На правах рукописи

ГИЛЬМУЛЛИН Тимур Мансурович

МОДЕЛИ И КОМПЛЕКС ПРОГРАММ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 05.13.18 – математическое моделирование, численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Казань – 2010

Работа выполнена в Казанском государственном техническом университете им. А.Н. Туполева

Научный руководитель: кандидат технических наук, доцент Аникин Игорь Вячеславович

Официальные оппоненты: доктор технических наук, профессор Захаров Вячеслав Михайлович

доктор технических наук, профессор Исмагилов Ильяс Идрисович

Ведущая организация: Новгородский государственный университет имени Ярослава Мудрого

Защита состоится «28» мая 2010 г. в 15[00] часов на заседании диссертационного совета Д 212.079.01 в Казанском государственном техническом университете им. А.Н. Туполева по адресу: 420111, г. Казань, ул. К. Маркса, д. 10, зал заседаний Учёного совета. Автореферат диссертации размещен на сайте Казанского государственного технического университета им. А.Н. Туполева www.kai.ru

С диссертацией можно ознакомиться в библиотеке Казанского государственного технического университета им. А.Н. Туполева.

Автореферат разослан «25» апреля 2010 г.

Учёный секретарь диссертационного совета
доктор физико-математических наук, профессор П.Г. Данилаев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. При проектировании современных информационных систем (ИС) вопросы защиты информации должны рассматриваться в качестве её неотъемлемой составляющей. Все возрастающее количество уязвимостей элементов информационных систем, а также угроз информационной безопасности (ИБ) способно привести к нанесению злоумышленником значительного ущерба организации.

Несмотря на то, что для ИС существуют определяемые российским законодательством требования по защите информации, в настоящее время особую значимость приобретают подходы к моделированию построения эффективных систем защиты с позиции ожидаемого ущерба и управления информационными рисками.

Проведенный анализ существующих подходов к управлению рисками информационной безопасности показывает, что основными сложностями их практической реализации являются следующие:

- трудная формализация решения задачи оценки и управления рисками ИБ;
- необходимость формализации модели информационной системы как объекта управления рисками ИБ, а также учета человеческого фактора нарушителя;
- нечеткость и качественность основных факторов риска ИБ – возможности реализации угроз ИБ и уровня ущерба;
- необходимость принятия решений о выборе системы защиты информации в условиях неопределенности и неполноты информации.

В связи с этим, при решении задачи оценки и управления рисками ИБ актуально использование таких методов искусственного интеллекта, как экспертные и нечеткие системы, показавшие свою эффективность при решении задач в условиях вышеперечисленных сложностей.

Исследованию проблемы управления рисками ИБ с позиций экспертных и нечетких систем посвящены работы таких российских и зарубежных ученых, как В.А. Герасименко, Д.П. Зегжды, П.Д. Зегжды, А.А. Кононова, С.С. Корта, И.Д. Медведовского, С.А. Петренко, Л. Хоффмана, В.И. Васильева, Т.К. Сиразетдинова, В.И. Гловы, И.В. Аникина, Р.И. Насырова, G.F. Florez, S.M. Bridges, R.B. Vaughn, P.F. Peter и других. Однако, несмотря на это, многие вопросы в данной области остаются недостаточно исследованными.

Таким образом, актуальной задачей является разработка моделей и алгоритмов для задачи оценки и управления рисками ИБ информационных систем, основанных на методах теории искусственного интеллекта.

Объект исследования: методы обеспечения информационной безопасности ИС.

Предмет исследования: модели и методы управления рисками ИБ для ИС.

Цель работы: повышение эффективности процесса управления рисками ИБ ИС и обоснованности выбора защитных мероприятий в нечетких условиях.

Научная задача: формализация моделей, алгоритмов оценки и управления рисками ИБ для ИС, а также разработка реализующего их комплекса программ.

Достижение цели и поставленной задачи потребовало:

- разработки концептуальной модели процесса управления рисками ИБ ИС;
- разработки теоретико-множественных моделей для задачи управления рисками информационной безопасности;
- разработки методики оценки и алгоритмов управления рисками ИБ ИС в нечетких условиях;
- разработки экспертного программного комплекса (ЭПК) управления рисками информационной безопасности;

– проведения экспериментальных исследований для оценки качества разработанных моделей, методики и алгоритмов.

Методы исследования. Для решения обозначенных задач использованы методы системного анализа, теоретико-множественного моделирования, теории нечетких систем, принятия решений в условиях неопределенности.

Достоверность полученных результатов обоснована корректным использованием методов математического моделирования, предложенными в диссертационной работе моделями и алгоритмами, строгостью доказательства теорем, результатами экспериментов и испытаний, а также тем, что полученные результаты не противоречат известным положениям других авторов.

Научная новизна работы заключается в следующем:

– разработана концептуальная модель предметной области «Управление рисками информационной безопасности ИС» в рамках ER-диаграммы типов, а также определена семантика её понятий в рамках теории категорий и функторов;

– разработаны новые модели, методика и алгоритмы для задачи управления рисками ИБ информационных систем в нечетких условиях;

– разработаны новые теоретико-множественные модели для задачи управления рисками ИБ информационных систем.

Теоретическая значимость работы заключается в следующем:

– предложен способ формализации понятий, основанный на теоретико-множественном подходе, и описана семантика предметной области «Управление рисками ИБ ИС»;

– доказаны теоремы о полноте квазиметрического пространства информационных систем, о существовании в нем не обязательно единственной неподвижной точки, и утверждения о существовании минимального риска ИБ для информационных систем, о существовании контрмеры, минимизирующей уровень риска ИБ;

– показана устойчивость разработанной модели информационной системы в смысле непрерывности по квазиметрике риска и оценена сложность разработанного алгоритма оценки уровня риска ИБ.

Практическая ценность работы заключается в разработке методики оценки и управления рисками ИБ ИС, а также реализующего её комплекса программ, позволяющего моделировать ИС, использовать нечеткие оценки экспертов. Практическое применение методики и комплекса программ позволяет выбирать наилучшую систему защиты информации для ИС с позиции ожидаемого ущерба.

По проблеме диссертационной работы опубликовано 10 работ, в том числе 1 статья в журнале из списка, рекомендованного ВАК РФ, 6 статей и 3 тезиса докладов.

Основные положения и результаты диссертации докладывались и обсуждались: на всероссийской научной конференции «Информационные технологии в науке, образовании» (Казань, 2007 г.), 5-ой ежегодной международной научно-практической конференции «Инфокоммуникационные технологии глобального информационного общества» (Казань, 2007 г.), 16-ой международной молодежной научной конференции «Туполевские чтения» (Казань, 2008 г.), 9-ой международной научно-технической конференции «Проблемы техники и технологий телекоммуникаций ПТиТТ'2008» (Казань, 2008 г.), международной научной конференции «Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта ISDMCI'2009» (Херсон, 2009), [illegible] молодежной научной конференции «Туполевские чтения» (Казань, 2009 г.), [illegible] научно-практической конфе-

ренции «Инфокоммуникационные технологии Глобального информационного общества ИКТ ГИО'2009 (Казань, 2009), 12-ой международной научно-технической конференции «Моделирование, идентификация, синтез систем управления МИССУ'2009» (Донецк, 2009).

Реализация результатов работы. Результаты исследования:

– прошли успешную апробацию и внедрены в опытную эксплуатацию в МВД Республики Татарстан;
– используются при решении задач управления рисками ИБ информационных систем в группе компаний «ЦЕНТР»;
– внедрены в учебный процесс ГОУ ВПО КГТУ им. А.Н. Туполева (КАИ) и используются при изучении материалов дисциплин «Анализ и управление рисками в информационных технологиях», «Экономика защиты информации».

Пути дальнейшей реализации. Разработанный комплекс программ предлагается использовать как инструмент эксперта для оценки состояния ИБ организации. В перспективе поставлена задача по созданию ЭПК, выполняющего оценку рисков ИБ с учетом требований действующих российских, международных, отраслевых и ведомственных стандартов в области информационной безопасности.

На защиту выносятся следующие результаты:

– концептуальная модель предметной области «Управление рисками ИБ ИС» и её семантическая интерпретация;
– теоретико-множественные модели для задачи управления рисками ИБ ИС;
– теоремы о полноте квазиметрического пространства информационных систем, о существовании в нем не обязательно единственной неподвижной точки; утверждения о существовании минимального риска ИБ для ИС, о существовании контрмеры, минимизирующей риск ИБ;
– методика нечеткой оценки рисков ИБ для ИС и управления ими;
– комплекс программ, предназначенный для моделирования ИС организаций, автоматизации процесса оценки рисков ИБ в нечетких условиях, а также формирования рекомендаций по управлению ими.

Структура и объём диссертации. Диссертация изложена на 185 страницах машинописного текста, содержит 46 рисунков, 13 таблиц, состоит из введения, четырёх глав, заключения, списка использованной литературы из 64 наименований на 6 страницах и 3 приложений на 40 страницах.

Сведения о личном вкладе автора. Разработана концептуальная модель предметной области «Управление рисками ИБ ИС». Разработаны теоретико-множественные модели для задачи управления рисками ИБ ИС. Разработана методика нечеткой оценки и управления рисками ИБ для ИС. Обосновано качество разработанной методики через определение устойчивости модели ИС. Реализован комплекс программ для моделирования ИС, оценки и управления рисками ИБ в нечетких условиях. Проведены экспериментальные исследования методики и работы комплекса программ.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулированы цели и задачи, приведено краткое содержание диссертационной работы.

В первой главе проведен анализ предметной области «Управление рисками ИБ ИС». Исследованы современная российская и международная нормативные базы, а также практика оценки и управления рисками в области ИБ. Отмечено, что

для решения задачи оценки и управления рисками ИБ ИС часто используются экспертные методы, где особенностями оценки факторов риска ИБ являются нечеткость и качественность оцениваемых свойств элементов информационных систем. Отмечена необходимость создания ЭПК для автоматизации процедур оценки рисков ИБ и выдачи рекомендаций по управлению ими. Поставлены основные задачи, решаемые в данной диссертации.

Ключевыми понятиями предметной области «Управление рисками ИБ ИС» являются понятия информационной системы, информационного ресурса, угрозы, уязвимости, контрмеры, риска ИБ.

Под ***риском ИБ*** понимается функция вероятности (P) реализации отдельным источником угрозы (T) отдельной потенциальной уязвимости (V) и результирующего влияния (I) этого враждебного события на организацию или индивида. Формально функция оценки риска записывается в виде $Risk = R(P(T, V), I)$. Исходя из этого, основными факторами риска ИБ считаются вероятность реализации инцидента и его результирующее влияние (ущерб).

Процесс управления рисками ИБ ИС включает в себя следующие этапы.

1. Анализ рисков ИБ (их идентификация).
2. Оценка рисков ИБ по некоторой методике.
3. Снижение рисков ИБ до приемлемого уровня путем введения контрмер.

Взаимодействие указанных этапов между собой, в процессе управления рисками ИБ, представлено в функциональной модели, изображенной на рис. 1.

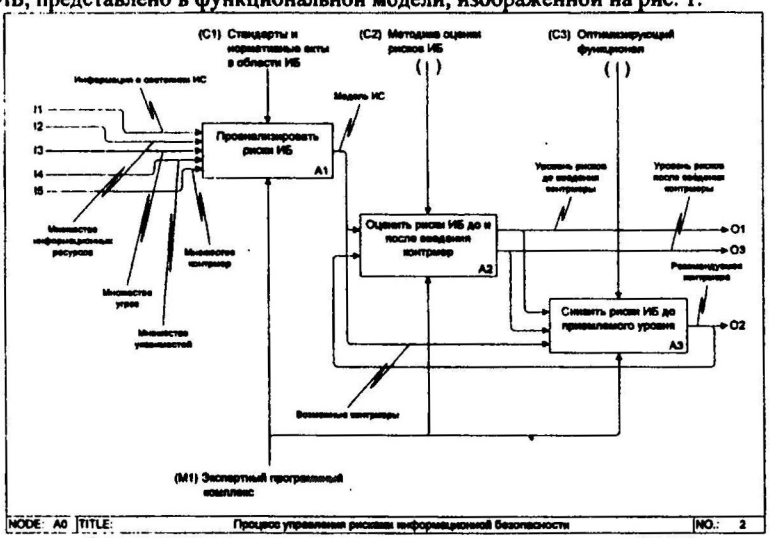

Рис. 1. Функциональная модель процесса управления рисками ИБ ИС

Особенностями любой ИС является наличие в ней элементов, подверженных риску, например, информационные серверы, линии связи и средства маршрутизации, базы данных и иная ценная информация, а также наличие отношений между ними, влияющих на уровень риска ИБ ИС. Учитывая это, а также проводя оценку рисков ИБ экспертным путем на порядковых шкалах, поставим формально задачу оценки и управления рисками ИБ информационных систем следующим образом.

Входные данные.

1. Задано множество ИС $I = \{IS_i\}_{i=\overline{1,m}}$ – объектов оценивания.
2. Каждая из информационных систем IS_i включает в себя различные классы элементов $M_k \subset E$, связанных между собой отношениями из множества R.
3. Задано множество шкал S, включающее в себя множества: S_e – шкалы для оценки свойств элементов $e_j \in E$, S_r – шкалы для оценки рисковых характеристик ИС, причем $S = S_e \cup S_r$, $S_e, S_r \neq \varnothing$.
4. Задано множество контрмер $C = \{CM_q\}_{q=\overline{1,l}}$, которые могут быть использованы для уменьшения рисков ИБ.

Требуется.

1. Построить формально обоснованное отображение $Risk: I \to S_r$ (для задачи оценки риска ИБ), ставящее в соответствие каждой из ИС IS_i, $i = \overline{1,m}$, уровень риска на шкале S_r.
2. Построить формально обоснованное отображение $Manage: I \times S_r \to C$ (для задачи управления риском ИБ), ставящее в соответствие каждой из ИС IS_i, $i = \overline{1,m}$, множество контрмер из C, уменьшающих уровень риска ИБ на основании заданных ограничений.

Проведен анализ существующих методик оценки и управления рисками ИБ ИС. Были выделены следующие свойственные им основные недостатки.

1. Теоретически не обоснована формализация понятий управления рисками ИБ.
2. Отсутствует универсальность применения методик для ИС произвольного вида.
3. Методики не основываются на моделях ИС, не учитывают их компоненты и связи между ними.
4. Качественные методики оценки рисков ИБ не обладают достаточной точностью получаемых результатов, а количественные методики сводятся к вероятностным оценкам, что в отсутствие статистики инцидентов не дает достоверных результатов.
5. Формируемые экспертами оценки факторов риска ИБ имеют нечеткий характер в силу неполноты и неточности доступной информации.

Таким образом, актуальна разработка методики оценки и управления рисками ИБ ИС, лишенной представленных выше недостатков и способной работать с нечеткими оценками эксперта.

Во второй главе создана концептуальная модель предметной области на основе ER-диаграмм типов. В рамках концептуальной модели проведена формализация основных понятий предметной области. Определено, что любая ИС характеризуется своими элементами, описываемыми в терминах разработанной концептуальной модели. Сформулированы и доказаны теоремы о полноте квазиметрического пространства информационных систем, о существовании в нем не обязательно единственной неподвижной точки, утверждения о существовании минимального риска ИБ для любой ИС, а также о существовании конечного набора контрмер, сводящих риск ИБ к минимальному уровню.

Концептуальное моделирование предметной области «Управление рисками ИБ ИС» осуществлялось в рамках теории категорий и функторов. Введены следующие типы объектов.

Базовый универсальный тип: $t_U = \text{UNIOBJECT} \in \text{Type}$. Он позволяет в концептуальной модели определять факт существования объекта. Специальные типы: $t_{Scale} = \text{SCALE}$ – измерительная шкала; $t_{IS} = \text{INFORMATION SYSTEM}$ – ИС; $t_{CoSys} = \text{COSYSTEM}$ – ИС после введения контрмер; $t_{Res} = \text{RESOURCE}$ – ресурсы;

t_T = THREAT – угрозы; t_V = VULNERABILITY – уязвимости; t_{CM} = COUNTERMEASURE – контрмеры; t_{Risk} = RISK – множество уровней риска ИБ. Дополнительные типы: t_{Sit} = SITUATION – отношения или операции между остальными объектами; t_{Name} = NAME – тип объектов, позволяющий описывать понятия предметной области на формальном языке; t_{Indef} = INDEFOBJECT – тип неопределенных объектов; t_{Def} = DEFOBJECT – тип определенных объектов.

Определение 1. Пусть $E = \{e_1, \ldots, e_n\} \subseteq \{t_U\}$ множество элементов ИС. Тогда под ***информационной системой*** порожденной элементами множества E будем понимать произвольное подмножество IS булеана P(E), то есть $IS \subseteq P(E)$.

Для нечеткой оценки свойств объектов предлагается среди измерительных шкал $\{t_{Scale}\}$ ввести упорядоченные F-множества нечетких переменных, характеризующие свойства других объектов: $FP_1, FP_2, \ldots$, названные далее нечеткими шкалами. Тогда нечеткие свойства объекта будут измеряться с помощью вектора нечетких базовых характеристик $fp = (fp_1, \ldots, fp_n)$, $fp_i \in FP_i$, $i = \overline{1, n}$, с функциями принадлежности $\mu_{fp_i}(x)$, $x \in \sigma(fp_i)$, где $\sigma(fp_i)$ – несущее множество для функции принадлежности свойства fp_i.

Модель информационного ресурса r для задач оценки и управления рисками ИБ представим в виде вектора нечетких базовых характеристик $fp_{Res}(r)$:

$$fp_{Res}(r) = (\text{Value}, CL, (AL_i), L_C, L_I, L_A, cv, \text{Damage}(r)), \quad (1)$$

где Value – ценность ресурса r, CL – уровень критичности ресурса r, (AL_i) – вектор уровней воздействия ресурса r на связанные с ним ресурсы ИС, L_C, L_I, L_A – уровни конфиденциальности, целостности и доступности, cv – относительная характеристика ценности ресурса r, Damage(r) – оценка ущерба для ресурса.

Любую угрозу ИБ наделим измеримыми свойствами «Потенциальная стоимость реализации угрозы на ресурс» ($Price_i$), «Предпочтение выбора угрозы по стоимости» ($Select_j$), «Уровень возможности реализации угрозы» ($Opportunity_k$). **Модель угрозы** t представим вектором нечетких базовых характеристик $fp_T(t)$:

$$fp_T(t) = ((Price_i), (Select_j), (Opportunity_k)). \quad (2)$$

Любая угроза ИБ для информационной системы потенциально увеличивает риск ИБ: $\forall th \in \{t_T\}\ \text{Risk}(IS \cup th) \geq \text{Risk}(IS)$.

Любую уязвимость ИС наделим измеримым свойством «Уровень простоты использования уязвимости» (EL_i). **Модель уязвимости** v представим вектором нечетких базовых характеристик $fp_V(v)$:

$$fp_V(v) = (EL_i). \quad (3)$$

Любая пара (угроза ИБ, уязвимость) для некоторой ИС обязательно увеличивает риск ИБ: $\forall th \in \{t_T\}\ \forall v \in \{t_V\}\ \text{Risk}(IS \cup (th, v)) > \text{Risk}(IS)$.

Любую контрмеру наделим измеримыми свойствами «Ценность» Value, «Относительная характеристика ценности» cv, «Эффективность введения контрмеры» Eff(cm, IS). **Модель контрмеры** с представим вектором нечетких базовых характеристик $fp_{CM}(c)$:

$$fp_{CM}(c) = (\text{Value}, cv, \text{Eff}(cm, IS)). \quad (4)$$

Любая контрмера для некоторой ИС обязательно уменьшает её риск ИБ: $cm \in \{t_{CM}\} \Leftrightarrow \text{Risk}(IS(E) \cup cm) < \text{Risk}(IS(E))$.

Нечеткой шкалой рисков ИБ названа шкала $RS_F = \{r \in \{t_{Risk}\} \mid r \in [0, 1]\} \subset RS$.

Введены операции над рисками и над ИС: $0(0)$, $1(0)$, $'(1)$, $\cup(2)$, $\cap(2)$. Введение данных операций позволяет определить в $\{t_{IS}\}$ и RS_F структуры булевых алгебр, которые образуют категорию. Таким образом, $\{t_{IS}\}$ и RS_F образуют категорию информационных систем и категорию рисков ИБ.

Функтором оценки риска ИБ названо отображение, сопоставляющее любым объектам IS из категории $\{t_{IS}\}$ объект Risk(IS(E)) из категории RS_F: Risk: $\{t_{IS}\} \to RS_F$. Значение $r = \text{Risk}(IS(E)) \in RS_F$ называется уровнем риска ИБ. Число $s \in RS_F$, такое, что $s = 1 - r \in RS_F$, $r \in RS_F$, называется уровнем ИБ.

Для исследования вопроса «близости» двух ИС в смысле их рисков ИБ введена квазиметрика риска как функция $\text{ModIS}: \{t_{IS}\} \times \{t_{IS}\} \to RS_F$:

$\forall IS_1, IS_2 \in \{t_{IS}\}$ $\text{ModIS}(IS_1, IS_2) = |\text{Risk}(IS_1) - \text{Risk}(IS_2)|$.

Доказаны следующие утверждения и теоремы.

Теорема 1. Квазиметрическое пространство $<\{t_{IS}\}, \text{ModIS}>$ является полным.

Теорема 2. Всякое сжимающее отображение $f: \{t_{IS}\} \to \{t_{IS}\}$, определенное в полном квазиметрическом пространстве $<\{t_{IS}\}, \text{ModIS}>$, имеет неподвижную точку IS, не обязательно единственную, такую что $f(IS) = IS$.

Утверждение 1. О существовании минимального риска ИБ для ИС.

Для любой ИС $IS(E) \in \{t_{IS}\}$ существует единственный уровень риска $r_{min} \in SR_F$ такой, что для любой контрмеры $c \in \{t_{CM}\}$, уровень риска ИБ для ИС с введенной контрмерой не меньше r_{min}.

Утверждение 2. О существовании контрмеры, минимизирующей риск.

Для любой ИС $IS(E) \in \{t_{IS}\}$ существует контрмера $c \in \{t_{CM}\}$ такая, что уровень риска ИБ для ИС с введенной контрмерой равен r_{min}.

Функцией оценки эффективности контрмеры для заданной ИС $IS(E) \in \{t_{IS}\}$ называется отображение, сопоставляющее любой паре (cm, IS) объектов типов t_{CM} и t_{IS} уровень эффективности на шкале $ES = [0, 1]$: $\text{Eff}: \{t_{CM}\} \times \{t_{IS}\} \to ES$.

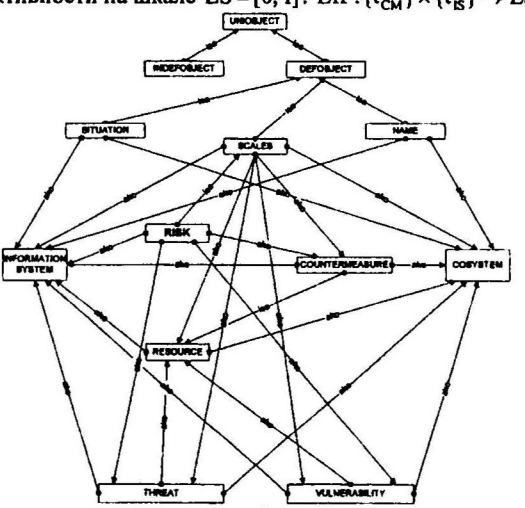

Рис. 2. Концептуальная модель предметной области заданная в виде ER-диаграммы типов

Для создания концептуальной модели предметной области «Управление рисками ИБ ИС», введены отношения: равенства (=), isa (is a – «относится к»), ako (a kind of – «является разновидностью») на множестве типов Type. Кроме этого, над типами введены операции объединения, пересечения, разности, дополнения. Концептуальная модель в виде ER-диаграммы типов объектов представлена на рис. 2.

В третьей главе разработаны алгоритмы для оценки свойств элементов ИС и согласования мнений экспертов. Предложены нечеткие шкалы для оценки свойств элементов ИС. Разработана методика для нечеткой оценки и управления рисками ИБ. Введены функции оценки риска ИБ и управляющего воздействия. Исследованы вопросы адекватности и эффективности разработанной методики. Схема алгоритма разработанной методики управления рисками ИБ представлена на рис. 3.

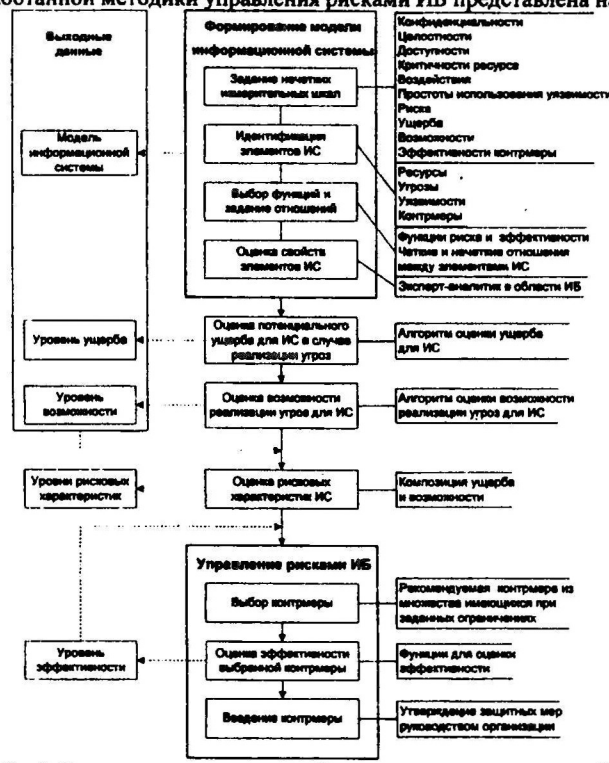

Рис.3. Схема алгоритма для нечеткой оценки и управления рисками ИБ

Для оценки уровня риска ИБ предлагается следующая теоретико-множественная **модель информационной системы**:

$$IS = \{R, T, V, C, Rel\}, \qquad (5)$$

где $R = \{r_k \mid r_k \in (t_{Res}), k = \overline{1, l}\}$ – множество ресурсов r_k, $T = \{t_j \mid t_j \in (t_T), j = \overline{1, n}\}$ – множество угроз t_j, $V = \{v_i \mid v_i \in (t_V), i = \overline{1, m}\}$ – множество уязвимостей v_i, $C = \{c_q \mid c_q \in (t_{CM}), q = \overline{1, p}\}$ – множество контрмер c_q, Rel – множество отношений между элементами ИС.

Для оценки свойств элементов ИС и уровней рисковых характеристик введены нечеткие шкалы FP определяющие следующие уровни свойств объектов.

1. Конфиденциальность FP_C.
2. Целостность FP_I.
3. Доступность FP_A.
4. Критичность ресурса FP_{CR}.
5. Воздействие элемента FP_{Affect}.
6. Простота использования уязвимости FP_{Easy}.
7. Риск ИБ FP_{Risk}.
8. Ущерб для ИС FP_{Damage}.
9. Возможность реализации угрозы $FP_{Opportunity}$.
10. Эффективность контрмеры FP_{Eff}.

На заданных нечетких шкалах принимают свои значения лингвистические переменные L_C, L_I, L_A, CL, AL, EL, RL, DL, OL, EffL соответственно. Рекомендуемые по умолчанию несущие множества выбраны, опираясь на исследования функции желательности Харрингтона. Пример задания несущих множеств на отрезке [0, 1] и функций принадлежности для нечеткой шкалы FP_{CR} представлен ниже (рис. 4). Аналогичным образом определены все 10 нечетких шкал.

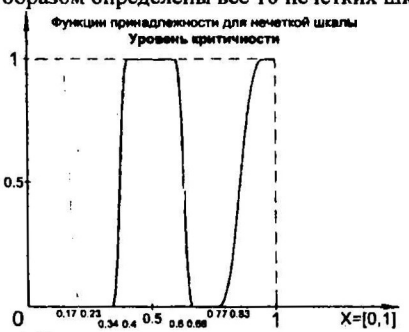

Рис. 4. Нечеткая шкала FP_{CR} «Критичность ресурса»

FP_{CR} = {Минимальный(Min), Низкий(H), Средний(C),
Высокий(B), Максимальный(Max)}

CL = Min, $\sigma_1^{FP_{CR}}(CL) = [0, 0.23]$, $\mu_1^{FP_{CR}}(x) = \mu_{CL}^4(x,\ 8, 20, 0)$.

CL = H, $\sigma_2^{FP_{CR}}(CL) = [0.17, 0.4]$, $\mu_2^{FP_{CR}}(x) = \mu_{CL}^2(x,\ 0.17, 0.23, 0.34)$.

CL = C, $\sigma_3^{FP_{CR}}(CL) = [0.34, 0.66]$, $\mu_3^{FP_{CR}}(x) = \mu_{CL}^2(x,\ 0.34, 0.4, 0.6)$.

CL = B, $\sigma_4^{FP_{CR}}(CL) = [0.6, 0.83]$, $\mu_4^{FP_{CR}}(x) = \mu_{CL}^2(x,\ 0.6, 0.66, 0.77)$.

CL = Max, $\sigma_5^{FP_{CR}}(CL) = [0.77, 1]$, $\mu_5^{FP_{CR}}(x) = \mu_{CL}^1(x,\ 0.77, 0.95)$.

Для согласования экспертных оценок, определенных в виде значений одной нечеткой шкалы, использовался следующий подход.

Пусть $B_1, \ldots, B_k$ – нечеткие множества заданные k экспертами с указанием функций принадлежности $\mu_{B_1}(x), \ldots, \mu_{B_k}(x)$ и несущих множеств $\sigma(B_1), \ldots, \sigma(B_k)$, $x \in \sigma(A)$, характеризующие их субъективное восприятие нечеткого понятия A.

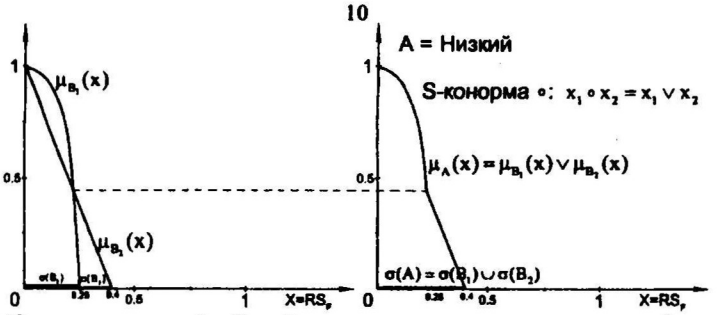

Рис. 5. Нечеткое множество A = Низкий, определенное путем согласования мнений экспертов

Определение 2. ***Согласованное нечеткое множество A*** (рис. 5) – это нечеткое множество, функция принадлежности которого – результат нечеткого объединения $\mu_{B_1}(x), \ldots, \mu_{B_k}(x)$ с помощью S-конормы $\circ$, а несущее множество – результат объединения $\sigma(B_1), \ldots, \sigma(B_k)$:

$$A = <\mu_A(x), \sigma(A)>,\ \mu_A(x) = \sum_{j=1}^{k} {}^{\circ}\mu_{B_j}(x),\ \sigma(A) = \bigcup_{j=1}^{k} \sigma(B_j).$$

Введены следующие четкие отношения из множества Rel между элементами информационной системы.

1. Отношение связи ресурсов: $Rel_1 \subset R \times R$.

$$Rel_1 = (Connect_R(r_\alpha, r_\beta))_{1\times 1},\ Connect_R(r_\alpha, r_\beta) = \begin{cases} 1, \text{ если } r_\alpha \text{ и } r_\beta \text{ связаны,} \\ 0, \text{ в противном случае.} \end{cases} \quad (6)$$

2. Отношение связи угроз с ресурсами: $Rel_2 \subset T \times R$.

$$Rel_2 = (Connect_T(t_\alpha, r_\beta))_{n\times 1},\ Connect_T(t_\alpha, r_\beta) = \begin{cases} 1, \text{ если } t_\alpha \text{ и } r_\beta \text{ связаны,} \\ 0, \text{ в противном случае.} \end{cases} \quad (7)$$

3. Отношение связи уязвимостей с угрозами: $Rel_3 \subset V \times T$.

$$Rel_3 = (Connect_V(v_\alpha, t_\beta))_{m\times n},\ Connect_V(v_\alpha, t_\beta) = \begin{cases} 1, \text{ если } v_\alpha \text{ и } t_\beta \text{ связаны,} \\ 0, \text{ в противном случае.} \end{cases} \quad (8)$$

4. Отношение связи контрмер с уязвимостями: $Rel_4 \subset C \times V$.

$$Rel_4 = (Connect_C(c_\alpha, v_\beta))_{p\times m},\ Connect_C(c_\alpha, v_\beta) = \begin{cases} 1, \text{ если } c_\alpha \text{ и } v_\beta \text{ связаны,} \\ 0, \text{ в противном случае.} \end{cases} \quad (9)$$

Введены следующие нечеткие отношения из множества Rel между элементами информационной системы, для «взвешивания» связанных элементов ИС.

1. Отношение критичности ресурса $rcr \subset R \times IS$, задаваемое на нечеткой шкале $FP_{CR}: \mu_{rcr}: R \times IS \to FP_{CR}$.

2. Отношение индуцирования ущерба $dir \subset R \times R$, задаваемое на нечеткой шкале $FP_{Affect}: \mu_{dir}: R \times R \to FP_{Affect}$.

3. Отношение простоты использования уязвимости $veur \subset V \times T$, задаваемое на нечеткой шкале $FP_{Easy}: \mu_{veur}: V \times T \to FP_{Easy}$.

Основными факторами риска ИБ для ИС являются ущерб, наносимый ИС в случае реализации некоторой угрозы, и возможность реализации этой угрозы.

Обозначим через $\circ$ – S-конорму, через * – T-норму, через $\neg$ – нечеткое отрицание – это некоторые операции композиции над нечеткими величинами, являющиеся обобщениями логических операций ИЛИ, И, НЕ соответственно.

При расчете **потенциального ущерба** для ИС используются нечеткие уровни конфиденциальности $L_C \in FP_C$, целостности $L_I \in FP_I$, доступности $L_A \in FP_A$, критичности $CL \in FP_{CR}$, воздействия $AL \in FP_{Affect}$ ресурса на ущерб для других ресурсов ИС. Их четкие значения, $Defuz(L_C)$, $Defuz(L_I)$, $Defuz(L_A)$, $Critical(r)$, $Affect(r_i, r_j)$ соответственно, получены дефазификацией нечетких величин методом центра тяжести. Введены следующие рисковые характеристики ИС.

Ценность CV информационной системы:

$$CV = \sum_{k=1}^{l} Value(r_k),$$

где $Value(r_k)$ – ценность ресурса r_k.

Относительная характеристика ценности $cv(r)$ ресурса r:

$$cv(r) = \frac{Value(r)}{CV}.$$

Уровень ущерба $Damage(r)$ по ресурсу r:

$$Damage(r) = \sum_{k=1}^{l}{}^{\circ}(Connect_R(r, r_k) * cv(r) * Critical(r) * Affect(r, r_k)).$$

Уровень потенциального ущерба Damage для ИС:

$$Damage = \sum_{k=1}^{l}{}^{\circ} Damage(r_k). \qquad (10)$$

Если определены уровни L_C, L_I, L_A, то по каждому из свойств конфиденциальности, целостности, доступности:

$$Damage_{C,I,A}(r) = Defuz(L_{C,I,A}) * Damage(r),\ Damage_{C,I,A} = \sum_{k=1}^{l}{}^{\circ} Damage_{C,I,A}(r_k).$$

При расчете **возможности реализации угроз** на ИС используются:

– нечеткий уровень простоты использования $EL \in FP_{Easy}$ уязвимости v при реализации угрозы t на ресурс r, определяемый экспертным путем, четкое значение $Easy(v, t)$ для которого получено как результат дефазификации EL;

– потенциальная стоимость $Price(t, r)$ реализации угрозы t на ресурс r, определяемая экспертным путем;

– предпочтение выбора по стоимости $Select(t, r)$ угрозы t на ресурс r, оценка которого осуществляется согласно выражению:

$$Select(t, r) = \neg\left(\frac{Price(t, r)}{\max\limits_{j} Price(t_j, r)}\right),\ \forall r \exists j\ Price(t_j, r) > 0.$$

Возможность $Opportunity(t, r)$ реализации угрозы t на ресурс r:

$$Opportunity(t, r) = Select(t, r) * \sum_{i=1}^{m}{}^{\circ}(Connect_V(v_i, t) * Easy(v_i, t)).$$

Возможность Opportunity реализации всех угроз на ИС:

$$Opportunity = \sum_{k=1}^{l}{}^{\circ} \sum_{j=1}^{n}{}^{\circ}(Connect_T(t_j, r_k) * Opportunity(t_j, r_k)). \qquad (11)$$

Общий нечеткий риск ИБ для информационной системы:

$$\mathrm{Risk(IS)} = \mathrm{Damage}^{*}\mathrm{Opportunity}. \qquad (12)$$

Остаточный риск ИБ для ИС – это общий нечеткий риск, рассчитанный после введения некоторой контрмеры cm. Обозначим его через r_{new}, а риск до введения контрмеры – через r_{old}. Контрмера «закрывает» связанные уязвимости, то есть те, для которых $\mathrm{Connect}_C(c_q, v) = 1$, $q = \overline{1, p}$, что уменьшает возможность реализации угроз или позволяет уменьшить возможный ущерб для информационной системы. При этом в соответствующих формулах исчезают некоторые слагаемые.

Были определены способы оценки уровней частных рисков ИБ для ИС, с учетом различных требований экспертов в области ИБ к проводимой оценке. Представлены следующие оценки риска ИБ до и после введения контрмер: интервальная, средние, лингвистическая на шкале FP_{Risk}. Введены функции конвертирования значений риска $r \in [0, 1]$ на различные шкалы.

Относительная оценка эффективности Eff(cm, IS) введения контрмеры cm:

$$\mathrm{Eff(cm, IS)} = (r_{old} - r_{new}) / r_{old}. \qquad (13)$$

Задача управления рисками поставлена как задача минимизации целевой функции $\mathrm{Risk(IS(E))} \to \min$.

Обозначим множество всех оптимальных, в некотором смысле, решений задачи минимизации риска для информационной системы $IS = IS(E)$ через $\mathrm{Opt(IS)} \subseteq C$.

Под **управляющим воздействием** Manage(IS) на ИС будем понимать функционал $\mathrm{Manage}: \{t_{IS}\} \to \mathrm{Opt(IS)}$, определяющий выбор и введение одной из контрмер $cm_q \in \mathrm{Opt(IS)}$, $q = \overline{1, p}$.

При решении задачи управления рисками ИБ рассмотрены следующие их **формальные постановки**.

1. Полный перебор возможных для ИС контрмер с выбором наиболее эффективных, сводящих риск к минимальному уровню:

$$cm_q \in \mathrm{Opt(IS)} \Leftrightarrow \mathrm{Risk}(IS \cup cm_q) = r_{min},\ cm_q \in C,\ q = \overline{1, p}.$$

$$\mathrm{Manage}_1(IS) = cm \Leftrightarrow \mathrm{Eff}(cm, IS) \geq \mathrm{Eff}(cm_i, IS)\ \ \forall cm, cm_i \in \mathrm{Opt(IS)}. \qquad (14)$$

2. Выбор контрмеры или нескольких контрмер с минимальной относительной характеристикой ценности и максимальной эффективностью при заданном максимально допустимом уровне остаточных рисков: $risk_{max} = \mathrm{Const}$, $risk_{max} \in RS_F$,

$$cm_q \in \mathrm{Opt(IS)} \Leftrightarrow \begin{cases} cv(cm_q) = \min\limits_i \{cv(cm_i)\}, \\ \mathrm{Eff}(cm_q, IS) \geq \mathrm{Eff}(cm_i, IS), \\ \mathrm{Risk}(IS \cup cm_q) \leq risk_{max},\ \forall cm_q, cm_i \in C,\ i, q = \overline{1, p}. \end{cases}$$

$$\mathrm{Manage}_2(IS) = cm \Leftrightarrow cm \in \mathrm{Opt(IS)}. \qquad (15)$$

3. Выбор контрмеры или нескольких контрмер с минимальным остаточным риском при заданном максимально допустимом уровне относительной характеристики ценности: $cv_{max} = \mathrm{Const}$, $cv_{max} \in [0, 1]$,

$$cm_q \in \mathrm{Opt(IS)} \Leftrightarrow \begin{cases} \mathrm{Risk}(IS \cup cm_q) \leq \mathrm{Risk}(IS \cup cm_i), \\ cv(cm_q) \leq cv_{max},\ \ \forall cm_q, cm_i \in C,\ i, q = \overline{1, p}. \end{cases}$$

$$\mathrm{Manage}_3(IS) = cm \Leftrightarrow cm \in \mathrm{Opt(IS)}. \qquad (16)$$

4. Выбор контрмеры или нескольких контрмер с минимальной относительной характеристикой ценности при заданном максимально допустимом уровне остаточных рисков: $risk_{max} = Const$, $risk_{max} \in RS_F$,

$$cm_q \in Opt(IS) \Leftrightarrow \begin{cases} cv(cm_q) \le cv(cm_i), \\ Risk(IS \cup cm_q) \le risk_{max}, \quad \forall cm_q, cm_i \in C, \; i,q = \overline{1,p}. \end{cases}$$

$$Manage_4(IS) = cm \Leftrightarrow cm \in Opt(IS). \qquad (17)$$

Управляющие воздействия Manage(IS) являются сжимающими отображениями. Согласно теореме 2, множество оптимальных и неулучшаемых альтернатив Opt(IS), может быть как пустым, так и содержать более одного элемента.

Для обоснования качества получаемых результатов большое значение имеет проверка устойчивости построенной модели ИС.

Определение 3. Будем считать, что модель (5) ***устойчива*** в смысле непрерывности по квазиметрике ModIS её функции Risk(IS(E)) как по каждой, так и по совокупности используемых в ней переменных, то есть:

$$\forall \varepsilon > 0 \; \exists \delta > 0 \;\; |e_1 - e_1'| < \delta \wedge \ldots \wedge |e_n - e_n'| < \delta \Rightarrow ModIS(IS(E),\ IS(E')) < \varepsilon,$$

где $E = \{e_1, e_2, \ldots, e_n\}$, $E' = \{e_1', e_2', \ldots, e_n'\}$ – элементы ИС с оценкой свойств до и после внесения малых изменений в их значения.

Все учитываемые в формулах (10)-(12) параметры вычисляются как значения непрерывных функций дефазификации от непрерывных функций принадлежности. Также в них используются бинарные операции, непрерывные по обоим аргументам. Поэтому, малые изменения в значениях различных параметров и риск-факторов в этих формулах приведут к малым изменениям значения риска ИБ, то есть модель (5) устойчива по своим параметрам.

Показано, что порядок роста сложности алгоритма расчета уровня риска, согласно выражению (12), равен $O(\max\{l^2, lmn\})$, где параметры l, m, n – количество ресурсов, уязвимостей и угроз соответственно.

Таким образом, эффективность процесса управления рисками ИБ определяется:

- теоретической обоснованностью разработанных моделей и алгоритмов;
- полнотой охвата элементов информационных систем;
- устойчивостью используемой модели информационной системы;
- учетом нечетких знаний эксперта;
- наличием процедуры снижения рисков ИБ;
- автоматизацией процесса управления рисками ИБ.

В четвёртой главе исследованы вопросы разработки баз знаний для ЭПК, выбора способа представления знаний, реализации разработанных моделей. Представлена модульная структура ЭПК. Рассмотрены вопросы моделирования ИС в ЭПК. Проведены экспериментальные исследования разработанной методики.

Для реализации методики разработан экспертный программный комплекс, модульная структура которого представлена на рис. 6. Комплекс реализует последовательность шагов, представленного на рис. 3 алгоритма.

Разработанная методика для нечеткой оценки рисков ИБ исследована на примере ИС, представленной на рис. 7. Для первой группы экспериментальных расчетов выбраны двойственные нечеткие операции * – граничное произведение $x_1 \circ x_2$ и $\circ$ – граничная сумма $x_1 \oplus x_2$. Для второй – двойственные нечеткие операции * – алгебраическое произведение $x_1 \cdot x_2$ и $\circ$ – алгебраическая сумма $x_1 \dot{+} x_2$. В качестве нечеткого отрицания выбрана операция «вычитание из единицы».

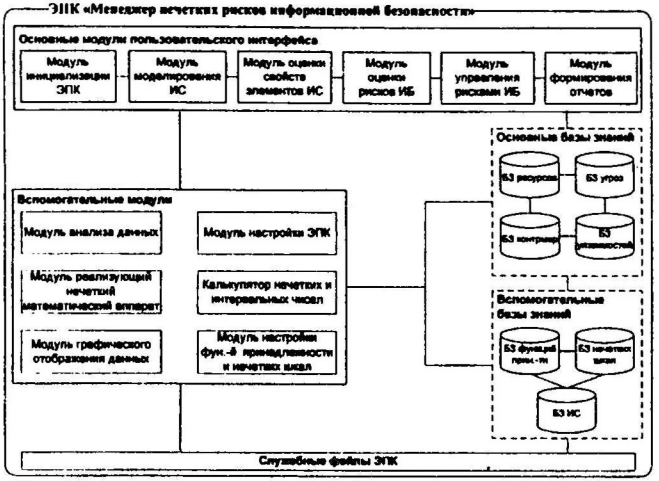

Рис. 6. Общая структура программных модулей комплекса для управления рисками ИБ

Шаг 0. Описание информационной системы

Информационная система представляет собой локальную сеть одного из отделов организации, состоящую из одного АРМ администратора сети, двух рабочих мест, почтового сервера и коммутатора, через который нет выхода во внешнюю сеть WAN. Формализация процесса анализа, оценки и управления рисками ИБ проведена с применением ЭПК «Менеджер нечетких рисков ИБ», в частности, используя модуль «Калькулятор нечетких и интервальных чисел». ЭПК позволяет проводить как количественную, так и качественную оценку рисков.

Рис. 7. Схема информационной системы – фрагмент локальной вычислительной сети

Шаг 1. Задание нечетких измерительных шкал

Задаются десять нечетких шкал, представленных выше. Определяется вид составляющих их функций принадлежности.

Шаг 2. Идентификация элементов информационной системы

Для формирования модели (5), исследуемой информационной системы, составляются индексированные списки ресурсов, угроз, уязвимостей и контрмер.

1. **Ресурсы** $r_k \in R$, $k = \overline{1,6}$:

Индекс	Описание
r_1	Почтовый сервер
r_2	Коммутатор
r_3	АРМ1 администратора
r_4	АРМ2 пользователя
r_5	АРМ3 пользователя
r_6	Линия связи

2. **Угрозы** $t_j \in T$, $j = \overline{1,7}$:

Индекс	Описание
t_1	Получение нарушителем несанкционированного физического доступа к элементам информационной системы
t_2	Получение нарушителем несанкционированного удаленного сетевого доступа к элементам информационной системы
t_3	Несанкционированная модификация информации в системе электронной почты
t_4	Компрометация конфиденциальной информации (ключей доступа к почтовому серверу) сотрудниками организации
t_5	Удаленные DoS-атаки на элементы информационной системы
t_6	Сбой сетевых настроек элементов информационной системы
t_7	Физическое уничтожение ресурсов информационной системы

3. **Уязвимости** $v_i \in V$, $i = 1,9$:

Индекс	Описание
v_1	Отсутствие регламента доступа в помещения с ресурсами
v_2	Отсутствие систем наблюдения за ресурсами
v_3	Отсутствие авторизации на внесение изменений в систему электронной почты
v_4	Отсутствие регламента работы с системой криптозащиты электронной почты
v_5	Отсутствие соглашений с сотрудниками о сохранении конфиденциальности ключевой информации
v_6	Возможность распределения ключевой информации между несколькими сотрудниками организации
v_7	Отсутствие аппаратного межсетевого экрана (МЭ) для ограничения доступа к подсети через коммутатор
v_8	Отсутствие системы обнаружения вторжений (IDS) на АРМ1 администратора
v_9	Отсутствие антивирусного и антишпионского ПО в ИС

4. **Контрмеры** $c_q \in C$, $q = 1,8$:

Индекс	Описание
c_1	Создание политики безопасности организации регламентирующей правила физического и сетевого доступа сотрудниками к ресурсам информационной системы
c_2	Внедрение системы физического контроля и разграничения доступа при помощи систем электронных пропусков
c_3	Внедрение инфраструктуры открытых ключей (PKI) для разграничения сетевого доступа к ресурсам информационной системы
c_4	Подписание сотрудниками при приеме их на работу соглашения о сохранении конфиденциальности ключевой информации
c_5	Установка аппаратного МЭ на коммутаторе
c_6	Установка IDS на АРМ1 администратора
c_7	Установка антивирусного и антишпионского ПО в информационной системы
c_8	Физическая защита ИС силами вневедомственной охраны

Шаг 3. Выбор функций и задание отношений

Множество четких отношений Rel_i, $i = \overline{1,4}$ между элементами ИС, задается функциями связей $Connect_R(r_1, r_2)$, $Connect_T(t, r)$, $Connect_V(v, t)$, $Connect_C(c, v)$ при помощи бинарных матриц (6)-(9). Граф связей изображен на рис. 8. Связанные элементы ИС «взвешены» значениями нечетких отношений критичности ресурса tcr, индуцирования ущерба dir, простоты использования уязвимости veur.

Шаг 4. Оценка свойств элементов информационной системы

Выполняется оценка нечетких характеристик ресурсов, угроз, уязвимостей и контрмер, задаваемых моделями (1)-(4).

Шаг 5. Оценка ущерба для ИС в случае реализации угроз

Оценивается уровень ущерба для ИС по формуле (10).

Шаг 6. Оценка возможности реализации угроз для ИС

Оценивается возможность реализации угроз на ИС по формуле (11).

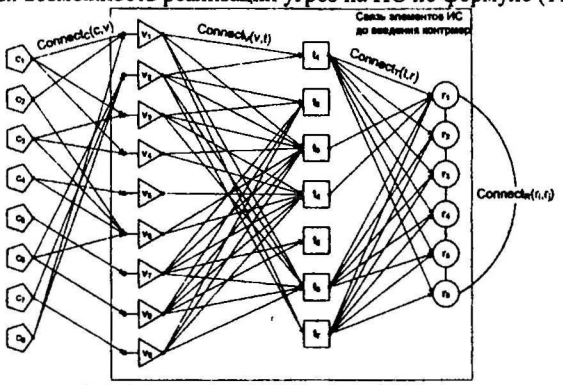

Рис. 8. Схема связей элементов ИС друг с другом

Шаг 7. Оценка рисковых характеристик

Для модели ИС в виде (5) оценивается риск ИБ для ИС по формуле (12):

Risk(IS)	$Risk_C$(IS)	$Risk_T$(IS)	$Risk_A$(IS)
0.95763	0.53632	0.86416	0.90866

Шаги 8, 9, 10. Выбор контрмеры. Оценка ожидаемой эффективности выбранной контрмеры. Введение контрмеры.

Рассчитываются новые (остаточные) риски ИБ для ИС по формуле (12):

c_q / хар-ка	1	2	3	4	5	6	7	8
Damage	0.95763							
Opportunity (новое знач.)	**0.97154**	**0.73310**	**0.71534**	**0.84705**	**0.88981**	**0.87512**	**0.86945**	**0.67891**
r_{new} (остаточный)	**0.93038**	**0.68503**	**0.68503**	**0.81116**	**0.85211**	**0.83804**	**0.83261**	**0.65014**

Рассчитывается ожидаемая эффективность для контрмер по формуле (13):

c_q / хар-ка	1	2	3	4	5	6	7	8
Eff(c, IS)	**0.02846**	**0.28466**	**0.28466**	**0.15295**	**0.11019**	**0.12488**	**0.13055**	**0.32109**

Оптимальные контрмеры выбираются и вводятся согласно формул (14)-(17). Для исследуемой ИС были заданы следующие ограничения на их поиск:

- максимально допустимый уровень остаточных рисков ИБ: 0.7;
- максимально допустимый уровень относительной ценности: 0.07;
- выбран способ управления определяемый функционалом $Manage_3$(IS).

Для выбранного способа управления рисками ИБ получен оптимальный результат в виде контрмеры c_3: $Manage_3(IS) = c_3$ – «Внедрение инфраструктуры открытых ключей (PKI) для разграничения сетевого доступа к ресурсам ИС».

По результатам исследования методики были даны следующие рекомендации. Использовать «более пологие» функции принадлежности для задания нечетких шкал, операции алгебраического произведения и суммы, нечеткого сложения ИЛИ.

В заключении сформулированы научные результаты, полученные в ходе работы над диссертацией, указаны направления дальнейших исследований в предметной области «Управление рисками информационной безопасности ИС».

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ предметной области «Управление рисками информационной безопасности информационных систем». Показана актуальность разработки методики оценки и управления рисками ИБ информационных систем, основанной на формальной модели ИС, учитывающей ее компоненты и связи между ними, а также способной работать с нечеткими оценками факторов риска ИБ.
2. Разработана функциональная модель процесса управления рисками ИБ ИС, а также модель данного процесса в рамках ER-диаграммы типов.
3. Предложен способ формализации понятий и описана семантика предметной области «Управление рисками ИБ ИС» в рамках теории категорий и функторов. Разработаны теоретико-множественные модели для задачи управления рисками ИБ, в частности – модели информационного ресурса, угрозы, уязвимости, контрмеры, информационной системы.
4. Сформированы и доказаны теоремы о полноте введенного квазиметрического пространства информационных систем, о наличии в нем для любого сжимающего отображения не обязательно единственной неподвижной точки. Сформулированы и доказаны утверждения о существовании минимального риска ИБ для ИС и о существовании контрмеры, минимизирующей уровень риска ИБ ИС.
5. Разработана методика оценки и управления рисками ИБ ИС в нечетких условиях. В методике предложены алгоритмы для оценки свойств элементов ИС, осуществлен обоснованный выбор нечетких шкал для оценки свойств элементов ИС, а также предложен метод нечеткого согласования мнений экспертов. Показана устойчивость разработанной модели информационной системы в смысле непрерывности по квазиметрике риска ИБ и оценена сложность разработанного алгоритма оценки уровня риска ИБ выражением $O(\max\{l^2, lmn\})$, где параметры l, m, n – количество ресурсов, уязвимостей и угроз соответственно.
6. Разработан экспертный программный комплекс, позволяющий моделировать ИС организаций, автоматизировать процесс оценки рисков ИБ в нечетких условиях, а также формировать рекомендации по управлению ими. Проведены экспериментальные исследования работы предложенных моделей, методики и алгоритмов на конкретных ИС. Их применение позволило повысить уровень информационной безопасности ИС за счет введения оптимальных контрмер, что для тестовой задачи составило 28.5%. По результатам экспериментов осуществлен обоснованный выбор операций T-норм и S-конорм для разработанной методики нечеткой оценки и управления рисками ИБ ИС.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В научных журналах, рекомендованных ВАК:

1. *Аникин И.В., Гильмуллин Т.М.* Моделирование объектов информационной безопасности для задачи оценки рисков // Научно-технические ведомости СПбГТУ. Информатика. Телекоммуникации. Управление. – 2009. – № 5. – С. 151-155.

В других журналах и материалах научных конференций:

2. *Аникин И.В., Гильмуллин Т.М.* Моделирование проблемной области «Оценка рисков» с помощью фреймовых моделей и семантических сетей // Информационные технологии в науке, образовании: Материалы Всероссийской научной конференции, г. Казань, 30-31 мая 2007 г. – Казань: Изд-во Казан. гос. техн. ун-та, 2007. – С. 537-540.

3. *Аникин И.В., Гильмуллин Т.М.* Подходы к оценке, анализу и управлению рисками информационной безопасности // Инфокоммуникационные технологии глобального информационного общества: Тезисы докладов 5-й ежегодной международной научно-практической конференции, г. Казань, 5-6 сентября 2007 г. – Казань: Изд-во Фолиантъ, 2007. – С. 79-82.

4. *Аникин И.В., Гильмуллин Т.М.* Подходы к оценке, анализу и управлению рисками информационной безопасности // Инфокоммуникационные технологии глобального информационного общества: Сборник докладов 5-й ежегодной международной научно-практической конференции, г. Казань, 5-6 сентября 2007 г. – Казань: Изд-во Фолиантъ, 2007. – С. 42-45.

5. *Гильмуллин Т.М.* Методика управления информационными рисками организации // Инфокоммуникационные технологии глобального информационного общества: Сборник докладов 7-й ежегодной международной научно-практической конференции, г. Казань, 10-11 сентября 2009 г. – Казань: Изд-во «Центр оперативной печати», 2009. – С. 464-468.

6. *Гильмуллин Т.М.* К вопросу о моделировании предметной области «Оценка, анализ и управление рисками в ИБ» // Проблемы техники и технологий телекоммуникаций ПТиТТ-2008: Тезисы докладов 9-й международной научно-технической конференции, г. Казань, 25-27 ноября 2008 г. – Казань: Изд-во Казан. гос. техн. ун-та, 2008. – С. 453-454.

7. *Гильмуллин Т.М.* Методика нечеткой оценки для уровня информационного риска организации // Моделирование, идентификация, синтез систем управления МИССУ'2009: Сборник тезисов Двенадцатой Международной научно-технической конференции, г. Донецк, 16-23 сентября 2009 г. – Донецк: Изд-во ИПММ НАН Украины, 2009. – С. 26-27.

8. *Гильмуллин Т.М.* Определение требований к программному комплексу для управления нечеткими рисками информационной безопасности // XVII Туполевские чтения: Международная молодежная научная конференция, 26-28 мая 2009 года: Труды конференции. Том IV. – Казань: Изд-во Казан. гос. техн. ун-та, 2009. – С. 114-116.

9. *Гильмуллин Т.М.* Развитие методики оценки рисков от Digital Security // XVI Туполевские чтения: Международная молодежная научная конференция, 28-29 мая 2008 года: Труды конференции. Том III. – Казань: Изд-во Казан. гос. техн. ун-та, 2008. – С. 89-90.

10. *Гильмуллин Т.М.* Экспертный программный комплекс для управления рисками информационной безопасности // Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта ISDMCI'2009: Материалы международной научной конференции. Том I., г. Евпатория, 18-22 мая 2009 г. – Херсон: Изд-во ХНТУ, 2009. – С. 255-258.

Формат 60×84 1/16. Бумага офсетная. Печать офсетная.
Печ.л. 1,25. Усл.печ.л. 1,16. Уч.-изд.л. 1,0.
Тираж 110. Заказ Н60.

Типография Издательства Казанского государственного
технического университета
420111 Казань, К. Маркса, 10