Уфа : УГАТУ, 2007 Вестник УГАТУ • Управление, ВТ и И Т. 9, № 4 (22). С. 77–84

УДК 519:368

Г. А. КУСТОВ

ЗАДАЧА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ КОМПАНИИ ДОБРОВОЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ

Обозначено место информационных рисков (ИР) в дереве рисков компаний добровольного медицинского страхования (ДМС). Выделены этапы и задачи управления ИР. Рассмотрены основные положения логико-вероятностного метода (ЛВМ) как механизма анализа и оценки ИР сложных систем. Рассмотрен пример оценки итоговой вероятности реализации опасного события для информационного ресурса конкретной страховой компании. *Риски страховой компании; этапы риск-анализа; информационные риски; логико-вероятностный метод; анализ и оценка опасного состояния ресурса информационной системы*

ВВЕДЕНИЕ

Актуальность исследований, представленных в этой статье, связана с принятием Федерального закона «О персональных данных» и реализацией законов «Об информации, информатизации и защите информации» и «О медицинском страховании граждан в Российской Федерации». Действительность такова, что нерешенными остаются проблемы правового, технического, финансового регулирования проблем функционирования медицинских информационных систем, которые располагают хранилищем весьма «дорогих данных». Открытыми остаются вопросы гарантий доступа к информации, ее цена, вопросы защиты врачебной тайны, обмена информацией с «третьими лицами» и, безусловно, вопрос об определении размера ущерба в случае реализации опасного состояния информационной системы.

Целью деятельности страховой компании (СК) является получение прибыли от проведения эффективной политики в области страхования и инвестирования. Другими словами, деятельность страховой компании сосредоточена на решении вопросов управления техническими, нетехническими и инвестиционными рисками.

Технические риски — это риски недостаточности средств страховой компании для выполнения обязательств по страховым выплатам, обусловленные выполнением ею страховых операций.

Инвестиционные риски связаны с инвестиционной деятельностью страховой компании.

Нетехнические риски обусловлены влиянием внешних и внутренних факторов, не связанных со страховой и инвестиционной деятельностью. К ним относятся риски, связанные с нарушением бизнес-процессов, в частности, риски управления, риск невыполнения нестраховых обязательств, риск неполучения средств от посредников и риски бизнеса.

К нетехническим рискам относятся и риски, связанные с функционированием информационных систем (ИС) и технологий организации. В рамках данной работы предлагается называть их «информационные риски» (ИР). Они являются важной составляющей группы нетехнических рисков.

На рис. 1 выделены технические риски. Алгоритмы их снижения представлены в работах [1, 2]. Цель данного исследования — эффективное управление информационными рисками.

Рассмотрим основные этапы риск-анализа и задачи, решаемые на каждом из этапов (табл. 1).

В данной статье остановимся подробнее на задаче определения структуры информационных рисков компании ДМС и на задаче оценки вероятности реализации опасного состояния ресурса ИС. Для решения этих задач предлагается использовать логико-вероятностный метод вычисления и анализа безопасности и риска И. А. *Рябинина* [3].

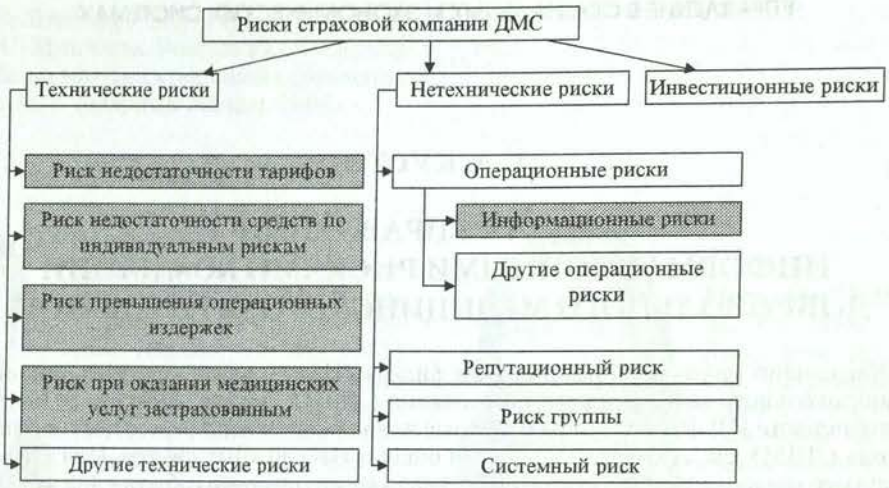

Рис. 1. Дерево рисков страховой компании ДМС

Таблица 1

Основные этапы риск-анализа и задачи, решаемые на каждом из этапов

Название этапа	Задачи
Этап идентификации	1. Задача определения структуры информационных рисков СК.
Этап анализа и оценки риска ресурсов и всей системы	2. Задача оценки интегрального риска информационной системы (ИС) СК: 2.1. задача оценки вероятности реализации опасного состояния ресурса ИС, 2.2. задача оценки ущерба при реализации опасного состояния ресурса ИС: 2.2.1. задача оценки материального ущерба, 2.2.2. задача оценки величины ущерба при утечке конфиденциальной информации или персональных данных, в том числе задача определения размера компенсации морального вреда.
Этап управления риском	3. Задача оценки и выбора наиболее эффективных контрмер. 4. Задача страхования информационных рисков. 5. Задача формирования величины нагрузки с учетом информационных рисков.

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ ЛВМ ВЫЧИСЛЕНИЯ И АНАЛИЗА БЕЗОПАСНОСТИ И РИСКА

ЛВМ возник в результате исследований проблем безопасности сложных систем. Основная идея метода состоит в сочетании логического и вероятностного подходов при решении задач оценки надежности и безопасности сложных систем — экономических, социальных, технических и др.

Сложные системы в общем случае являются человеко-машинными системами, состоящими из таких элементов, как оборудование, компьютеры, программные средства, действия персонала и т. д. [3].

Каждый элемент может быть связан с другими элементами специфическим образом, поэтому важным этапом является выяснение взаимосвязей и топологии системы.

В ЛВМ используются понятия **опасного состояния системы** и **опасности** — способности системы переходить в опасное состояние. Начинается описание опасного состояния системы с составления **сценария опасного состояния**, который строится с помощью дизъюнкций и конъюнкций над **инициирующими условиями** и **событиями**.

В качестве инициирующих условий и событий выступают отказы одного или нескольких элементов системы.

Каждому элементу системы ставится в соответствие **логическая переменная** x_k

($k = \overline{1,h}$) с двумя возможными состояниями (например, работоспособности/отказа, готовности/не готовности и т. п.) с заданными вероятностными параметрами этих состояний p_k и $q_k = 1 - p_k$.

Сценарий является основой для составления логической функции или функции алгебры логики (ФАЛ), описывающей опасное состояние системы.

Следующим шагом является преобразование функции алгебры логики к вероятностной функции, которая в дальнейшем используется для получения количественной оценки вероятности реализации опасного состояния.

1.1. Постановка задачи

Дано: ресурс, для которого выделены опасные состояния S_j, $j = \overline{1,m}$.

Требуется найти: вероятности реализации опасных состояний P_j ресурса S_j, $j = \overline{1,m}$ и значимость каждого инициирующего условия или события (в терминах теории безопасности — угрозы) с точки зрения вклада в реализацию опасного состояния.

1.2. Алгоритм решения

Шаг 1. Составление сценария опасного состояния S_j.

Шаг 2. Построение функции алгебры логики $f(x_1, \ldots, x_h)$ с использованием операций конъюнкции и дизъюнкции на основе сценария опасного состояния S_j.

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

Шаг 4. Расчет вероятности реализации опасного состояния P_j с помощью вероятностной функции.

Шаг 5. Расчет значимости каждой угрозы с точки зрения вклада в реализацию опасного состояния.

1.3. Шаг 1. Составление сценария опасного состояния

Составление сценария опасного состояния системы можно представить в виде последовательности:

1) выделение конечного события — опасного состояния (отказа),

2) выделение промежуточных событий, приводящих к реализации опасного состояния и получаемых как комбинация двух или более инициирующих событий,

3) выделение инициирующих событий-угроз.

Для представления опасного состояния используется дерево событий или отказов.

На рис. 2 представлен пример сценария опасного состояния в виде дерева событий.

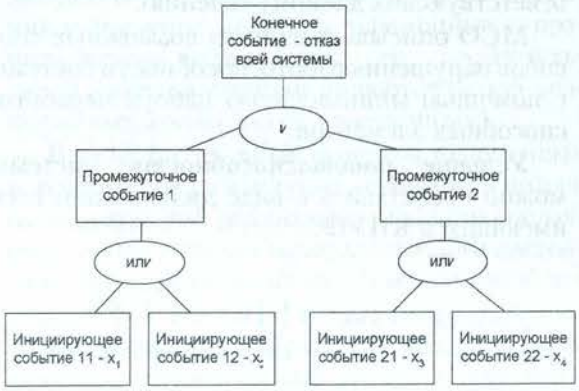

Рис. 2. Пример дерева событий для описания опасного состояния системы

1.4. Шаг 2. Построение функции алгебры логики

С помощью дерева событий составляется функция алгебры логики, описывающая условия работоспособности системы или перехода системы в опасное состояние.

При этом для описания условий работоспособности системы используется понятие ***«кратчайший путь успешного функционирования»***, а для описания условий отказа или перехода системы в опасное состояние используется понятие ***«минимальное сечение отказов»***.

Кратчайший путь успешного функционирования (КПУФ) есть конъюнкция таких элементов системы, ни один из которых нельзя изъять, не нарушив успешного функционирования системы:

$$W_l = \bigcap_{k \in Kwl} x_k,$$

где K_{wl} — множество номеров переменных, соответствующих данному пути.

КПУФ позволяет описать один из вариантов успешного функционирования системы, причем набор элементов минимальный.

Совокупность ребер графа, при удалении которых граф теряет свою целостность, называют ***разрезом*** или ***сечением***.

Минимальное сечение отказов (МСО) системы есть конъюнкция отрицаний тех элементов, ни один из которых нельзя изъять,

не нарушив условия неработоспособности системы:

$$Q_l = \bigcap_{k \in Kql} \overline{x_k},$$

где K_{ql} — множество номеров переменных, соответствующих данному сечению.

МСО описывает один из возможных способов нарушения работоспособности системы с помощью минимального набора неработоспособных элементов.

Условие работоспособности системы можно представить в виде дизъюнкции всех имеющихся КПУФ:

$$f(x_1, x_2, \ldots, x_h) = \bigcup_{l=1}^{d} W_l = \bigcup_{l=1}^{d} \bigcap_{k \in Kwl} x_k.$$

Условие неработоспособности системы можно представить в виде дизъюнкции всех МСО:

$$f(x_1, x_2, \ldots, x_h) = \bigcup_{l=1}^{t} Q_l = \bigcup_{l=1}^{t} \bigcap_{k \in Kql} \overline{x_k}.$$

Пример. Пусть дерево событий имеет вид, представленный на рис. 2.

КПУФ являются: $x_1 \cap x_3$, $x_1 \cap x_4$, $x_2 \cap x_3$, $x_2 \cap x_4$.

МСО являются: $\overline{x_1} \cap \overline{x_2}$, $\overline{x_3} \cap \overline{x_4}$.

Тогда условие работоспособности имеет вид

$$f(x_1, x_2, x_3, x_4) = (x_1 \cap x_3) \cup (x_1 \cap x_4) \cup (x_2 \cap x_3) \cup (x_2 \cap x_4).$$

Условие неработоспособности имеет вид

$$f(x_1, x_2, x_3, x_4) = (\overline{x_1} \cap \overline{x_2}) \cup (\overline{x_3} \cap \overline{x_4}).$$

1.5. Шаг 3. Построение вероятностной функции

На предыдущем этапе была получена ФАЛ $f(x_1, x_2, \ldots, x_h)$, описывающая опасное состояние системы как дизъюнкцию всех МСО.

Следующим шагом является преобразование ФАЛ к специальному виду, в котором производится замещение каждой логической переменной вероятностью ее равенства единице. Этот вид ФАЛ называют формой перехода к полному замещению (ФППЗ). ФППЗ являются совершенная дизъюнктивная нормальная форма, ортогональная дизъюнктивная нормальная форма и бесповторная ФАЛ в базисе конъюнкция-отрицание.

Построение вероятностной функции (ВФ) на основе ФППЗ осуществляется согласно специальным правилам. Результатом данного этапа является вероятностная функция $P(f(x_1, x_2, \ldots, x_h) = 1) = P(\{p_k, q_k\}, k = \overline{1, h})$.

Правила построения ВФ для ФАЛ, представленной в ФППЗ [3]:

1) каждая логическая переменная в ФППЗ заменяется вероятностью ее равенства единице:

$$P\{x_i = 1\} = p_i,$$
$$P\{x_i = 0\} = P\{\overline{x_i} = 1\} = q_i = 1 - p_i;$$

2) отрицание функции заменяется разностью между единицей и вероятностью равенства этой функции единице;

3) операции логического умножения и сложения заменяются операциями арифметического умножения и сложения.

1.6. Шаг 4. Расчет оценки вероятности реализации опасного состояния

Подставляя значения $p_k, q_k (k = \overline{1, h})$ в ВФ, полученную на предыдущем этапе, получаем оценку вероятности реализации опасного состояния.

2. ПРИМЕНЕНИЕ ЛВМ ПРИ АНАЛИЗЕ И ОЦЕНКЕ ИР КОМПАНИИ ДМС

В данной работе информационная система департамента ДМС страховой компании рассматривается как отдельная система, состоящая из ресурсов. Отказ какого-либо из ресурсов приводит к невозможности выполнения департаментом ДМС одной или нескольких своих функций.

ЛВМ используется для получения количественных оценок вероятностей реализации опасных состояний для каждого из информационных ресурсов. Таким образом, каждый ресурс в ЛВМ в свою очередь тоже рассматривается как система.

2.1. Описание ресурсов системы

В табл. 2 представлены ресурсы департамента ДМС исследуемой страховой компании. Для выделения ресурсов департамента ДМС использовался перечень ресурсов, представленный в методике CRAMM [4]. В результате были выделены четыре группы ресурсов:

1) информационные ресурсы;
2) сервисы;

3) физические ресурсы;

4) программное обеспечение.

Для информационных ресурсов выделены следующие опасные состояния:

1) потеря ресурса (П);

2) временная недоступность ресурса (Н);

3) сочетание потери ресурса и отсутствия резервной копии ресурса (С);

4) нарушение конфиденциальности ресурса (К).

Для сервисов опасным состоянием является временная недоступность (П). Для физических ресурсов опасными состояниями являются невосстанавливаемый и восстанавливаемый аппаратный отказ (О). Для программного обеспечения опасными состояниями являются сбой и отказ программного обеспечения (О).

Величина потерь от однократной реализации опасного состояния зависит от типа ресурса и типа опасного состояния. Оценки величины потерь от однократной реализации опасного состояния для каждого ресурса были получены в результате совместной работы с сотрудниками СК. Вопрос оценки величины потерь от нарушения конфиденциальности информационного ресурса был выделен в отдельную задачу.

Частота реализации опасного состояния в течение года была рассчитана на основе статистических данных или оценена экспертно.

Стоимость считается низкой, если восстановление сервиса производится в течение одного/двух часов, средней, если восстановление сервиса производится в течение одного рабочего дня, и высокой во всех остальных случаях.

В этой статье рассмотрим только часть ресурсов компании ДМС, а именно информационные ресурсы.

2.2. Выбор опасных состояний ресурсов для анализа

Теперь необходимо выявить те опасные состояния, потери от которых наиболее существенны, то есть наиболее значимые состояния. Для них в дальнейшем будут строиться сценарии опасных состояний и выявляться наиболее значимые угрозы (инициирующие события или условия).

На величину потерь от реализации того или иного опасного состояния или на значимость опасного состояния влияют два фактора — собственно стоимость потерь от однократной реализации опасного состояния и частота реализации опасного состояния в течение рассматриваемого временного интервала.

Для **предварительной оценки** стоимости потерь от реализации определенного опасного состояния в течение года предлагается использовать подход на основе нечеткой логики, а именно алгоритм Мамадани [5]. Входными данными для алгоритма являются описание и значения нечетких переменных и правила вывода вида «если ... , то ... ». Результатом работы алгоритма являются четкие значения выходной(ых) переменной(ых).

В качестве входных нечетких переменных в данном случае выступят «стоимость потерь от однократной реализации опасного состояния» и «частота реализации опасного состояния в течение года». В качестве выходной переменной — значимость опасного состояния.

Результатом данного этапа является перечень опасных состояний ресурсов, для которых необходимо провести дальнейший анализ.

2.3. Составление сценария опасного состояния

На рис. 3 представлен сценарий опасного состояния «нарушение конфиденциальности БД системы аналитической поддержки деятельности страховой компании» (подсистема «Учет оперативной деятельности»).

2.4. Построение функции алгебры логики

Согласно описанному сценарию логическая функция выглядит следующим образом:

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

2.5. Построение вероятностной функции

Для расчета итоговой вероятности опасного события функция алгебры логики переводится в базис конъюнкция-отрицание и вычисляется по формуле

$$F = \overline{\overline{X_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}} \; \overline{X_{11}X_{12}X_{13}X_{14}X_{15}X_{16}X_{17}X_{18}X_{19}X_{20}X_{21}X_{22}} \; \overline{X_{23}X_{24}X_{25}X_{26}X_{27}X_{28}X_{29}X_{30}X_{31}X_{32}}}.$$

Таблица 2

Информационные ресурсы компании ДМС

№	Название ресурса	Тип опасного события	Экспертная оценка частоты реализации опасного события в течение года	Оценка стоимости реализации опасного события, руб.
1	БД системы аналитической поддержки деятельности страховой компании (САИД СК)	П	Средняя 0,33	Низкая 5 000
		Н	Средняя 0,2	Низкая 5 000
		К	Средняя 0,15	Очень высокая 3 400 000
2	Ежедневные резервные копии БД САИД СК за последние 30 дней	С	Низкая 0,01	Высокая 384 000
		К	Низкая 0,02	Очень высокая 3 400 000
3	Хранилище агрегированных данных	П	Средняя 0,20	Низкая 5 000
		Н	Средняя	Средняя 5 000
		К	Низкая 0,02	Очень высокая 4 800 000
4	Еженедельные резервные копии хранилища агрегированных данных за последние 12 недель	С	Низкая 0,01	Очень высокая 700 000
		К	Низкая 0,02	Очень высокая 1 152 000
5	Почтовые адресные книги сотрудников департамента ДМС	П	Средняя 0,35	Низкая 10 000
		К	Средняя 0,10	Высокая 950 000
6	Почтовые БД сотрудников департамента ДМС	П	Средняя 0,25	Средняя 475 000
		К	Низкая 0,09	Очень высокая 1 900 000
7	Электронные документы департамента ДМС, хранящиеся на сетевом диске (тексты договоров, отчеты, письма и пр.)	П	Высокая 0,55	Высокая 576 000
		К	Средняя 0,12	Очень высокая 2 304 000

2.6. Расчет оценки вероятности реализации опасного состояния

В базисе конъюнкция-отрицание для расчета итоговой вероятности опасного события элементарные составляющие события могут быть заменены их вероятностями, полученными в результате экспертной оценки.

Расчетное значение вероятности

$$F = 0{,}49.$$

Величина риска реализации опасного события R может быть определена как

$$R = F \cdot S,$$

где S — оценка стоимости реализации опасного события из табл. 2.

Таким образом, получаем

$$R = 0{,}49 \cdot 3400000 = 1\,666\,000 \text{ (руб.)}$$

Это значительная сумма для СК. В примере рассчитанная вероятность реализации опасного события значительно превосходит первоначальную экспертную оценку. Полученный результат говорит о более тщательной оценке информационных рисков ресурсов с помощью ЛВМ.

Задачу о вкладе составляющих в итоговый риск автор решил, используя также ЛВМ.

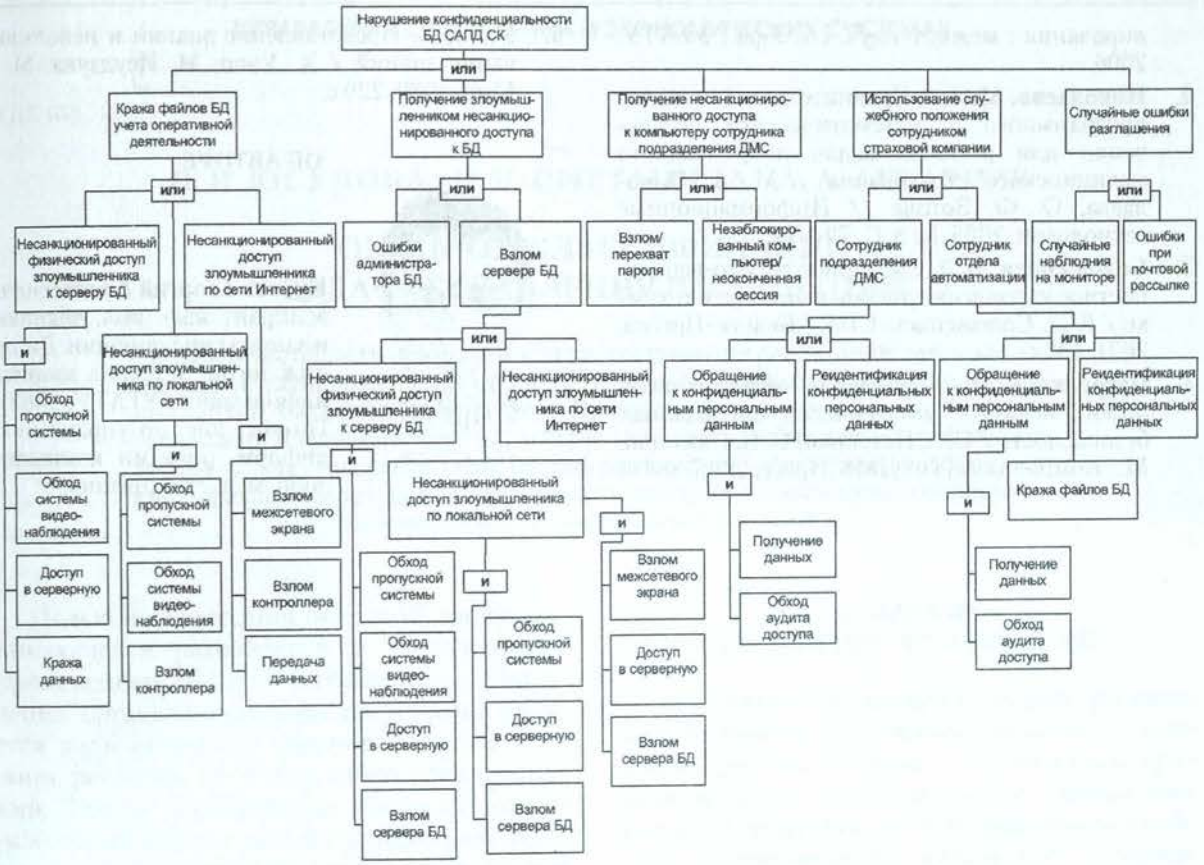

Рис. 3. Сценарий опасного состояния «Нарушение конфиденциальности БД САПД СК»

Таблица 3

Вероятности составляющих событий сценария «Нарушение конфиденциальности БД САПД СК»

$X1$	$X2$	$X3$	$X4$	$X5$	$X6$	$X7$	$X8$	$X9$	$X10$	$X11$	$X12$	$X13$	$X14$	$X15$	$X16$
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
$X17$	$X18$	$X19$	$X20$	$X21$	$X22$	$X23$	$X24$	$X25$	$X26$	$X27$	$X28$	$X29$	$X30$	$X31$	$X32$
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

Наиболее существенные ингредиенты заслуживают особого внимания и влекут за собой определение контрмер. Реализация алгоритма построения медианы Кемени позволила решить задачу выбора наиболее эффективных контрмер.

ЗАКЛЮЧЕНИЕ

ЛВМ предоставляет механизм для анализа опасных состояний информационной системы и теоретически обосновывает подход к количественной оценке риска.

Применение метода позволяет наиболее полно учитывать особенности реализации угроз в сложных информационных системах и выявлять вклад конкретной угрозы в реализацию опасного состояния ресурса и всей системы.

Эта информация является ключевой для принятия решения о выборе контрмер аналитиком информационной безопасности.

Кроме того, наиболее значимые опасные состояния ресурсов могут быть проанализированы с высокой степенью детализации.

Повторная оценка риска ИС может быть произведена при существенных изменениях в сценариях опасных состояний ресурсов или в составляющих информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. **Кустов, Г. А.** Управление рисками в добровольном медицинском страховании / Г. А. Кустов, О. Ф. Зотова // Принятие решений в условиях неопределенности. Вопросы моде-

лирования : межвуз. науч. сб. Уфа : УГАТУ, 2006.

2. **Николаева, М. А.** Сравнительный анализ программного и математического обеспечения для решения задач добровольного медицинского страхования / М. А. Николаева, О. Ф. Зотова // Информационные технологии. 2005. № 8. С. 72–79.
3. **Соложенцев, Е. Д.** Сценарное логико-вероятностное управление риском в бизнесе и технике / Е. Д. Соложенцев. СПб. : Бизнес-Пресса, 2004. 432 с.
4. **Петренко, С. А.** Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. М. : Компания АйТи ; ДМК Пресс, 2005. 384 с.
5. **Уэно, Х.** Представление знаний и использование знаний / Х. Уэно, М. Исудзука. М. : Мир, 1989. 220 с.

ОБ АВТОРЕ

Кустов Георгий Алексеевич, аспирант каф. выч. техники и защиты информации. Дипл. инж. по орг. и технол. защиты информации (УГАТУ, 2003). Готовит дис. по управлению информ. рисками компании добр. мед. страхования.