ ИНФОРМАЦИОННЫХ РИСКОВ

В процессе эксплуатации информационной системы возникает необходимость совершенствования СУИР. Такая необходимость обусловливается:

— возрастанием годового ущерба от определенных информационных рисков;

— появлением новых информационных рисков;

— изменением существующих рисков;

— модернизацией информационной системы;

— изменением масштабов и сложности бизнес-процессов предприятия;

— изменениями в смежных информационных системах;

— природными явлениями;

— появлением новых правовых актов;

— изменениями в политической и экономической жизни общества.

Если по результатам анализа состояния СУИР признается необходимой ее модернизация, то следует перейти к этапу решения оптимизационной задачи выбора механизмов защиты.

Формальная постановка задачи выбора может быть представлена в следующем виде. Известно множество значимых рисков $R = \{r_1, r_2, ..., r_N\}$. Для каждого риска r_n, $n = 1, 2, ..., N$, определен ущерб в денежной форме u_{r_n}. Ущербы по всем рискам образуют множество ущербов $U = \{u_{r_1}, u_{r_2}, ..., u_{r_N}\}$. Каждый ущерб u_{r_n} определен при условии, что в отношении n-го риска не применяется никаких механизмов защиты.

Определен кортеж механизмов защиты $M = (m_1, m_2, ..., m_K)$, элементы которого могут использоваться в СУИР. Каждый k-й механизм защиты характеризуется множествами параметров R_k и E_k, а также параметром c_k. Множество $R_k = (r_{k1}, r_{k2}, ..., r_{kJ})$ составляют информационные риски, которым противодействует k-й механизм защиты.

С помощью множества показателей $E_k = (e_{k1}, e_{k2}, ..., e_{kN})$ оценивается эффективность k-го механизма защиты относительно n-го риска. Элемент e_{kn} множества показывает, какая часть ущерба от n-го информационного риска будет предотвращена при работе k-го механизма защиты. Величина e_{kn} изменяется в пределах $0 \leqslant e_{kn} < 1$. Эффективность всех механизмов защиты может характеризоваться с помощью матрицы E:

$$E = \begin{pmatrix} e_{11} & e_{12} & \dots & e_{1N} \\ e_{21} & e_{22} & \dots & e_{2N} \\ \dots & \dots & \dots & \dots \\ e_{K1} & e_{K2} & \dots & e_{KN} \end{pmatrix}.$$

На практике определенным информационным риском часто управляют с помощью нескольких механизмов. Формально это означает, что в столбцах матрицы E может быть несколько элементов, отличных от нуля. Эффективность управления риском n с применением нескольких механизмов не может определяться с помощью аддитивного показателя $\sum_{k=1}^{K} e_{kn}$, так как в этом случае суммарный показатель может равняться единице и даже ее превысить. При подсчете общей эффективности снижения ущерба от риска n, при условии включения в СУИР всех K рассматриваемых механиз-

мов, может использоваться мультипликативный показатель

$$\prod_{k=1}^{K}(1-e_{kn}) = (1-e_{1n})(1-e_{2n})...(1-e_{Kn}),$$

характеризующий общую часть ущерба от риска n, которая сохранится при включении всех K механизмов защиты.

Параметр c_k представляет собой затраты предприятия на приобретение или на изменение, разработку, создание, а также на внедрение и эксплуатацию k-го механизма. Часто руководство предприятия не может направить на совершенствование СУИР денежные средства, превышающие определенную сумму $C_{\max}$.

Известны также элементы матрицы совместимости механизмов управления информационными рисками:

$$D = \begin{pmatrix} d_{11} & d_{12} & \dots & d_{1K} \\ d_{21} & d_{22} & \dots & d_{2K} \\ \dots & \dots & \dots & \dots \\ d_{K1} & d_{K2} & \dots & d_{KK} \end{pmatrix},$$

где

$$d_{ij} = \begin{cases} 1, \text{если } i\text{-й и } j\text{-й механизмы совместимы;} \\ 0 \text{ в противном случае.} \end{cases}$$

Несовместимыми считаются механизмы, не допускающие совместного использования в одной СУИР механизмов без существенного изменения их структур. Например, не могут быть применены программные средства, разработанные для компьютерных систем с различными операционными системами.

Несовместимыми следует считать также механизмы, выполняющие одинаковые функции и совместное применение которых не приводит к повышению эффективности системы. Такие механизмы построены, как правило, на одних и тех же принципах по сходным технологиям. Например, не имеет смысла применять в одной СУИР различные системы шифрования данных, хранящихся на внешних запоминающих устройствах. В то же время программные фильтры и контроль оператором вводимой информации являются совместимыми механизмами, повышающими достоверность вводимой информации. Совместимые механизмы могут применяться интегрировано в различных сочетаниях для комплексного противодействия риску.

Множество механизмов, входящих в СУИР, задается с помощью бинарного вектора конфигурации $X = (x_1, x_2, ..., x_K)$, где

$$x_k = \begin{cases} 1, \text{если } k\text{-й механизм включен в систему;} \\ 0 \text{ в противном случае.} \end{cases}$$

Механизмы защиты $x_i, x_j \in X$ совместимы, если $x_i x_j \leqslant d_{ij}$, $i = \overline{1, K}$, $j = \overline{1, K}$.

Общий ущерб U^0, который ожидается после введения в СУИР механизмов защиты, назовем остаточным. Он определяется бинарным вектором конфигурации. С учетом введенных обозначений выражение для вычисления остаточного ущерба может быть представлено в следующем виде:

$$U^0(x_1, x_2, ..., x_K) = \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K}(1 - e_{kn}x_k).$$

Постановка задачи оптимального выбора механизмов защиты от информационных рисков может быть представлена следующим образом:

определить бинарный вектор $X^*(x_1^*, x_2^*, ..., x_K^*)$, обеспечивающий минимум суммы остаточного ущерба от всех значимых рисков и затрат на применение механизмов защиты:

$$\min\left(\sum_{k=1}^{K}(c_k x_k) + \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K}(1 - e_{kn}x_k) \right), \quad (1)$$

при

$$x_i x_j \leqslant d_{ij}, \quad i = \overline{1, K}, \quad j = \overline{1, K}, \quad (2)$$

$$\sum_{k=1}^{K}(c_k x_k) \leqslant C_{\max}. \quad (3)$$

В общем случае эффективность k-го механизма e_{kn} в отношении риска n зависит от вектора X, т. е. возможно влияние включения $k + 1$-го механизма в СУИР на эффективность k-го механизма. Эта зависимость может быть учтена при вычислении мультипликативного показателя эффективности.

Кроме того, эффективность механизмов защиты зависит, как правило, от затрат, связанных с их применением. Поэтому в альтернативной постановке задачи оптимизации определения механизмов защиты эффективность k-го механизма e_{kn} может быть представлена как функция механизма $e_{kn} = (x_1, x_2, ..., x_{k-1}, x_{k+1}, ..., x_K, c_k)$. Переход к более сложной постановке задачи оправдан, если эффективность механизмов существенно зависит от включения других механизмов в СУИР.

Задача определения механизмов защиты от информационных рисков, которые необходимо ввести в СУИР дополнительно или для замены существующих механизмов, относится к нелинейным дискретным бинарным задачам переборного типа [9]. Решение таких задач возможно методами полного перебора, ветвей и границ, динамического программирования. Точный метод ветвей и границ не применим для решения поставленной задачи, так как целевая функция не является монотонной [10]. При решении практических задач значимые информационные риски исчисляются десятками,

а число механизмов управления рисками может быть на порядок больше. При такой размерности решение задачи методом полного перебора проблематично.

Субоптимальные решения, удовлетворяющие практическим целям управления информационными рисками, могут быть получены эвристическими методами. Для решения поставленной задачи предлагается применить эвристический пошаговый метод. Его достоинство заключается в сочетании локальной оптимизации на каждом шаге с учетом влияния принимаемых решений на конечный результат, что позволяет повысить точность решения. При этом существенно снижается вычислительная сложность по сравнению с методом полного перебора. Время реализации алгоритма полиномиально зависит от числа переменных в отличие от зависимости, близкой к экспоненциальной, при полном переборе.

Сущность метода заключается в выборе на каждом шаге одного из возможных механизмов, обеспечивающего получение максимального эффекта. Эффект определяется размером снижения расходов на управление рисками (суммой затрат собственно на управление рисками и размера ущерба) в результате применения очередного механизма и упущенной выгодой от невозможности применения на последующих шагах механизмов, несовместимых с включаемым в систему очередным механизмом. Таким образом, на каждом шаге анализируется не только локальный эффект от включения в систему механизма, но и рассматриваются последствия этого шага в дальнейшей работе алгоритма, в которой учитываются ограничения на расходы, связанные с применением механизмов защиты от информационных рисков.

Для формального представления алгоритма вводятся следующие обозначения: h — номер выполненного шага алгоритма; $X_h(x_{h1}, x_{h2}, ..., x_{hK})$ — состояние вектора конфигурации после h-го шага; $W(h)$ — множество механизмов, включенных в число применяемых на h-м шаге; $S(h)$ — множество механизмов еще не включенных в число применяемых на h-м шаге, но совместимых с механизмами множества $W(h)$; $\Omega(h)$ — множество механизмов, несовместимых с множеством $W(h)$, т. е. исключаемых из дальнейшего рассмотрения; $U_n^0(h)$— остаточный ущерб от n-го риска после выбора механизмов на первых h шагах.

Таким образом, значения $x_{hk} = 1$ соответствуют механизмам, уже отобранным на первых h шагах алгоритма, т. е. входящим во множество $W(h)$.

Пусть $m_{h+1} \in S(h)$ — механизм, выбираемый на h+1-м шаге из множества $S(h)$. Выбор механизма m_{h+1} означает, что соответствующая компонента вектора $X_h(x_{h1}, x_{h2}, ..., x_{hK})$ становится равной единице. Предположим, что выбранному механизму m_{h+1} в векторе X_h соответствует компонента с номером k.

Тогда величина, на которую уменьшится ущерб от n-го риска при выборе на шаге $h + 1$ механизма m_{h+1} с номером k, равна $\Delta U_n(h + 1, k)$ и определяется следующим образом: $\Delta U_n(h + 1, k) = U_n^0(h)e_{kn}$. Оставшаяся величина ущерба от n-го риска $U_n^0(h + 1, k) = U_n^0(h)(1 - e_{kn})$.

Суммарное уменьшение ущербов от рисков всех видов при выборе на $h + 1$-м шаге k-го механизма

$$\Delta U(h + 1, k) = \sum_{n=1}^{N} \Delta U_n(h + 1, k) = \sum_{n=1}^{N} U_n^0(h)e_{kn}.$$

Упускаемая возможность снижения ущербов на последующих шагах алгоритма $\Delta U_\tau^-(h + 1, k)$ обусловлена исключением применения на следующих шагах механизма τ, несовместимого с механизмом k ($\tau \in \Omega(h)$), и вычисляется как

$$\Delta U_\tau^-(h + 1, k) = \sum_{n=1}^{N} U_n^0(h)(1 - e_{kn})e_{\tau n}\bar{d}_{k\tau}s_{h\tau},$$

где $\bar{d}_{k\tau}$ — инверсное значение $d_{k\tau}$ из матрицы совместимости D (если $d_{k\tau} = 1$, то $\bar{d}_{k\tau} = 0$ и наоборот); множитель $s_{h\tau} = 1$, если $\tau \in S(h)$ и $s_{h\tau} = 0$ в противном случае.

Присутствие множителя $s_{h\tau}$ в этом выражении позволяет учитывать на шаге $h + 1$ механизм τ, который стал несовместным только на шаге $h + 1$ в результате включения механизма k. Величина $U_n^0(h)(1 - e_{kn})$есть остаточный ущерб от n-го риска после применения механизма k на шаге $h + 1$;

Суммарная упускаемая возможность снижения ущербов, в случае выбора на $h + 1$-м шаге k-го механизма из-за исключения несовместимых с ним механизмов,

$$\Delta U^-(h + 1, k) = \sum_{\tau=1}^{K}\sum_{n=1}^{N} U_n^0(h)(1 - e_{kn})e_{\tau n}\bar{d}_{k\tau}s_{h\tau}.$$

Для оценки эффекта от включения на шаге $h + 1$ k-го механизма защиты введем величину $Э(h + 1, k)$:

$$Э(h + 1, k) = \Delta U(h + 1, k) - (\Delta U^-(h + 1, k) + c_k).$$

Эффект от включения механизма k в СУИР определяется как разность суммы прямого уменьшения ущербов от всех видов рисков и суммы затрат на управление k-м информационным риском и размера упущенного уменьшения ущербов в дальнейшем.

Вместо эффекта удобнее пользоваться безразмерной величиной — удельным эффектом $Э_y(h + 1, k) = Э(h + 1, k)/C_{max}$.

В соответствии с введенными обозначениями эвристический алгоритм состоит из следующих шагов. На каждом шаге h для $m \in S(h)$ вычисляется $Э_y(h + 1, k)$ и выбирается такой механизм m^* с номером k^*, для которого удельный эффект $Э_y(h + 1, k^*)$ имеет наибольшее значение и при этом не исчерпываются выделенные средства, т. е. выполняется условие (3). Если такого механизма нет, то работа алгоритма прекращается и в качестве оптимального принимается вектор $X^*(x_1^*, x_2^*, ..., x_K^*)$.

Проверка эвристического метода показала, что его точность зависит от размерности задачи. При малом числе рисков около 90 % реализаций дают решение, полностью соответствующее результатам, полученным полным перебором. Отклонения результатов эвристического метода на случайных наборах исходных данных возрастают с увеличением размерности задачи. Это объясняется тем, что в расчет принимаются упускаемые возможности снижения ущербов из-за невозможности использования всех несовместных механизмов на каждом шаге. Причем учитывается влияние и тех механизмов, которые по окончания работы алгоритма не войдут в число оптимальных. Точность алгоритма может быть повышена путем изменения порядка вычисления общей упускаемой возможности снижения ущерба. На каждом шаге целесообразно рассматривать эффект снижения ущерба только от нескольких наиболее эффективных механизмов, вероятность включения которых в альтернативных вариантах высока.

На рынке механизмов управления информационными рисками часто предлагаются готовые подсистемы, включающие в свой состав комплекс механизмов защиты, которые называются агрегированными. Наличие комплексных механизмов в СУИР и возможность применения таких механизмов для ее совершенствования придает особенности процессу оптимизации системы.

Пусть для создания СУИР может быть применено множество комплексных механизмов $KM = (km_1, km_2, ..., km_L)$, а также множество отдельных автономных механизмов $M = (m_1, m_2, ..., m_K)$. Часть автономных механизмов может входить в состав комплексных механизмов защиты.

Предположим, что эффективность автономных механизмов при включении их в состав комплексных механизмов не изменяется. Тогда задача оптимального выбора механизмов защиты от информационных рисков, с учетом ранее введенных обозначений, может быть формально представлена следующим образом.

Определить общий бинарный вектор конфигурации автономных и комплексных механизмов $X_0^*(x_1^*, x_2^*, ..., x_K^*, x_{K+1}^*, x_{K+2}^*, ..., x_{K+L}^*)$, обеспечивающий минимум целевой функции

$$\sum_{k=1}^{K+L} c_k x_k + \sum_{n=1}^{N} \left(u_n \prod_{k=1}^{K+J} (1 - e_{kn} x_k) \right),$$

при

$$x_i x_j \leqslant d_{ij}, \quad i = \overline{1, K+L}, \quad j = \overline{1, K+L};$$

$$\sum_{k=1}^{K+L} (c_k x_k) \leqslant C_{max}.$$

Для решения задачи могут быть применены те же методы, что и для решения задачи (1)—(3). Вычислительная сложность алгоритмов при этом возрастает, так как размерность вектора X_0 больше размерности вектора X.

ЗАКЛЮЧЕНИЕ

Значимость проблемы управления информационными рисками требует перехода от управления безопасностью информации к системному управлению информационной сферой предприятия. Управление информационной сферой предприятия организуется с помощью системы управления информационными рисками, в процессе модернизации которой осуществляется выбор механизмов защиты от информационных рисков. Один из возможных подходов к решению этой задачи представлен в настоящей работе.

ЛИТЕРАТУРА

1. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2004. 384 с.
2. *Прангишвили И.В.* Системный подход и общесистемные закономерности. — М.: СИНТЕГ, 2000. — 528 с.
3. *Ефремова Т.Ф.* Новый словарь русского языка. Толково-словообразовательный. Т. 1. — М.: Русский язык, 2000. — 1233 с.
4. *Найт Ф.Х.* Риск, неопределенность и прибыль. — М.: Дело, 2003. — 360 с.
5. *Балабанов И.Т.* Риск-менеджмент. — М.: Финансы и статистика, 1996. — 192 с.
6. *Луман Н.* Понятие риска // THESIS. — 1994. — № 5. — С. 135—160.
7. *Управление* риском: Риск. Устойчивое развитие. Синергетика. — М.: Наука, 2000. — 431 с.
8. *Молчанов А.А.* Моделирование и проектирование сложных систем. — Киев: Выща школа, 1988. — 359 с.
9. *Гэри М., Джонсон Д.* Вычислительные машины и трудноразрешаемые задачи. — М.: Мир, 1982. — 416 с.
10. *Кузнецов О.П., Адельсон-Вельский Г.М.* Дискретная математика для инженера. — М.: Энергоатомиздат, 1988. — 480 с.

Статья представлена к публикации членом редколлегии В.В. Кульбой.

Завгородний Виктор Иванович — канд. техн. наук, доцент, Федеральное государственное образовательное учреждение высшего профессионального образования Финансовая академия при Правительстве Российской Федерации, e-mail: zvi@rambler.ru .