На правах рукописи

КУДРЯВЦЕВА Рима Тимиршаиховна

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

(на примере высшего учебного заведения)

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

А В Т О Р Е Ф Е Р А Т

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. Черняховская Лилия Рашитовна
	канд. техн. наук, доц. Дуленко Вячеслав Алексеевич
Ведущая организация	Республиканский научно-технологический и информационный комплекс «Баштехинформ» АН РБ

Защита диссертации состоится 17 октября 2008 г. в 10.00 часов
на заседании диссертационного совета Д-212.288.07
при Уфимском государственном авиационном техническом университете
по адресу: 450000, г. Уфа, ул. К.Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан _____ сентября 2008 г.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Одной из важнейших составляющих успешного развития общества является защищенность его информационных ресурсов. Информация в современном информационном обществе становится одним из ключевых элементов бизнеса, она становится предметом купли-продажи, обладающим стоимостными характеристиками. Любые процессы в финансово-промышленной, политической или социальной сфере сегодня напрямую связаны с информационными ресурсами и использованием информационных технологий.

Современные информационные технологии предлагают неограниченные возможности для развития бизнеса, предоставляя необходимую для принятия решений информацию нужного качества и в нужное время. Информация, критичная для бизнеса, должна быть доступной, целостной и конфиденциальной. В то же время, в связи с возрастающей сложностью информационных систем и используемых в них информационных технологий, возрастает и количество уязвимостей и потенциальных угроз этим системам.

Очевидно, что вопросы информационной безопасности сегодня актуальны не только для правительственных и коммерческих структур. В последнее время в связи с коммерциализацией отечественных вузов и тенденциями выхода российского образования на европейский и мировой рынок образовательных услуг остро стоит вопрос об обеспечении устойчивого функционирования и повышении конкурентоспособности образовательных учреждений.

В соответствии с федеральной программой развития науки и инноваций «Научно-технологическая база России» на 2007-2012 годы планируется развитие ведущих вузов страны не только как крупных учебных, но и как базовых научных центров с привлечением крупного и среднего бизнеса к организации учебного процесса и научных исследований. В связи с этим задачи обеспечения защиты информационных ресурсов образовательного учреждения и связанные с ними вопросы анализа информационных рисков и управления ими приобретают особую актуальность.

Объект исследования – система защиты информации высшего учебного заведения.

Предмет исследования – методическое, алгоритмическое и программное обеспечение системы защиты информации.

Цель и задачи исследования

Целью исследований работы является повышение эффективности управления информационной безопасностью (ИБ) вуза на основе разработки моделей и алгоритмов анализа и управления информационными рисками с использованием технологий когнитивного моделирования.

Для достижения этой цели требуется решить следующие задачи:

1. Провести системный анализ бизнес-процессов вуза как объекта защиты и определить требования к обеспечению информационной безопасности вуза.

2. Разработать комплекс моделей, определяющих основные компоненты информационных рисков вуза (модели угроз, злоумышленников, уязвимостей, ущерба).

3. Разработать алгоритмы анализа и управления информационными рисками вуза с использованием нечетких когнитивных карт.

4. Разработать инструментальные программные средства для оценки уровня информационных рисков вуза и выбора необходимых контрмер для управления информационной безопасностью.

Методы исследования

При решении поставленных в работе задач использовались методы системного анализа, теории когнитивного моделирования, теории графов, нечеткой логики, имитационного моделирования, автоматизированного проектирования информационных систем, а также методы программирования.

Результаты, выносимые на защиту

1. Функциональные и информационные модели бизнес-процессов вуза, определяющие основные требования к его информационной безопасности.

2. Комплекс системных моделей, определяющих основные компоненты информационных рисков вуза.

3. Алгоритмы анализа и управления информационными рисками вуза на основе нечетких когнитивных карт.

4. Программное обеспечение для автоматизации анализа и управления информационными рисками вуза на основе построения нечетких когнитивных карт.

Научная новизна

Научная новизна работы состоит в том, что анализ и управление информационной безопасностью, в отличие от существующих подходов, предложено проводить с помощью построения нечеткой когнитивной карты исследуемого объекта. При этом:

1. Для определения списка концептов, требуемых для исследования, предложено провести системное моделирование бизнес-процессов исследуемого объекта на основе SADT-технологии, которое позволяет выявить взаимосвязи и информационное содержание этих процессов, произвести классификацию основных информационных активов вуза, определить наиболее значимые информационные ресурсы и требуемый уровень их защищенности.

2. Для определения степени влияния концептов друг на друга предложено построение системных моделей, определяющих основные компоненты риска

(модель угроз, злоумышленников, уязвимостей, потенциального ущерба), которые позволяют учесть специфику и сложившийся уровень информационной безопасности вуза и его структурных подразделений, дать более точную оценку угроз на информационную систему вуза.

3. Предложен алгоритм анализа информационных рисков вуза, основанный на использовании математического аппарата нечетких когнитивных карт, позволяющий получить не только качественную, но и количественную оценку влияния различных дестабилизирующих факторов (угроз) на величину потенциального ущерба от действия этих угроз, определить состав необходимых контрмер (средств защиты) для управления информационными рисками с учетом ограничений на выделенные ресурсы, а также эффективность вводимых мероприятий.

Практическая значимость и внедрение результатов работы

Предложенные алгоритмы анализа и управления информационными рисками, основанные на построении нечетких когнитивных карт вуза как для вуза в целом, так и для его структурных подразделений, позволяют определить наиболее уязвимые места информационной системы и выбрать необходимые контрмеры для снижения информационных рисков.

Разработанные инструментальные программные средства для анализа и управления информационными рисками на основе построения нечетких когнитивных карт позволяют автоматизировать процессы когнитивного моделирования и сократить в 1,5…2 раза время оценки рисков и выработки необходимых контрмер по управлению информационной безопасностью вуза. Получены 4 свидетельства РосАПО об официальной регистрации программ для ЭВМ.

Разработанная методика оценки информационных рисков вуза и реализующие ее инструментальные программные средства внедрены в учебный процесс подготовки специалистов по специальности 090104 «Комплексная защита объектов информатизации».

Апробация работы

Основные положения диссертационной работы докладывались и обсуждались на следующих научных конференциях:

– 6-й международной научно-технической конференции «Проблемы техники и технологии телекоммуникаций», Уфа, 2005.

– Международной научно-технической конференции «Информационно-вычислительные технологии и их приложения», Пенза, 2005.

– Второй Международной научно-практической конференции «Исследование, разработка и применение высоких технологий в промышленности», Санкт-Петербург, 2006.

– Российской научно-технической конференции «Мавлютовские чтения», Уфа, 2006.

– XVI Всероссийской научно-методической конференции «Актуальные проблемы качества образования и пути их решения», Москва, 2006.

– VIII Международной научно-практической конференции «Информационная безопасность», Таганрог, 2006.

– Международных научных конференциях «Компьютерные науки и информационные технологии», Карлсруэ, Германия, 2006; Уфа, 2007.

Публикации

Список публикаций по теме диссертации содержит 17 работ, в том числе 13 статей и материалов научно-технических конференций, из них 2 статьи в изданиях из перечня ВАК РФ, 4 свидетельства об официальной регистрации программ для ЭВМ.

Структура и объем работы

Диссертационная работа состоит из введения, четырех глав, заключения, библиографического списка и изложена на 142 страницах машинописного текста. Библиографический список включает 144 наименований литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационной работы, сформулированы цели и задачи исследования.

Первая глава посвящена анализу задачи управления информационной безопасностью организаций (предприятий). Рассмотрены основные законы и стандарты, регулирующие нормативно-правовые вопросы поддержания ИБ на различных уровнях структурной организации общества.

Отмечается, что центральное место при обеспечении режима ИБ в организациях занимает задача анализа информационных рисков и управления ими. Однако известные корпоративные документы по обеспечению режима ИБ не предлагают универсальную методику управления рисками для различных типов организаций ввиду специфики бизнес-процессов каждой организации. Кроме того, существующие подходы не обладают достаточной наглядностью, имеют в основном описательный (качественный) характер и сводятся к формальной проверке выполнения (или невыполнения) требований стандартов по ИБ таких, как ИСО/МЭК 17799, ИСО/МЭК 27001. В данных подходах практически не проработаны вопросы количественной оценки ущерба от воздействия угроз на информационные ресурсы (активы), не производится анализ чувствительности оценок ущерба по отношению к основным дестабилизирующим факторам или уязвимостям, не дается должного обоснования выбору эффективных контрмер для снижения информационных рисков.

Поскольку бизнес-процессы, протекающие в вузе, структура информационных ресурсов и информационных потоков, поддерживающих эти бизнес-

процессы, значительно отличаются от процессов, ресурсов и потоков, характерных для типовой компании (предприятия, организации), то анализ вуза (и в первую очередь, его информационных систем) как объекта защиты с целью выявления основных источников угроз, уязвимостей, защищаемых ресурсов и разработка соответствующих методов и алгоритмов анализа и управления рисками, предназначенных для совершенствования системы управления ИБ вуза и его подразделений, является актуальной задачей.

Во второй главе излагается системный подход к построению системы управления информационной безопасностью вуза. При этом управление ИБ рассматривается как регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании имеющихся средств защиты информации. Система управления информационной безопасностью **(**СУИБ) вуза рассматривается как составная часть системы управления качеством, реализующей цели и требования стандарта ISO 9001, которая в свою очередь, является составной частью системы организационного управления вузом.

Анализ информационных рисков вуза включает в себя следующие основные этапы:

1. Идентификация информационных активов вуза.
2. Определение ценности идентифицированных активов.
3. Идентификация угроз и уязвимостей для идентифицированных активов.
4. Оценка рисков (ущерба) в случае реализации угроз.

В соответствии с данными этапами, в работе анализируются особенности информационной системы вуза, структура его информационных активов и характер информационных потоков, которые являются определяющими при оценке риска. Производится функциональное и информационное моделирование основных бизнес процессов вуза с помощью IDEF- технологий. Целью моделирования является выявление наиболее значимых информационных ресурсов, потеря которых может сказаться на жизнедеятельности вуза, и определение эффективных мер защиты этих ресурсов.

Современный вуз – это многофункциональная сложная иерархическая организационная система, состав бизнес-процессов которой определяется миссией, целями и задачами, поставленными перед вузом. На рис. 1 приведена функциональная модель основных бизнес-процессов вуза. Декомпозиция этой модели позволяет детализировать выполнение перечисленных бизнес-процессов, уточнить их содержание и формы взаимодействия.

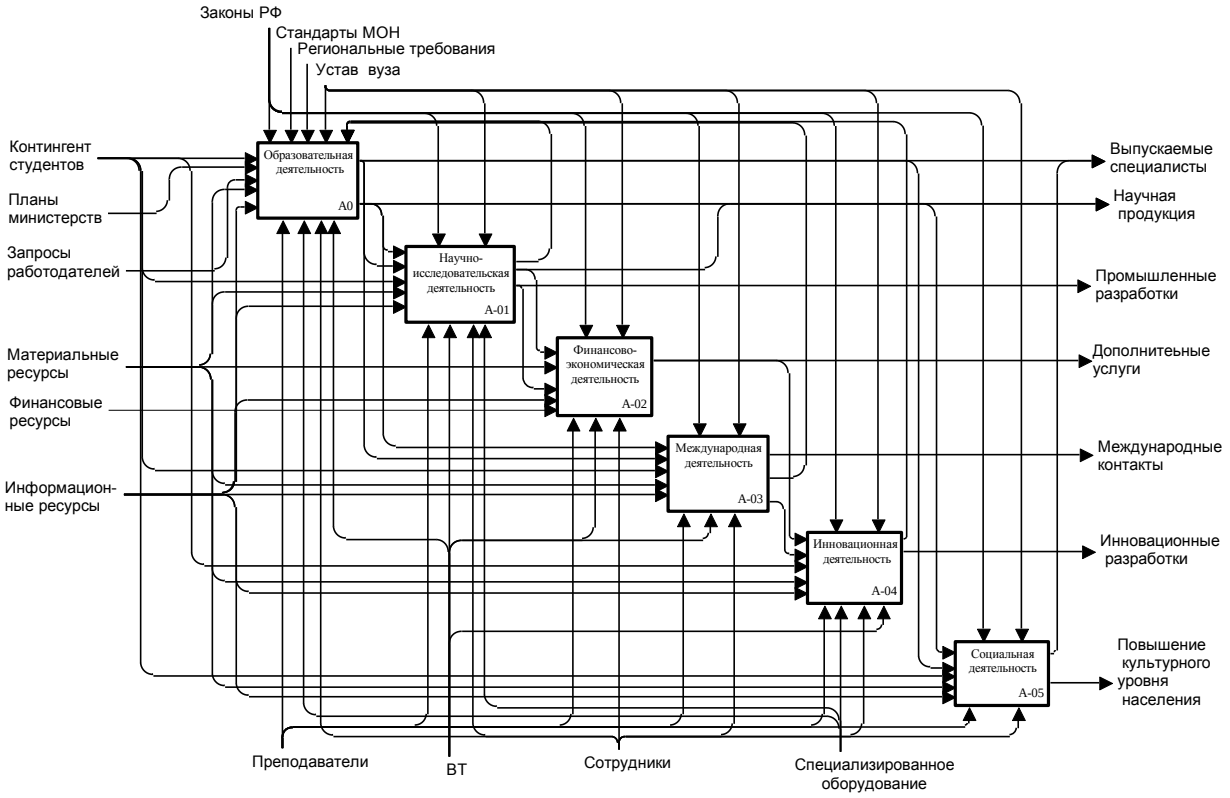

Рисунок 1 – Функциональная модель основных бизнес-процессов вуза

Следующим шагом анализа бизнес-процессов вуза является построение комплекса информационных моделей на основе технологии IDEF1X. На рис. 2 приведен пример построения информационной модели для одного из этапов учебного процесса – рубежного контроля знаний студентов.

Построение комплекса информационных моделей позволяет идентифицировать задействованные информационные активы и провести их категорирование, в том числе по степени конфиденциальности.

Следующим этапом анализа рисков является выявление источников основных угроз информационной системе вуза. В работе построены модели различных типов злоумышленников, характерных для вуза (студент, сотрудник, посетитель, хакер-одиночка, хакерская группа, конкурент, преступные группировки и организации), отличающихся по своим целям, мотивам и возможному потенциалу.

Рассмотрены функциональные модели информационных потоков, позволяющие выявить основные виды уязвимостей для защищаемых информационных активов вуза. Приведена классификация основных видов ущерба, которые может понести вуз от реализации возможных угроз его информационной системе.

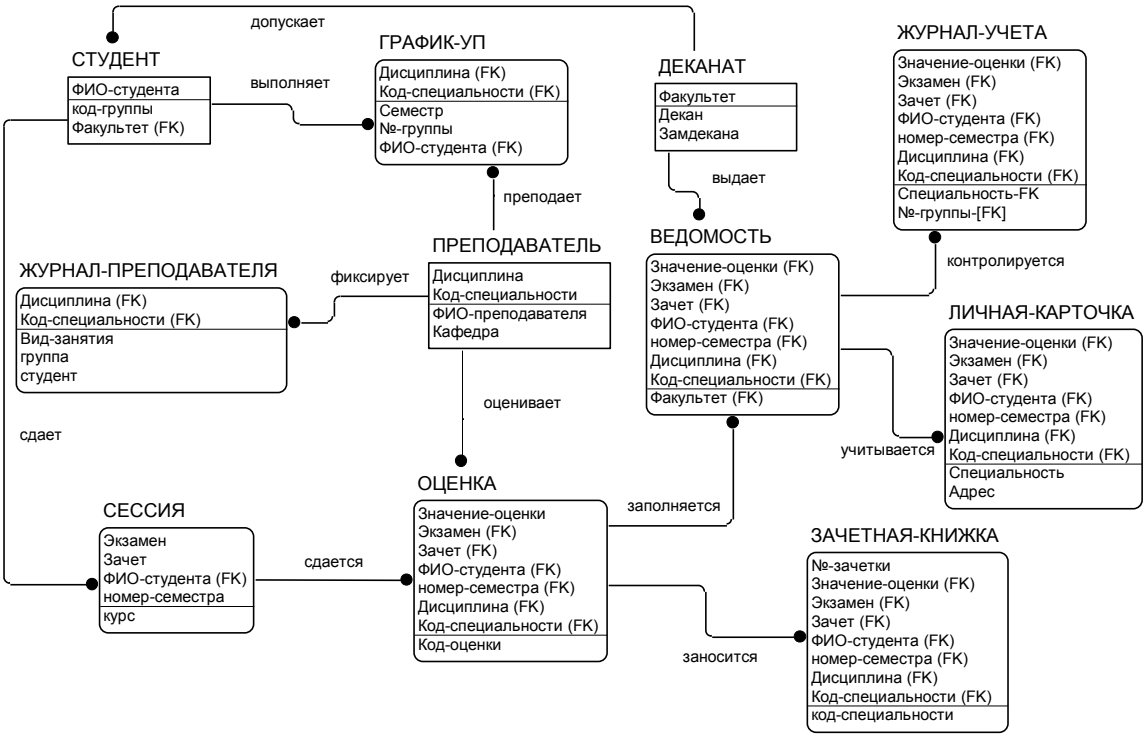

Рисунок 2 – Информационная модель этапа учебного процесса (рубежного контроля знаний студентов)

В третьей главе предложены алгоритмы оценки защищенности информационных активов вуза, основанные на построении нечетких когнитивных карт. Когнитивная карта – это знаковый ориентированный граф, в вершинах которого располагаются ключевые факторы объекта моделирования (концепты), связанные между собой дугами, отображающими причинно-следственные связи между ними. Эти связи характеризуют степень (силу) влияния концептов друг на друга и задаются с помощью нечетких весов W_{ij}, интервальных оценок или лингвистических термов. В общем случае, нечеткая когнитивная карта определяется как кортеж множеств: НКК= $\{C, F, W\}$, где C – конечное множество вершин (концептов); F – конечное множество связей между концептами; W – конечное множество весов этих связей.

На рис. 3 приведен пример построения НКК для оценки информационных рисков вуза. Для решения задачи анализа все концепты разделены на 5 типов: C^G – множество целевых факторов; C^U – множество дестабилизирующих факторов (угроз); C^S – множество информационных активов; C^I – множество базисных факторов (промежуточных концептов-индикаторов); C^R – множество управляющих факторов. В табл. 1 указаны выделенные для анализа концепты и их переменные состояния. Веса связей задавались на базе экспертных оценок с помощью термов лингвистических переменных («слабо», «средне», «силь-

но») на шкале [0,1]. В качестве целевых анализируемых факторов выбраны три концепта – «Репутация», «Качество образования» и «Материально-техническое состояние», определяющие состояние вуза на рынке образовательных услуг.

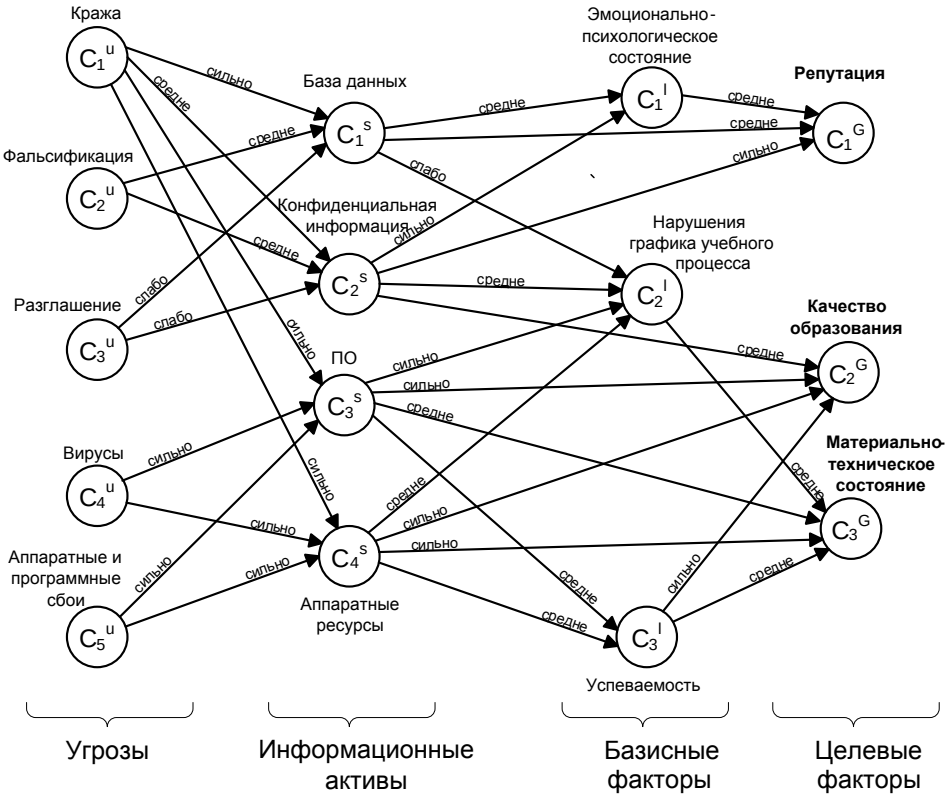

Рисунок 3 – НКК для оценки информационных рисков вуза

Построенная таким образом НКК позволяет оценить влияние как отдельных угроз, так и совокупности угроз на тот или иной целевой фактор.

Общий эффект влияния концепта C_i^U (угрозы) на концепт C_j^G (целевой фактор) при этом определяется матрицей достижимости

$$\mathbf{T} = \sum_{i=1}^{n-1} \mathbf{W}^i ,$$

где $\mathbf{W}^i = \|W_{ij}\|_{n \times n}$ – матрица смежности НКК; W_{ij} – вес связи между i-м и j-м концептами НКК; n – число концептов НКК. При нечетких значениях весов W_{ij} операции умножения и сложения заменяются соответственно на операции нахождения минимума и максимума. Так, непрямой эффект влияния C_i^U на C_j^G определяется минимальным из значений весов связей, встречающихся на пути T_k:

$$T_k(C^U_i \rightarrow C^G_j) = min\ \{W_{ij}\}.$$

Полный (суммарный) эффект от воздействия C^U_i на C^G_j:

$$T(C^U_i \rightarrow C^G_j) = max\ \{T_1, T_2, ..., T_N\},$$

где T_k – непрямой эффект между угрозой C^U_i и целевым фактором C^G_j; $\{W_{ij}\}$ – множество весов связей на пути между концептами C^U_i и C^G_j; N – число непрямых эффектов (число путей между концептами C^U_i и C^G_j).

Риск j-го целевого фактора по отношению к i-ой угрозе определяется по формуле:

$$R_{ij} = P_i \cdot T(C^U_i \rightarrow C^G_j) \cdot r_j\ ,$$

где r_j – ценность j-го ресурса; $T(C^U_i \rightarrow C^G_j)$ – полный эффект воздействия C^U_i на C^G_j; P_i – вероятность i-ой угрозы.

Суммарный риск R по отношению к учитываемому множеству угроз:

$$R = \sum_{i=1}^{m} \sum_{j=1}^{k} \nu_j \cdot R_{ij},$$

где m – число учитываемых угроз; k – число целевых факторов; ν_j – значимость j- го целевого фактора, определяемая экспертно.

Таблица 1 – Концепты и переменные состояния НКК

№	Концепт	Наименование концепта	Переменная состояния x_i
1.	C_1^U	Кража	Среднее количество хищений / ед. вр.
2.	C_2^U	Модификация	Среднее количество несанкционированных изменений / ед. вр.
3.	C_3^U	Разглашение	Среднее количество разглашений / ед. вр.
4.	C_4^U	Вирусы	Среднее количество вирусных атак /ед.вр.
5.	C_5^U	Аппаратные и программные сбои	Среднее количество и сбоев /ед. вр.
6.	C_1^S	Базы данных	Степень достоверности информации, содержащейся в БД, %
7.	C_2^S	Конфиденциальная информация	Степень сохранности конфиденциальной информации, %
8.	C_3^S	Программное обеспечение	Уровень готовности ПО, %
9.	C_4^S	Аппаратные ресурсы	Работоспособность компьютеров и других аппаратных средств, %
10.	C_1^I	Эмоционально-психологическое состояние	Количество стрессовых ситуаций / инцидентов, ед.
11.	C_2^I	Нарушения графика учебного процесса	Количество срывов занятий, ед.
12.	C_3^I	Уровень успеваемости студентов	Средний уровень знаний в пятибалльной системе
13.	C_1^G	Репутация вуза	Число негативных публикаций или высказываний, ед.
14.	C_2^G	Качество образования	Количество выпускников, работающих по специальности, %
15.	C_3^G	Материально-техническое состояние	Капитализация, руб.; Оснащенность ВТ, ЭВМ/студ.

В табл. 2 приведены оценки влияния угроз C_1^U … C_5^U на целевые факторы C_1^G … C_3^G. Анализ НКК показывает, что при заданной таким образом экспертами силе связи между концептами реализация угрозы «Кража» по отношению к информационным ресурсам вуза «сильно» влияет на концепты «Качество образования» и «Материально-техническое состояние» и «средне» влияет на концепт «Репутация» вуза. Задавая в абсолютных или условных единицах стоимость целевых факторов C^G_i, далее можно определить потенциальный риск (ущерб) как для отдельных целевых факторов от действия тех или иных угроз, так и общий (суммарный) риск.

Таблица 2 – Оценка степени влияния угроз на целевые факторы

Угроза (C^U_i)	Полный эффект влияния угрозы на целевой фактор до введения контрмер			Полный эффект влияния угрозы на целевой фактор после введения контрмер		
	$\boldsymbol{C^G_1}$	$\boldsymbol{C^G_2}$	$\boldsymbol{C^G_3}$	$\boldsymbol{C^G_1}$	$\boldsymbol{C^G_2}$	$\boldsymbol{C^G_3}$
$\boldsymbol{C^U_1}$	средне	сильно	сильно	слабо	средне	средне
$\boldsymbol{C^U_2}$	средне	средне	средне	слабо	слабо	слабо
$\boldsymbol{C^U_3}$	слабо	слабо	слабо	слабо	слабо	слабо
$\boldsymbol{C^U_4}$	-	сильно	сильно	-	средне	средне
$\boldsymbol{C^U_5}$	-	сильно	сильно	-	средне	средне

Использование НКК дает при этом возможность не только наглядно выявить негативные процессы, протекающие в информационной системе при действии угроз, но и указать наиболее уязвимые места и пути ослабления воздействия угроз за счет введения соответствующих управляющих воздействий (контрмер) $\{C^R_k\}$, что позволяет добиться снижения уровня информационных рисков до приемлемого значения.

Так, если в качестве угрозы, воздействующей на информационные ресурсы вуза, рассматриваются вирусы (концепт C_4^U), а уровень силы этой угрозы на целевые факторы C^G_2 («Качество образования») и C^G_3 («Материально-техническое состояние») определяется значением лингвистической переменной «сильно», то для снижения влияния данной угрозы необходимо ввести такие контрмеры, как выбор стратегии антивирусной защиты, подходящей антивирусной программы, управление антивирусными программами и т. д. Это позволит снизить степень влияния концепта C^U_4 на концепты C^G_2 и C^G_3 до уровня «средне» (табл.2). В табл. 3 приведены рекомендуемые мероприятия (множество управляющих факторов) и оценки степени их влияния на указанные концепты. Соответствующая НКК после введения контрмер (концепты C^R_1 … C^R_{31}) приведена на рис.4.

Таблица 3 – Множество управляющих факторов

Обозначение	Наименование концепта	Влияние концепта на связь W_{ij}	Обозначение	Наименование концепта	Влияние концепта на связь W_{ij}
C^R_1, C^R_5, C^R_7	Разграничение уровней доступа пользователей	средне	C^R_{18}	Организация процедуры хранения документов	средне
C^R_2, C^R_6, C^R_8, C^R_3, C^R_4	Контроль и управление доступом в помещение	средне	C^R_{20}	Разработка процедуры восстановления после вирусных атак	средне
C^R_9, C^R_{10}	Разработка и внедрение концепции защиты от вирусов	сильно	C^R_{19},C^R_{21}, C^R_{25}	Разработка процедуры по оперативному реагированию на инциденты	средне
C^R_{11}, C^R_{12}	Административные и технические средства контроля работы пользователей	средне	C^R_{22}, C^R_{23}	Использование лицензионного ПО, разграничение доступа	средне
C^R_{13}, C^R_{16}	Мероприятия по предовращению конфликтов в коллективе	средне	C^R_{24}, C^R_{26}, C^R_{27}	Техническая поддержка аппаратных ресурсов	средне
C^R_{14}, C^R_{17}, C^R_{28}	Формирование корпоративной культуры	средне	C^R_{29}, C^R_{30}, C^R_{31}	Разработка мероприятий по повышению стабильности учебного процесса	средне
C^R_{15}	Резервное копирование	сильно			

Анализ соотношения полученных рисков и затрат на мероприятия по их уменьшению позволяет определить рациональные способы управления ИБ вуза и обосновать требуемые затраты на безопасность.

Принятие решений о выборе необходимых контрмер и оценке допустимого уровня риска должно проводиться по критерию «стоимость-эффективность». При этом возможны следующие постановки задачи выбора управляющих факторов для снижения рисков:

1) $R_\Sigma \le R_{доп.}$ при $S_\Sigma \to min$ –определение минимальных затрат на реализацию мероприятий по защите информации при обеспечении допустимого уровня риска;

2) $S_\Sigma \le S_{доп.}$ при $R_\Sigma \to min$ –определение минимизации риска при заданных затратах на вводимые мероприятия.

Здесь: R_Σ и S_Σ - суммарный риск и затраты на мероприятия (контрмеры) по защите информации; $R_{доп.}$ и $S_{доп.}$ – допустимые значения суммарного риска и затрат.

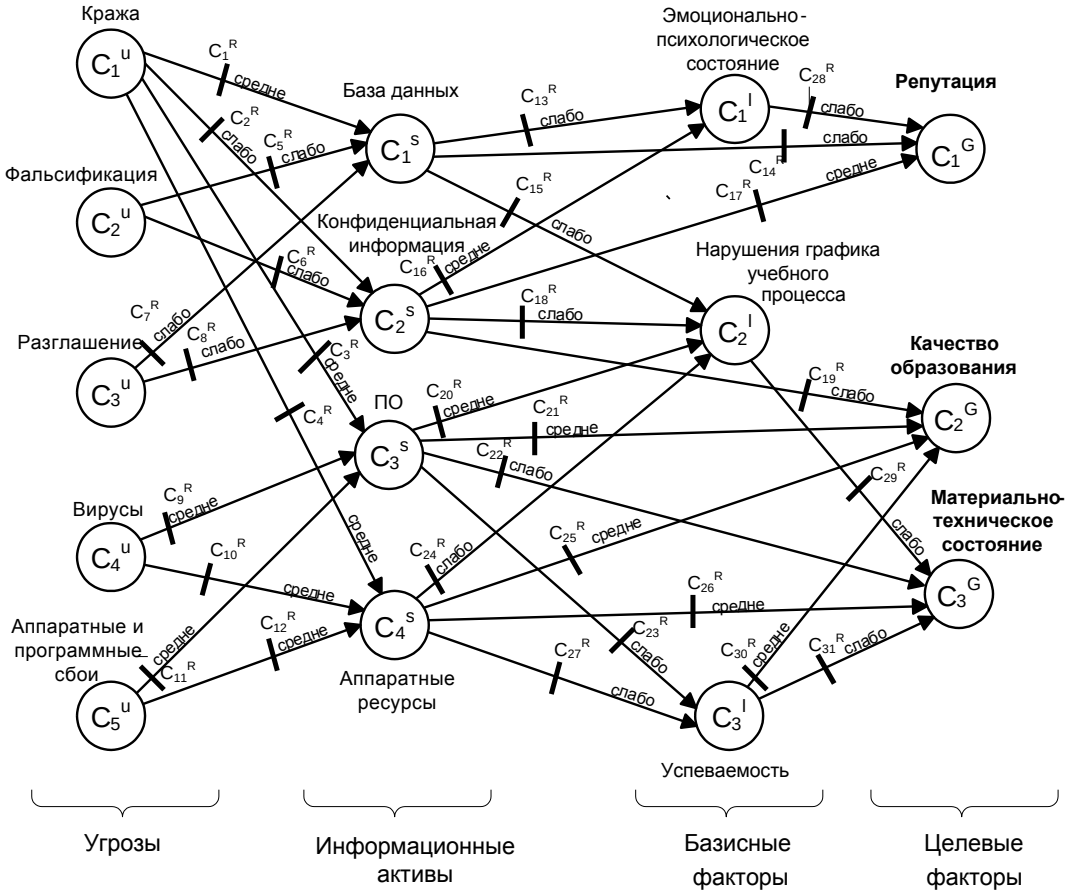

Рисунок 4 – НКК для оценки информационных рисков вуза с указанием множества управляющих факторов

Эффективность управляющих воздействий рассчитывается по формуле:

$Э = \frac{R'_{\Sigma} - R_{\Sigma}}{R'_{\Sigma}}$, где $R`_{\Sigma}$ – рассчитанный первоначальный риск; R_{Σ} – риск после введения дополнительных контрмер.

В четвертой главе приведена методика обеспечения ИБ вуза на основе оценки информационных рисков с помощью нечетких когнитивных карт. Предлагаемый подход обеспечивает наглядность на этапе оценки влияния основных угроз информационной системе вуза, что дает удобный инструмент для поддержки принятия решений на всех уровнях политики безопасности вуза, включая административный уровень.

Описаны разработанные в ходе исследования программные продукты *CognitiveRiskAnalizer*, *RiskManagement* и *FCM Builder* (рис. 5), применение которых позволяет автоматизировать и сократить сроки анализа информационных рисков и выбора необходимых контрмер по управлению ИБ вуза.

Предложена структура системы поддержки принятия решений (СППР) по управлению информационными рисками вуза с использованием технологий когнитивного моделирования, применение которой позволит повысить объек-

тивность и оперативность принимаемых решений по управлению ИБ вуза, направленных на снижение потенциальных потерь от действия возможных внешних и внутренних угроз.

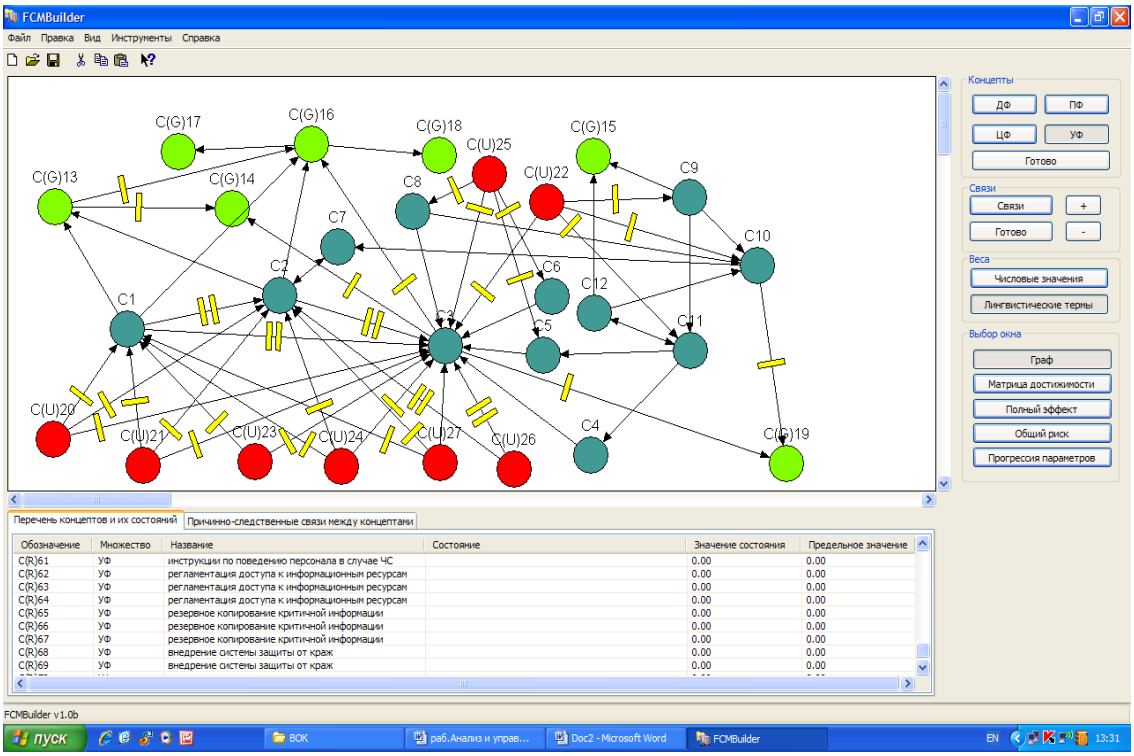

Рисунок 5 – Интерфейс программы *FCM Builder*

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. На основе системного анализа бизнес-процессов вуза как объекта защиты разработаны функциональные и информационные модели основных бизнес-процессов, определяющих различные аспекты деятельности вуза в сфере образования и науки, которые позволяют выявить его основные информационные ресурсы и определить требуемый уровень их защищенности.

2. Предложен комплекс системных моделей, определяющих основные компоненты информационных рисков вуза (модели угроз, злоумышленников, уязвимостей, потенциального ущерба от действия угроз) с учетом особенностей бизнес-процессов, протекающих в вузе как сложном распределенном объекте защиты.

3. Разработаны алгоритмы анализа и управления информационными рисками вуза, основанные на построении нечетких когнитивных карт. Предложено выделить в качестве базовых типов концептов: информационные активы, дестабилизирующие факторы (угрозы), базисные факторы (промежуточные концепты-индикаторы) и управляющие факторы, сила связей между которыми за-

дается экспертным путем. Это позволяет дать количественную оценку влияния основных угроз на информационные активы вуза, выявить наиболее уязвимые места информационной системы, представить эффективный механизм принятия решений по обеспечению информационной безопасности вуза.

4. Разработаны инструментальные программные средства для оценки уровня информационных рисков вуза, позволяющие автоматизировать процедуру построения НКК, оценивать уровень информационных рисков и вырабатывать необходимые контрмеры для управления ИБ вуза.

Предложенный метод оценки информационных рисков вуза с использованием НКК позволяет сократить в 1,5…2 раза время на принятие решений по выбору необходимых контрмер, обеспечивая снижение информационных рисков за счет введения эффективных управляющих воздействий (контрмер) при ограничении суммарных затрат на защиту информации.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Анализ и управление информационной безопасностью вуза на основе когнитивного моделирования / Васильев В.И., Кудрявцева Р.Т. // Системы управления и информационные технологии, 2007, № 1(27). – С. 74-81.

2. Системный анализ информационных рисков с применением нечетких когнитивных карт / Гузаиров М.Б., Васильев В.И., Кудрявцева Р.Т. // Инфокоммуникационные технологии, 2007. Том 5, № 4. – С. 96-101.

В других изданиях

3. Моделирование системы защиты информационных ресурсов подразделения ВУЗа с помощью Марковских моделей / Васильев В.И.. Вишнякова Т.О., Кудрявцева Р.Т. // Проблемы техники и технологии телекоммуникаций : Материалы шестой Междунар. научно-техн. конференции, 28 –30 ноября 2005 г., - Уфа: УГАТУ. – С. 192-193.

4. Оценка защищенности объекта информатизации с использованием методов экспертных оценок и нечеткой логики / Кудрявцева Р.Т., Волох О.Л., Кайбышева А.И. // Информационно-вычислительные технологии и их приложения : Сб. материалов Междунар. научно-техн. конференции, декабрь 2005 г., г. Пенза. – С. 122-125.

5. Разработка организационных мер защиты информации с помощью нечеткого когнитивного моделирования / Кудрявцева Р.Т., Савина И.А., Шарипова И.И. // Информационно-вычислительные технологии и их приложения : Сб. материалов Междунар. научно-техн. конференции, Пенза, 2005. – С. 125-128.

6. Когнитивное моделирование системы защиты информационных ресурсов подразделения ВУЗа / Кудрявцева Р.Т., Савина И.А., Шарипова И.И. // Высокие технологии, фундаментальные и прикладные исследования, образование : Сб. трудов Второй Междунар. научно-практич. конференции «Исследование, разработка и применение высоких технологий в промышленности». Т.4. - Санкт-Петербург, 2006. – С. 33-34.

7. Применение скрытых Марковских моделей в оценке защищенности предприятия / Кудрявцева Р.Т., Чавдаров П.Г. // Высокие технологии, фундаментальные и прикладные исследования, образование : Сб. трудов Второй Междунар. научно-практич. конференции «Исследование, разработка и применение высоких технологий в промышленности». Т.5. - Санкт-Петербург, 2006. – С. 135-136.

8. Анализ и управление информационными рисками в высшем учебном заведении / Васильев В.И., Кудрявцева Р.Т. // Российская научно-техн. конференция «Мавлютовские чтения». Т. 1. - Уфа, 2006.– С. 34-40.

9. Анализ системы информационной защиты ВУЗа с помощью когнитивного моделирования / Васильев В.И., Кудрявцева Р.Т. // Актуальные проблемы качества образования и пути их решения : Материалы XVI Всероссийской научно-методической конференции, Москва, 2006. – С. 232-234.

10. Алгоритм расчета рисков при оценке защищенности организации / Кудрявцева Р.Т., Савина И.А., Шарипова И.И. // Информационная безопасность : Материалы VIII Междунар. научно-практической конференции. Ч.1. - Таганрог: Изд-во ТРТУ, 2006. – С. 95-98.

11. Алгоритм расчета рисков при оценке информационной безопасности организации / Кудрявцева Р.Т., Савина И.А., Шарипова И.И. // Компьютерные науки и информационные технологии (*CSIT*'2006) : Труды 8-ой Международной конференции. Т. 2. - Карлсруэ, Германия, 2006– С. 180-182 (на англ. языке).

12. Моделирование информационных рисков вуза в среде MATLAB с помощью когнитивного подхода / Васильев В.И., Кудрявцева Р.Т., Шарипова И.И., Савина И.А. // Вычислительная техника и новые информационные технологии : Межвузовский научный сборник. Вып. 6. Уфа, 2007. – С. 170-177.

13. Построение нечетких когнитивных карт для моделирования информационных рисков вуза в среде *MATLAB* / Васильев В.И., Кудрявцева Р.Т., Шарипова И.И., Савина И.А. // Компьютерные науки и информационные технологии (CSIT'2007) : Труды 9-ой Международной конференции. Т.1. - Уфа, 2007. – С. 194-197 (на англ. языке).

14. Свид. об офиц. рег. программы для ЭВМ № 2006612795. Программа для расчета и анализа рисков с применением когнитивных технологий / Васильев В.И., Кудрявцева Р.Т., Савина И.А. М. : Роспатент, 2006.

15. Свид. об офиц. рег. программы для ЭВМ № 2006612929. Управление информационными рисками / Васильев В.И., Кудрявцева Р.Т., Шарипова И.И., Асадуллин В.М. М. : Роспатент, 2006.

16.Свид. об офиц. рег. программы для ЭВМ № 2006613038. Программный модуль оценки защищенности информационных ресурсов предприятия / Васильев В.И., Кудрявцева Р.Т., Чавдаров П.Г. М. : Роспатент, 2006.

17.Свид. об офиц. рег. программы для ЭВМ № 2007613536 Универсальное решение для автоматизации анализа и управления рисками с использованием нечетких когнитивных карт (*Fuzzy Cognitive Maps Builder*) / Васильев В.И., Кудрявцева Р.Т., Юдинцев В.А. М. : Роспатент, 2007.

Диссертант Р.Т. Кудрявцева

КУДРЯВЦЕВА Рима Тимиршаиховна

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

(на примере высшего учебного заведения)

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук

Подписано к печати 12.09.2008. Формат 60х84 1/16.
Бумага офсетная. Печать плоская. Гарнитура Таймс.
Усл. печ. л. 1,0. Усл. кр. – отт. 1,0. Уч. – изд. л.0,9.
Тираж 100 экз. Заказ № 372

ГОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К.Маркса,12.