На правах рукописи

КУСТОВ Георгий Алексеевич

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ОРГАНИЗАЦИИ НА ОСНОВЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА

(на примере компании добровольного медицинского страхования)

Специальность: 05.13.19 – Методы и системы защиты информации,

информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа 2008

Работа выполнена
на кафедре вычислительной техники и защиты информации
Уфимского государственного авиационного технического университета

Научный руководитель — д-р техн. наук, проф.
Васильев Владимир Иванович

Официальные оппоненты — д-р техн. наук, проф.
Мельников Андрей Витальевич

канд. техн. наук
Погорелов Дмитрий Николаевич

Ведущая организация — ГОУ ВПО **«Самарский государственный университет»**

Защита диссертации состоится 17 декабря 2008 в 10:00
на заседании диссертационного совета Д-212.288.07
при Уфимском государственном авиационном техническом университете
по адресу: 450000, Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «___» ноября 2008 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. **С.С. Валеев**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В связи с принятием Федерального закона «О персональных данных» и реализацией законов «Об информации, информационных технологиях и защите информации» и «О медицинском страховании граждан в Российской Федерации» возросла значимость эффективного управления рисками информационных систем персональных данных. В настоящее время нерешенными остаются многие задачи правового, технического и финансового регулирования в медицинских информационных системах, содержащих конфиденциальные данные. Остаются открытыми вопросы обеспечения гарантированного доступа к информации, защиты врачебной тайны, обмена информацией с «третьими лицами» (со страховыми компаниями), оценки величины выплат, компенсирующих моральный вред, вследствие утечки конфиденциальной информации. По классификации категорий персональных данных, предложенной Федеральной службой по техническому и экспортному контролю (ФСТЭК), данные о состоянии здоровья граждан относятся к самой важной – первой категории, а информационные системы (ИС) компаний добровольного медицинского страхования относятся к классу ИС, для которых нарушение безопасности обрабатываемых персональных данных может привести к значительным негативным последствиям для субъектов персональных данных.

Согласно данным отчетов аудиторской компании Perimetrix только 5% российских организаций не пострадали от утечек данных в 2007 г. Как отмечается в исследовании «Инсайдерские угрозы в России 2008», чаще всего похищаются персональные данные (57%), детали конкретных сделок (47%) и финансовые отчеты (38%).

Целью деятельности страховой компании (СК) является получение прибыли от проведения эффективной политики в области страхования и инвестирования. Деятельность страховой компании сосредоточена на решении вопросов управления техническими, нетехническими и инвестиционными рисками. Информационные риски (ИР) являются важной составляющей группы нетехнических рисков. При управлении СК роль информационных рисков значительна. Поэтому исследования, направленные на решение задач, связанных с анализом, оценкой информационных рисков в страховой компании добровольного медицинского страхования (СК ДМС) и выбором эффективных контрмер по их снижению являются актуальными.

Объект и предмет исследования. Объектом диссертационного исследования является информационная система СК ДМС. Предметом исследования является математическое и программное обеспечение управления информационными рисками страховой компании.

Целью диссертационной работы является снижение информационных рисков компании добровольного медицинского страхования на основе разрабатываемых моделей, методов и методик анализа и управления рисками информационной системы.

Для достижения этой цели в диссертации поставлены и решены следующие задачи:

1. Формирование структуры системы управления информационными рисками СК ДМС на основе логико-вероятностного метода (ЛВМ).
2. Разработка моделей количественной оценки информационных рисков и анализа качества решений, принимаемых на их основе.
3. Разработка метода оценки компенсации морального ущерба в случае нарушения конфиденциальности информации.
4. Разработка метода формирования наиболее эффективного набора контрмер для планирования бюджета информационной безопасности.
5. Разработка методики страхования информационных рисков на примере информационной системы конкретной СК ДМС.

Методы исследования. При решении поставленных в работе задач использовались основные положения методологии структурного анализа и проектирования, системного анализа, теории вероятностей и математической статистики, теории принятия решений, методов экспертных оценок.

На защиту выносятся:

1. Структура системы управления информационными рисками СК ДМС.
2. Модели идентификации и количественной оценки информационных рисков.
3. Метод оценки морального ущерба в случае нарушения конфиденциальности информации.
4. Метод оценки и выбора наиболее эффективных контрмер.
5. Методика начисления брутто-премии при страховании информационных рисков.
6. Программное обеспечение системы управления информационными рисками организации.

Научная новизна работы состоит в следующем:

1. Предложена новая структура системы управления информационными рисками, основанная на использовании ЛВМ для идентификации и количественной оценки рисков в информационных системах, отличающаяся использованием различной степени детализации сценариев опасных состояний ИС в зависимости от их значимости и позволяющая повысить достоверность оценки информационных рисков.
2. Разработана функциональная модель процесса управления информационными рисками, основанная на применении SADT методологии, использование которой позволяет обоснованно выбрать состав и функции основных этапов анализа и управления рисками организации.
3. Поставлена и решена задача определения структуры ущерба компании при нарушении конфиденциальности. Предложен метод оценки компенсации морального ущерба в случае нарушения конфиденциальности, основанный на модификации метода предпочтений и замещений, который отличается использованием балльных оценок и позволяет оценить вклад морального ущерба в структуру информационных рисков.

4. Предложен новый метод формирования эффективного набора контрмер на основе ЛВМ с использованием иерархического перебора, отличающийся учетом влияния контрмер на инициирующие события и позволяющий определить оптимальный набор контрмер при заданных бюджетных ограничениях.
5. Разработана методика страхования информационных рисков, основанная на применении предложенных моделей и методов анализа и управления рисками, что позволяет дать обоснованные рекомендации для выбора объектов страхования и размеру страховой суммы и премии.

Практическая значимость и внедрение результатов. Предложенные модели и методы позволяют снизить на 58–67 % информационные риски СК ДМС при заданных бюджетах информационной безопасности и могут использоваться на практике при идентификации, анализе, оценке информационных рисков, формировании набора контрмер и начислении страховой премии в практике страхования информационных рисков.

Разработанное программное обеспечение «Система управления информационными рисками на основе логико-вероятностного метода» внедрено в страховой компании ООО «МСК «УралСиб»», Уфимском филиале СК ООО «Росгосстрах-Аккорд» и в Уфимском филиале Центрального коммерческого банка.

Апробация работы

Основные положения, представленные в диссертационной работе, докладывались на следующих конференциях:

-VIII-ой научной конференции студентов и аспирантов – КРЭС 2006. Томск, ТУСУР, 2006 г.;

-II-ой республиканской научно-практической конференции «Актуальные вопросы современной медицины и здравоохранения», Уфа, БГМУ, 2006;

-XI-ой международной научно-технической конференции «Системный анализ в проектировании и управлении», СПб, Политехнический университет, 2007;

-IX-ой Международной научной конференциях «Компьютерные науки и информационные технологии» (CSIT 2007), Уфа, 2007;

-III Всероссийской зимней школе – семинаре аспирантов и молодых ученых, Уфа, 2008.

Публикации

Результаты диссертационной работы отражены в 12 публикациях, в том числе в 2-х статьях из перечня ВАК Рособрнадзора. Получено свидетельство Федеральной службы по интеллектуальной собственности, патентам и товарным знакам № 2008612183 о государственной регистрации программы для ЭВМ «Система управления информационными рисками на основе логико-вероятностного метода».

Структура работы. Диссертационная работа состоит из введения, 4-х глав, заключения, списка литературы, включающего 89 наименований, приложений. Содержание работы изложено на 152 страницах.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность исследований в области управления рисками информационной безопасности. Формулируются цель работы и задачи исследований, научная новизна и практическая ценность выносимых на защиту результатов.

Первая глава посвящена обзору и сравнительному анализу методов управления информационными рисками (ИР).

Рассматривается общий подход к управлению рисками в страховой компании добровольного медицинского страхования. На основе Европейского страхового законодательства выделяется группа нетехнических рисков – рисков, не связанных со страховой деятельностью. На *информационные риски* (рис. 1), входящие в эту группу, приходится до трети от интегрального риска организации.

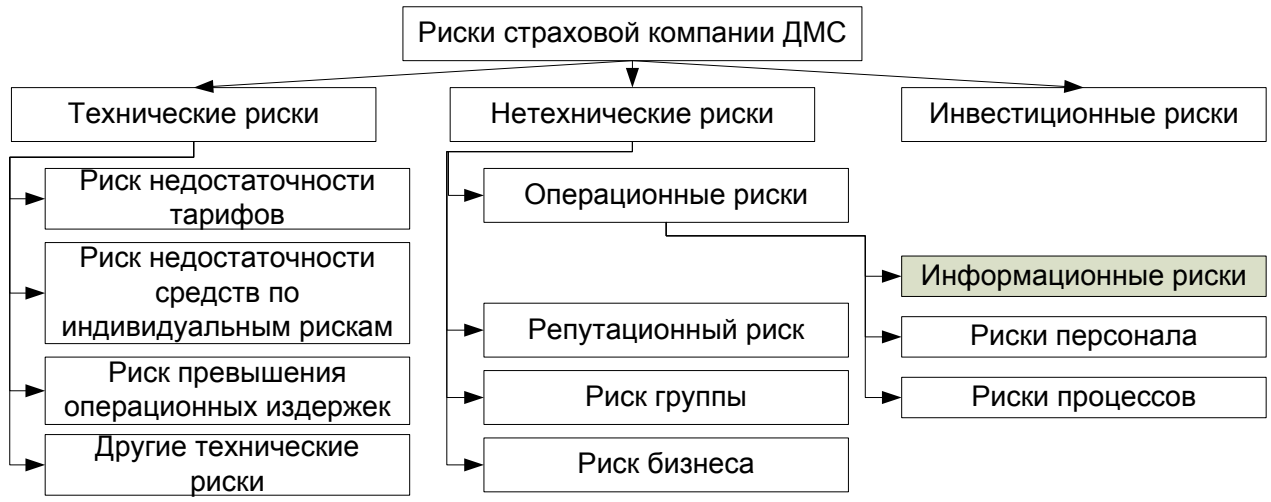

Рисунок 1 – Риски страховой компании ДМС

Отмечается, что формально решение задачи управления информационными рисками (если говорить о снижении риска) может быть сведено к выполнению следующих этапов:

1. Идентификация ресурсов информационной системы страховой компании.
2. Идентификация и анализ угроз, действующих на эти ресурсы.
3. Анализ и оценка уровня информационных рисков для каждого ресурса и информационной системы в целом.
4. Управление риском - выбор мер для снижения информационных рисков (контрмер) и анализ эффективности управления.

Производится обзор известных методик выполнения каждого из этапов риск-менеджмента. Анализируются известные подходы к оценке различных видов потенциального ущерба, а также существующие методики измерения рисков.

Законодательная база рассматривается как фундамент эффективного управления информационными рисками.

Проанализированы известные подходы к управлению ИР; в качестве эффективного способа управления рассматривается страхование ИР. С одной сто-

роны, это эффективная контрмера, с другой – способ передачи управления риском другой компании. Приведена классификация объектов страхования, виды и этапы страхования, способы определения страховых премий.

Дан обзор программных средств анализа и управления рисками, представленных двумя классами – ПО базового уровня и ПО полного анализа рисков. Среди известных реализаций – Cobra, CRAMM, Risk Advisor, Risk Watch, система управления информационной безопасностью «АванГард», ГРИФ 2006, КОНДОР 2006.

Формулируются цель и задачи исследований диссертационной работы.

Во второй главе предложен подход к анализу, оценке и управлению информационными рисками, основанный на применении логико-вероятностного метода. Основные этапы управления риском, задачи и методы, решаемые на каждом из этапов, представлены в таблице 1.

Задачи и методы исследования на этапах управления риском Таблица 1

Название этапа	**Задачи**	**Подход к решению**
Идентификация ресурсов ИС и угроз	1.Определение структуры информационных рисков СК.	На основе ЛВМ
Анализ и оценка риска ресурсов и всей системы	2.Выбор наиболее значимых опасных состояний ИС. 3.Оценка интегрального риска информационной системы СК: 3.1.Оценка вероятности реализации опасного состояния ресурса ИС; 3.2.Оценка ущерба при реализации опасного состояния ресурса ИС: 3.2.1.Оценка структуры ущерба при утечке конфиденциальной информации; 3.2.2.Определение размера компенсации морального ущерба.	На основе карт рисков или алгоритма Мамдани На основе ЛВМ Методика разработана в диссертации Модифицированный метод предпочтений и замещений
Управление риском	4.Формирование наиболее эффективного набора контрмер. 5.Оценка уровня риска ИС с учетом контрмер и оценка эффективности решения задачи управления информационными рисками 6.Определение премий при страховании информационных рисков.	Метод разработан в диссертации На основе ЛВМ и модификации методики Росс-госстрахнадзора

Данные подходы к решению задачи управления рисками реализованы в системе управления информационными рисками на основе логико-вероятностного метода (СУИР ЛВМ). Первый уровень функциональной модели системы представлен на рисунке 2.

Задача 1. Определение структуры информационных рисков ИС

ИС представляет собой совокупность ресурсов: программных, аппаратных, каналов связи и ресурсов данных. Отказ какого-либо из ресурсов приводит

к невозможности выполнения компанией одной или нескольких своих функций.

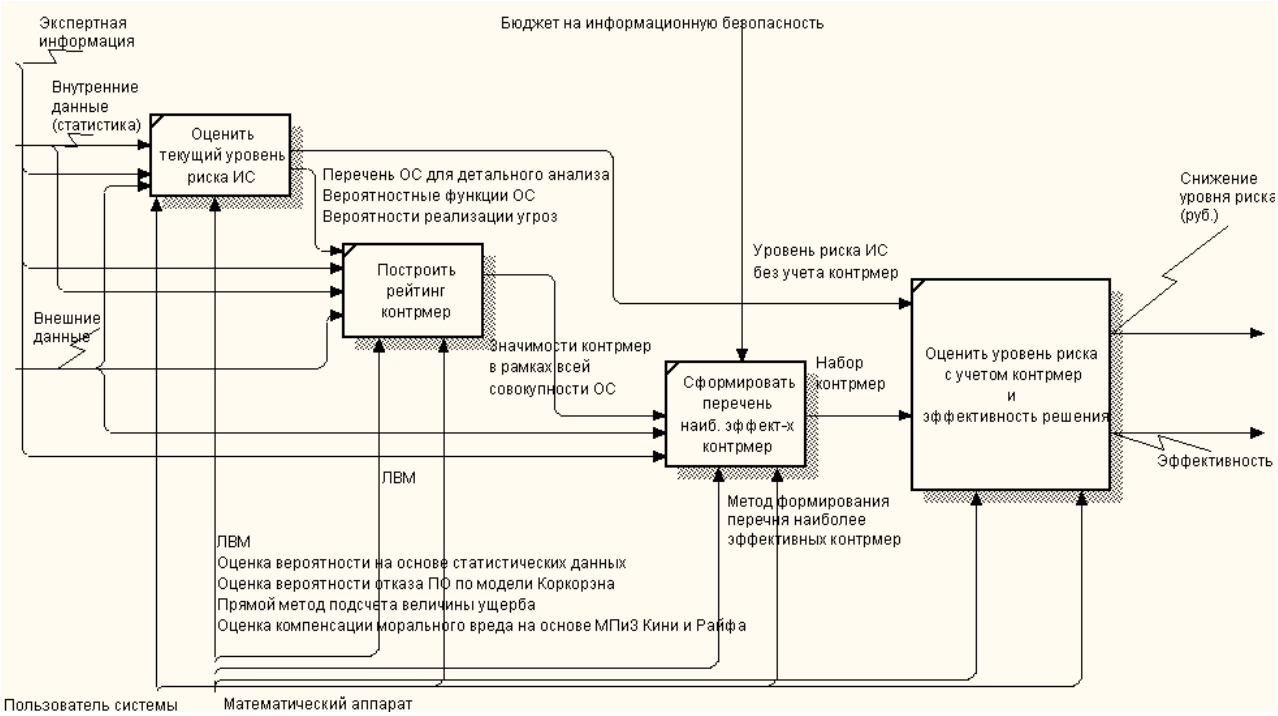

Рисунок 2 – Функциональная модель системы

Под *риском системы* рассматривается сумма рисков ресурсов, из которых состоит система:

$$R = \sum_{i=1}^{n} R_i \,, \qquad (1)$$

где R_i – риск i-го ресурса, n – количество ресурсов. С каждым ресурсом связано множество опасных состояний (ОС), реализация которых приводит к отказу, нарушению конфиденциальности, доступности или целостности данного ресурса.

Под *риском i-го ресурса* понимается сумма рисков, связанных с реализацией опасных состояний данного ресурса:

$$R_i = \sum_{j=1}^{M_i} r_{ij} \,, \qquad (2)$$

где r_{ij} – риск реализации j-го опасного состояния i-го ресурса, $j = \overline{1, M_i}$; M_i – количество опасных состояний i-го ресурса.

Под *риском реализации j-го опасного состояния i-го ресурса* понимается произведение вероятности P_{ij} и стоимости потерь C_{ij} от реализации данного опасного состояния ресурса:

$$r_{ij} = P_{ij} * C_{ij} \,. \qquad (3)$$

Таким образом, идентификация рисков ИС представлена:

1) описанием структуры ресурсов ИС;
2) описанием множества опасных состояний ресурсов ИС;
3) описанием множества угроз инициирующих ОС.

Задача 2. Выбор наиболее значимых опасных состояний ИС

Для ОС системы, идентифицированных на предыдущем этапе, классификация опасных состояний по группам значимости рисков производится на основе карты рисков или алгоритма нечеткой логики Мамдани. Предварительный анализ ИР осуществляется по двухфакторной методике – формула (3).

Согласно данной классификации производится выбор способа управления, который зависит от двух параметров: размера ущерба и вероятности реализации ОС в течение года. Малые риски не требуют внимания андеррайтеров, т.е. управление рисков сводится к их *игнорированию, отказу от управления*. Катастрофические риски и высокие риски с малой частотой принято страховать, т.е. осуществлять *передачу управления риском*. Если ресурс подвержен высоким и частым рискам, то его лучше просто заменить – *отказ от ресурса*. Остальные риски требуют анализа, определенной степени детализации при оценке; управление ими сводится к осуществлению превентивных мер по *снижению риска*.

В работе рассматривается более детально один из способов управления информационными рисками, а именно – *метод снижения частоты ущерба или предотвращения убытка.* Для группы рисков средней значимости используются результаты предварительной оценки, для ОС высокой значимости производится детализированный расчет вероятности на основе ЛВМ и построенных сценариев реализации ОС.

Задача 3.Оценка интегрального риска информационной системы

Оценка вероятности реализации опасного состояния ресурса ИС

Дано:

1. Ресурс с номером i, для которого выделены опасные состояния S_{ij}, $j=\overline{1,m}$, где m – число возможных состояний.
2. Структура ОС и вероятности инициирующих событий (угроз) x_k, $k=\overline{1,h}$.

Требуется найти:

1. Вероятности P_{ij} реализации опасных состояний *i-го* ресурса S_{ij}, $j=\overline{1,m}$.
2. Значимости $Z(x_k)$ каждого инициирующего условия или события x_k с учетом его вклада в реализацию опасного состояния S_{ij}; k – номер инициирующего события или угрозы $k=\overline{1,h}$.

Алгоритм решения

Шаг 1. Составление сценария опасного состояния S_{ij}.

Шаг 2. Построение функции алгебры логики (ФАЛ) $f(x_1,...,x_h)$ с использованием операций конъюнкции и дизъюнкции на основе сценария опасного состояния S_{ij}.

Шаг 3. Построение вероятностной функции (ВФ) $P_{ij}\{f(x_1,...,x_h)=1\}$ на основе функции алгебры логики.

Шаг 4. Расчет вероятности P_{ij} реализации опасного состояния с помощью вероятностной функции.

Шаг 5. Расчет значимости $Z(x_k)$ каждой угрозы с учетом ее вклада в реализацию опасного состояния.

Значимость элемента (угрозы) определяется на вероятностной модели как частная производная ВФ:

$$Z(x_k) = \frac{\partial P}{\partial P_k} = P\{\Delta_{xk} f(x_1,...,x_h) = 1\}. \quad (4)$$

Если задача решается для нескольких ОС, то под значимостью k-ой угрозы для данного ОС понимается величина

$$\overline{Z}(x_k) = Z(x_k) * s_k = \frac{\partial P}{\partial P_k} * s_k = \frac{\partial r}{\partial P_k}, \quad (5)$$

где s_k – величина ущерба в случае реализации ОС; r – величина ущерба для данного ОС.

Оценки вероятностей отказов аппаратных ресурсов и программного обеспечения – статистически достоверные данные исследуемых ИС. При вычислении рисков таких ресурсов, как программное обеспечение, предлагается воспользоваться аналитическими моделями надежности, в частности моделью Коркорена.

Оценка ущерба при реализации опасного состояния ресурса ИС

В работе приведены варианты оценки ущерба для различных ОС:

- для физического ресурса: невосстанавливаемый и восстанавливаемый аппаратный отказ;
- для информационного ресурса: потеря ресурса, временная недоступность ресурса, сочетание потери ресурса и отсутствия резервной копии ресурса, нарушение конфиденциальности ресурса;
- для программного ресурса: сбой, отказ, несанкционированный доступ;
- для информационного канала: временная недоступность.

Для подсчета ущерба используются известные подходы, такие, как прямой счет, и оценка пороговых значений риска.

Для *i-го* риска размер случайного ущерба U_i изменяется в пределах

$$a_i \le U_i \le b_i, \quad (6)$$

где a_i и b_i – соответственно минимальный и максимальный возможный ущерб по *i-му* риску. Тогда размер общего (суммарного) случайного ущерба изменяется в пределах

$$\sum_{i=1}^{n} a_i \le U \le \sum_{i=1}^{n} b_i = B, \quad (7)$$

где n – число оцениваемых рисков.

Общий ожидаемый ущерб EU определяется по формуле:

$$EU = \sum_{i=1}^{n} EU_i \quad (8)$$

где EU – математическое ожидание общего ущерба; EU_i - математическое ожидание ущерба по *i-му* риску. В зависимости от типа опасного состояния предлагается несколько вариантов оценки стоимости потерь.

Оценка структуры ущерба при утечке информации

Описана структура ущерба при нарушении конфиденциальности ресурса. Выделены убытки: *прямые* – восстановление информации, уведомление пострадавших, создание call-центра, судебное расследование, почтовые услуги, услуги консультантов, аудиторов, создание служб для общения с прессой; *косвенные* – это потеря инвесторов, партнеров, клиентов, снижение конкурентоспособности, моральный ущерб пострадавших; *упущенная прибыль*– это снижение привлекательности марки, репутационные издержки.

Определение размера компенсации морального ущерба

Данная задача рассматривается как многокритериальная на основе модификации метода предпочтений и замещений. Новым является использование статистических данных и балльных оценок для построения одномерных функций ценности и использование значения многомерной функции ценностей для выявления доли выплат.

В данной задаче рассматриваются только денежные компенсации. Поэтому предполагается, что если максимальная сумма выплат равна S_{max}, то, в зависимости от конкретной ситуации, выплаты есть доля S_{max}.

Дано:

- максимальная сумма выплат – S_{max};
- критерии, по которым возможна оценка ситуаций;
- шкалы, экспертные данные для построения одномерных функций ценности.

Требуется построить:

- многомерную функцию ценности, предусматривающую оценку любой ситуации выплат.

Найти: реальную сумму выплаты.

Основные этапы алгоритма построения многомерной функции ценности с помощью метода предпочтений и замещений представлены в диссертации.

Таким образом, этап анализа и оценки риска ИС представляется как:

1) классификация ОС по группам значимости;
2) оценка вероятностей ОС ресурсов ИС, в том числе выявление меры влияния угроз на реализацию опасных состояний;
3) оценка стоимости потерь от реализации опасных состояний.

Задача 4. Формирование перечня наиболее эффективных контрмер ИС

Пронумеруем угрозы, отобранные для дальнейшего рассмотрения опасных состояний заново. Для этого введем новый индекс $v = \overline{1,V}$, учитывающий каждую из угроз для каждого опасного состояния каждого ресурса ИС. При введении нового индекса учитывается тот факт, что одна и та же угроза может встречаться в нескольких опасных состояниях. В этом случае под значимостью угрозы понимается сумма значимостей этой угрозы в различных опасных состояниях. Конечная цель – уменьшение уровня риска ИС посредством реализации набора контрмер $\{g_t\}$, $t = \overline{1,T}$. Для контрмеры известна стоимость ее реализации s_t, также задана величина s_0 – бюджет, выделенный на обеспечение информационной безопасности организации.

Вариант 1

Дано: матрица $\|a_{tv}\|$, где $t=\overline{1,T}$, $v=\overline{1,V}$, $a_{tv}\in\{0,1\}$,

a_{tv}=1, если контрмера g_t влияет на угрозу x_v, иначе a_{tv}=0;

z_v – значимость угрозы x_v;

s_t – стоимость контрмеры t; s_0 – бюджет ИБ на контрмеры.

Требуется найти: бинарный вектор $(b_1, b_2, \ldots, b_T)^{\mathrm{T}}$, $b_t\in\{0,1\}$, такой, что:

$$\sum_{t=1}^{T}\left(\sum_{v=1}^{V} z_v a_{tv}\right)b_t \to \max \qquad \text{при} \sum_{t=1}^{T} s_t b_t \le s_0. \tag{9}$$

Вариант 2

Дано: матрица $\|\Delta p_v^t\|$, где $t=\overline{1,T}$, $v=\overline{1,V}$, Δp_v^t – изменение вероятности реализации угрозы с номером v при попадании контрмеры с номером t в перечень контрмер для реализации или *0*, если контрмера с номером t не оказывает влияния на угрозу с номером v.

Требуется найти: бинарный вектор $(b_1, b_2, \ldots, b_T)^{\mathrm{T}}$, которому соответствует максимальное изменение интегрального риска системы $\Delta R\to\max$ согласно формулам (1)–(3) такого, что:

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}\Delta P_{ij} * C_{ij}\right)\to\max \qquad \text{при} \quad \sum_{t=1}^{T} s_t b_t \le s_0,\ b_t\in\{0,1\},\ t=\overline{1,T},\ v=\overline{1,V}. \tag{10}$$

Для обоих вариантов метода определения эффективного набора контрмер будет использоваться направленный перебор на множестве бинарных векторов длины T при упорядочивании стоимости контрмер по убыванию.

Замечание. В варианте 2 для решения задачи необходимо знать Δp_v^t для всех контрмер, в том числе и для тех, которые не войдут в перечень контрмер для реализации, что требует дополнительных временных затрат.

Задача 5. Оценка уровня риска ИС с учетом контрмер и оценка эффективности решения задачи управления информационными рисками

Пусть уровень риска ИС с учетом выбранных для реализации контрмер равен $\overline{R}$, S_0 – бюджет ИБ на контрмеры. Тогда эффективность *Ef*, выбранных для реализации контрмер, определяется формулой:

$$Ef = \frac{R-\overline{R}-S_0}{R} * 100\% \tag{11}$$

Задача 6. Определение страховых премий при страховании информационных рисков

Управление риском для определенных выше групп рисков может осуществляться страхованием ресурсов информационной системы.

Пусть ΔR – величина снижения среднего риска:

$$\Delta R = p*S - B, \tag{12}$$

где S – страховая сумма; B – размер страховой премии.

В том случае, если страхование массовое, используется модифицированная методика имущественного страхования Росгосстрахнадзора. Брутто–премия в расчете на S руб. страховой суммы:

$$B = \frac{S * p * (1 + 1{,}2\alpha(\gamma)\sqrt{\frac{1-p}{np}})}{1-h}, \qquad (13)$$

где S – страховая сумма по конкретному договору страхования;
p – вероятность наступления страхового случая по конкретному договору страхования;
α(γ) - значение коэффициента гарантии безопасности, соответствующее принятому уровню доверительной вероятности;
h – страховая нагрузка компании;
n – предполагаемое количество договоров, отнесенных к периоду страхования.

Отличия от методики расчета тарифных ставок по рисковым видам страхования Росгосстрахнадзора:

1. Индивидуальный подход к определению брутто-премии без использования андеррайтингового коэффициента.
2. Необходимость применения специальных методов для определения индивидуальных характеристик страхуемого объекта.
3. Отсутствие входных данных, использующих статистику выплат и премий прошлых периодов.

При индивидуальном страховании страховая сумма определяется как сумма, близкая к потенциальному ущербу, а страховая премия - как величина риска рассматриваемого ресурса.

В третьей главе решается задача оценки информационных рисков департамента ДМС страховой компании. Описывается структура информационной системы, формируется набор наиболее значимых опасных состояний ресурсов.

В результате проведенного анализа выделены четыре группы ресурсов: информационные ресурсы (7 ед.), сервисы (3 ед.), физические ресурсы (16 ед.), программное обеспечение (9 ед.). «Уровни значимости» опасных состояний ресурсов ИС СК ДМС, оцененные по алгоритму нечеткой логики Мамдани, представлены в диссертационном исследовании. По пороговой величине значимости опасных состояний или карте рисков, получен набор опасных состояний группы «Высокой значимости» для дальнейшего анализа с помощью логико-вероятностного метода. Аналогичные расчеты по управлению рисками для информационной системы коммерческого банка представлены в приложении 1.

Пример оценки риска реализации опасного состояния «Нарушение конфиденциальности базы данных системы аналитической поддержки данных страховой компании (БД САПД СК)» на основе логико-вероятностного метода представлен ниже поэтапно.

Шаг 1. Составление сценариев опасных состояний ресурсов.

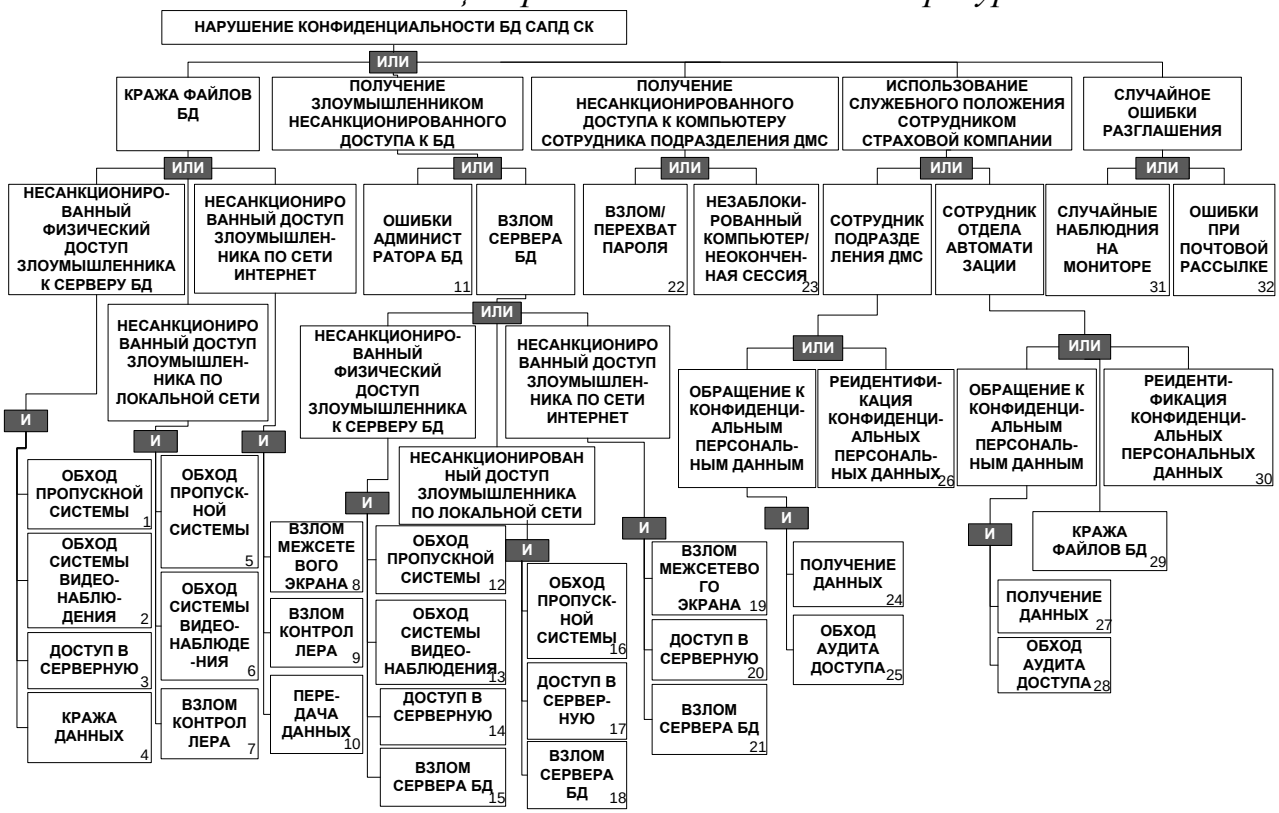

Рисунок 3 – Сценарий ОС «Нарушение конфиденциальности БД САПД СК»

Шаг 2. Построение функции алгебры логики.

Согласно описанному сценарию, логическая функция принимает вид:

$$F=X_1X_2X_3X_4 \cup X_5X_6X_7 \cup X_8X_9X_{10} \cup X_{11} \cup X_{12}X_{13}X_{14}X_{15} \cup X_{12}X_{13}X_{14}X_{15} \cup X_{16}X_{17}X_{18} \cup$$
$$\cup X_{19}X_{20}X_{21} \cup X_{22} \cup X_{23} \cup X_{24}X_{25} \cup X_{26} \cup X_{27}X_{28} \cup X_{29} \cup X_{30} \cup X_{31} \cup X_{32}$$

Шаг 3. Построение вероятностной функции.

Для расчета итоговой вероятности опасного события функция алгебры логики приводится в базис конъюнкция-отрицание. Таким образом, получаем:

$$F=\overline{\overline{X_1X_2X_3X_4}\ \overline{X_5X_6X_7}\ \overline{X_8X_9X_{10}}\ \overline{X_{11}}\ \overline{X_{12}X_{13}X_{14}X_{15}}\ \overline{X_{16}X_{17}X_{18}}\ \overline{X_{19}X_{20}X_{21}}\ \overline{X_{22}}\ \overline{X_{23}}\ \overline{X_{24}X_{25}}\ \overline{X_{26}}\ \overline{X_{27}X_{28}}\ \overline{X_{29}}\ \overline{X_{30}}\ \overline{X_{31}}\ \overline{X_{32}}}$$

Шаг 4. Расчет оценки вероятности реализации опасного состояния.

В базисе конъюнкция-отрицание для расчета итоговой вероятности опасного состояния инициирующие события могут быть заменены их вероятностями, полученными на основе статистических данных и экспертных оценок (таблица 2).

Вероятности инициирующих событий сценария «Нарушение конфиденциальности БД САПД СК» Таблица 2

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}
0,5	0,4	0,3	0,1	0,5	0,4	0,05	0,01	0,05	0,8	0,005	0,5	0,1	0,3	0,1	0,5
X_{17}	X_{18}	X_{19}	X_{20}	X_{21}	X_{22}	X_{23}	X_{24}	X_{25}	X_{26}	X_{27}	X_{28}	X_{29}	X_{30}	X_{31}	X_{32}
0,4	0,05	0,01	0,01	0,2	0,07	0,05	0,3	0,1	0,15	0,5	0,05	0,1	0,15	0,01	0,005

Расчетное значение вероятности опасного состояния P= 0,4821.

Величина риска реализации опасного состояния R, определяемая как $R = P \cdot S$,где S – оценка ущерба от реализации опасного состояния, составляет

$$R = 0{,}4821 \cdot 3\,400\,000 = 1\,639\,140 \text{ (руб.)}.$$

На рисунке 4 представлен анализ результатов управления рисками информационных систем трех различных организаций – ИСО 1, ИСО 2, ИСО 3 (рис. 4А) и доли ИР, приходящиеся на каждый способ управления (рис. 4В).

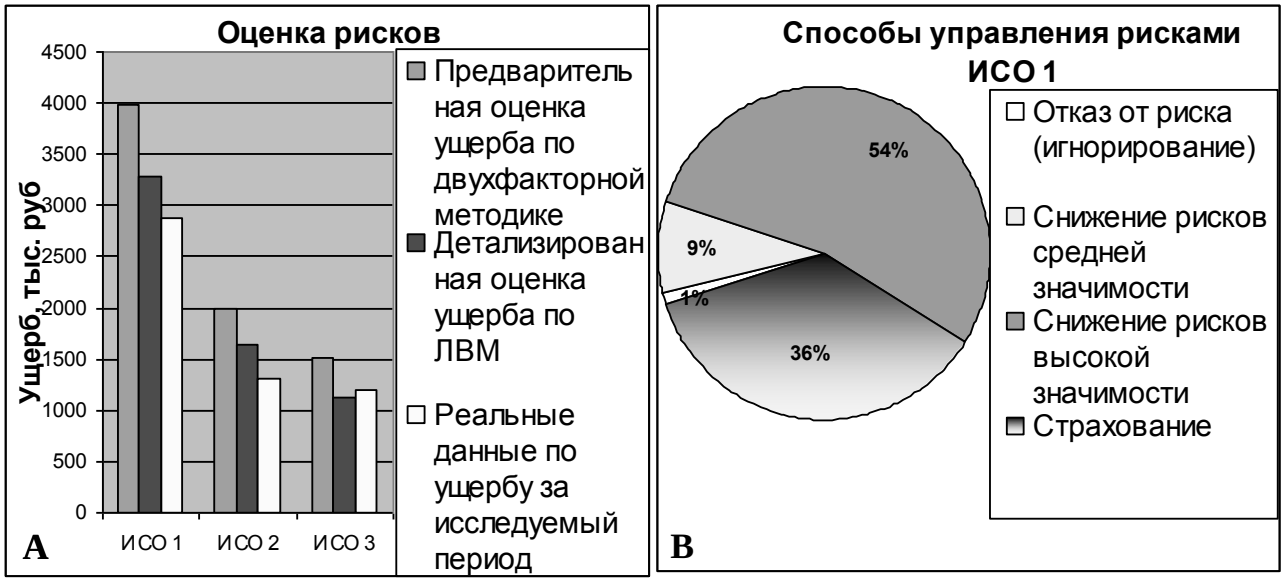

Рисунок 4 – Анализ результатов внедрения

При сравнении результатов детализированная оценка ИР по ЛВМ ближе к реальному ущербу, чем оценка по двухфакторной методике.

В четвертой главе рассматривается программное обеспечение, реализующее подходы и алгоритмы, представленные во второй главе.

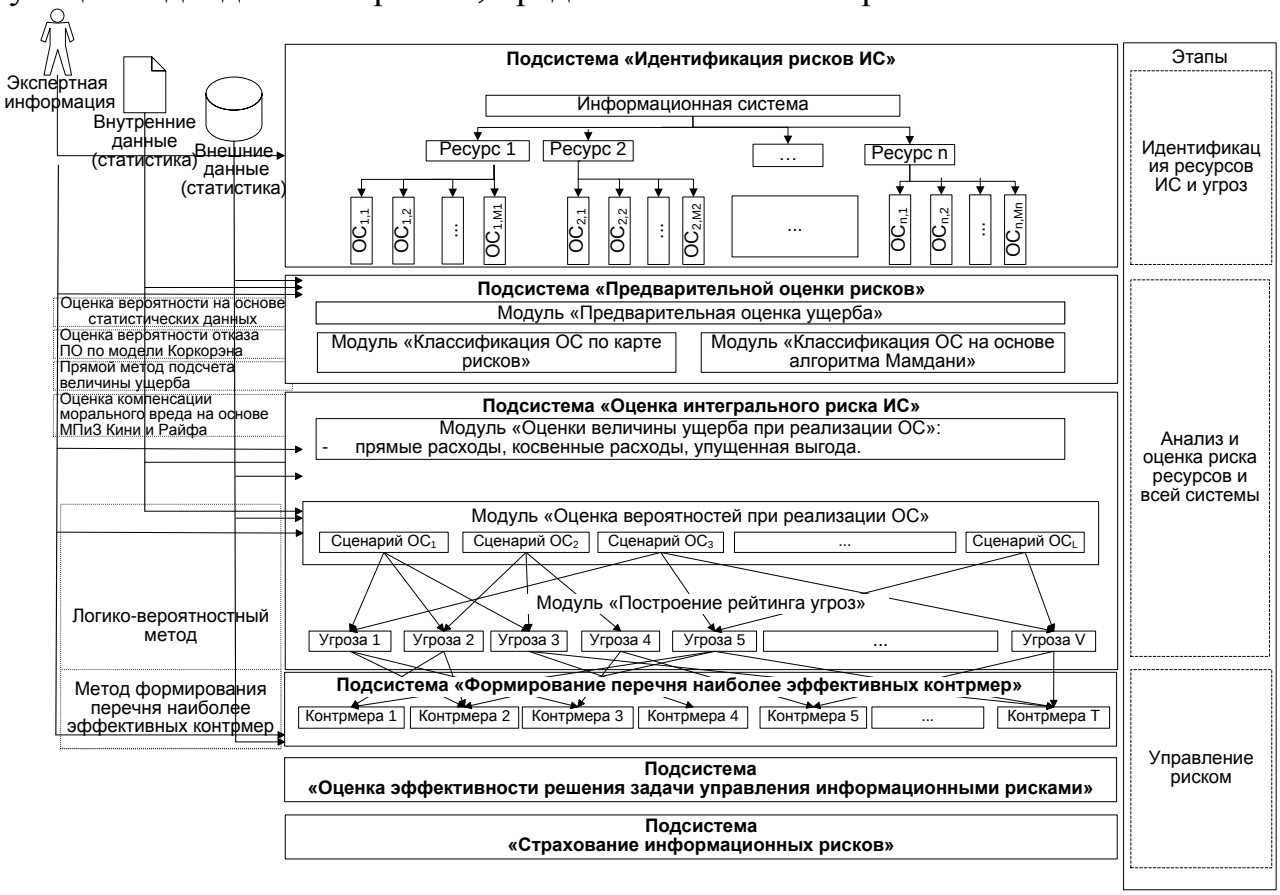

Рисунок 5 – Структура программного комплекса «СУИР ЛВМ»

На рисунке 6 представлен интерфейс «СУИР ЛВМ» на примере автоматизированного расчета вероятности опасного состояния «Нарушение конфиденциальности БД САПД СК». Результат расчета риска до и после внедрения контрмер для этого сценария выделен в окне Scenarios. В центральной части формы расположены входные данные сценария, справа - матрица эффективности контрмер для инициирующих событий.

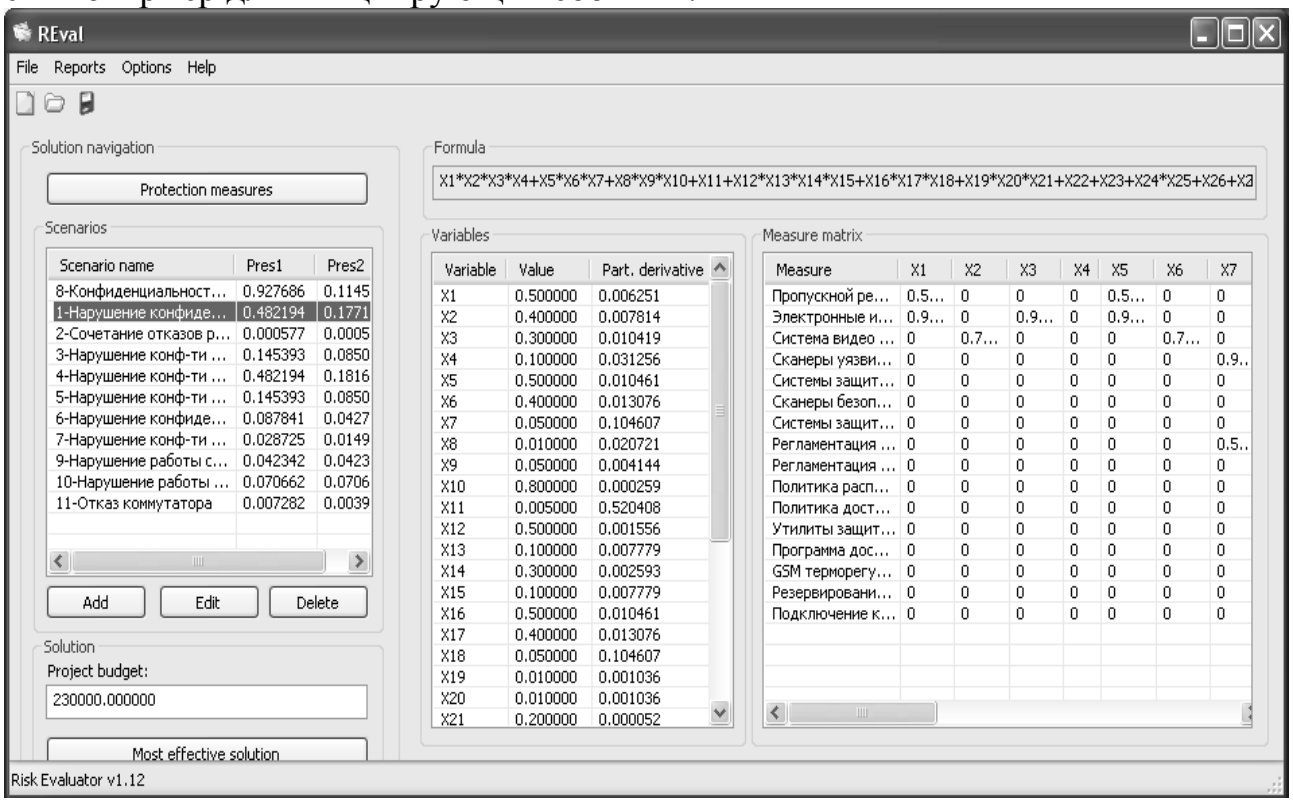

Рисунок 6 – Интерфейс программного комплекса «СУИР ЛВМ»

Проведен сравнительный анализ разработанной системы с современными системами управления информационными рисками.

Разработанная «СУИР ЛВМ» является представителем класса систем анализа защищенности и управления риском. Данная программа позволяет моделировать риски безопасности средних и крупных информационных систем организаций с высокой степенью адекватности. Система позволяет рационально распределить время на оценку ИС: игнорировать малозначимые риски, быстро оценивать средние риски и с высокой степенью детализации и точности оценивать наиболее значимые риски.

Высокая точность оценки рисков ИС важна не только для внутренних целей организации, но и при взаимодействии с представителями внешних организаций, такими, как аудиторы надзорных органов и андеррайтеры страховых компаний.

Пользователями системы являются специалисты по ИБ, системные администраторы, аудиторы и андеррайтеры СК. Для работы с программным средством требуется уровень квалификации специалиста по ИБ.

В реализованной программе модель системы является статической. Существуют два состояния: начальное (текущее) и конечное (состояние, после

внедрения выбранного эффективного набора контрмер и страхования части опасных состояний). СУИР может быть дополнена до динамического варианта, в котором поддерживается последовательное внедрение наборов контрмер и учет изменений структуры информационной системы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Предложена структура системы управления информационными рисками СК ДМС на основе ЛВМ и разработанных моделей, которая позволяет анализировать, оценивать информационные риски компании и снижать их за счет эффективных контрмер.
2. Разработана функциональная модель процесса управления информационными рисками, основанная на применении SADT-методологии, использование которой позволяет обоснованно выбрать состав и функции основных этапов анализа и управления рисками СК ДМС. На основе данной модели предложена методика количественной оценки рисков, учитывающая различную степень детализации опасных состояний в зависимости от их значимости на основе алгоритма нечеткой логики Мамдани, карты рисков и логико-вероятностного подхода:
   - применение алгоритма Мамдани для оценки значимости ОС позволило снизить временные затраты эксперта по информационной безопасности на анализ опасных состояний ИС СК ДМС на 40%;
   - эффективность решения задачи управления ИР СК ДМС составила 59% и 68% для первого и второго варианта алгоритмов соответственно для фиксированного бюджета.
3. Предложен метод оценки ущерба при реализации опасных состояний, в том числе оценки компенсации морального ущерба в случае нарушения конфиденциальности информации, который основан на модификации метода предпочтения и замещения.
4. Предложен метод формирования эффективного набора контрмер, основанный на применении ЛВМ, использование которого позволяет определить оптимальный состав программно- аппаратных средств и организационных мероприятий при заданном бюджете ИБ.
5. Разработана методика страхования информационных рисков, основанная на применении предложенных моделей и методов анализа и управления рисками, что позволяет дать обоснованные рекомендации по выбору объектов страхования и размеру страховой суммы и премии.
6. Разработано программное обеспечение СУИР СК ДМС, позволяющее осуществлять поддержку основных этапов риска-анализа в процессе управления информационными рисками организации.

Система управления информационными рисками на основе логико-вероятностного метода (свидетельство об офиц. регистрации программы для ЭВМ. №2008612183) внедрена в ООО «МСК «УралСиб»», ООО «Росгосстрах-Аккорд» и Уфимском филиале Центрального коммерческого банка.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в периодическом издании из списка ВАК:

1. Задача управления информационными рисками компании добровольного медицинского страхования / Кустов Г.А. // Вестник УГАТУ, серия «Управление, вычислительная техника и информатика» Т.9, №4(22), 2007.- Уфа: УГАТУ.–С. 77–84.
2. Методы принятия решений в задачах управления риском на примере исследования риска неэффективного лечения в лечебно-профилактическом учреждении / Зотова О.Ф., Зиборов Г.С., Кустов Г.А. // Управление риском, №4 (44), 2007 - М.: Изд-во Анкил.–С. 62–66.

***Другие публикации*:**

3. Защита систем микроплатежей / Васильев В.И., Кустов Г.А. // Информационная безопасность: Материалы VI Международной научно-практической конференции. - Таганрог: Изд-во ТРТУ, 2004.–С. 62–63.
4. Организация и защита данных в системах аналитической поддержки деятельности компании ДМС / Зотова О.Ф., Кустов Г.А. // Принятие решений в условиях неопределенности. Вопросы моделирования: Межвузовский научный сборник. – Уфа: УГАТУ, 2006.–С. 56–61.
5. Защита конфиденциальности в медицинских базах данных / Калабухов М.С., Кашаев Т.Р., Кустов Г.А. // Актуальные вопросы современной медицины и здравоохранения: Материалы Республиканской Научно-практической конференции Уфа: БГМУ, 2006.–С. 114–181.
6. Управление рисками в добровольном медицинском страховании / Кустов Г.А., Зотова О.Ф. // Принятие решений в условиях неопределенности. Вопросы моделирования: Межвуз. научн. сб.- Уфа: УГАТУ, 2007.–С. 91–98.
7. Задача управления информационными рисками страховой компании / Кустов Г.А., Николаева М.А., Зотова О.Ф. // Компьютерные науки и информационные технологии (CSIT’2007): Тр. 9-го Междунар. симп. Уфа, Россия, 2007. Уфа: УГАТУ, 2007. Т. 1.–С. 102–107. (Статья на англ. яз.).
8. Комплексный подход к управлению рисками страховой компании ДМС / Кустов Г.А., Николаева М.А., Зотова О.Ф. // Системный анализ в проектировании и управлении: Труды XI международной научно-технической конференции. СПб.: Изд-во Политехнического университета, 2007,–С. 84–86.
9. Оценка морального ущерба при нарушении конфиденциальности / Кустов Г.А. Степанова М.К. // Мавлютовские чтения: Всероссийская молодежная научная конференция. Уфа: УГАТУ, 2007.–С. 39–40.
10. Система управления информационными рисками на основе логико-вероятностного метода / Кустов Г.А. // Информатика управление и компьютерные науки: Третья всероссийская зимняя школа-семинар аспирантов и молодых ученых, Сборник статей, Уфа: УГАТУ 2008. Т.1 –С. 338–346.

Диссертант *Г.А.Кустов*