Уфа : УГАТУ, 2008 Вестник УГАТУ • Управление, ВТ и И Т. 10, № 2 (27). С. 199–209

УДК 004.056:378.095

В. И. ВАСИЛЬЕВ, И. А. САВИНА, И. И. ШАРИПОВА

ПОСТРОЕНИЕ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ ДЛЯ АНАЛИЗА И УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ ВУЗА

Рассмотрен подход к решению задачи анализа и управления информационными рисками вуза, основанный на использовании нечетких когнитивных карт. Предложена методика построения и интерпретации такой карты для анализа и управления информационными рисками, иллюстрируемая примером ее использования. *Информационная безопасность* ; *нечеткие когнитивные карты* ; *анализ рисков* ; *управление рисками*

Безопасность информационных ресурсов имеет большое значение для обеспечения нормальной работы любого предприятия, независимо от сферы его деятельности. Нарушение доступности, целостности или конфиденциальности информации приводит к существенным временным и финансовым затратам. Это относится не только к потенциально опасным объектам (в промышленности или в военной сфере), но и к таким социально значимым учреждениям, как высшее учебное заведение. Университет представляет собой даже более питательную среду для угроз информационной безопасности, чем другие гражданские организации. Как правило, в вузах, где имеются и постоянно воспроизводятся уникальные информационные ресурсы, почему-то практически не уделяется внимание проблеме защиты информации. Поэтому решение вопросов обеспечения информационной безопасности для высших учебных заведений становится особенно важным и своевременным.

Необходимость обеспечения безопасности вузов (в том числе и информационной) начинает сегодня осознаваться на государственном уровне. Эти перемены отразились и в законодательстве сферы образования. Так, появилась комплексная программа Министерства образования и науки России на 2004–2007 гг. «Безопасность образовательного учреждения», а также научно-исследовательский проект «Обеспечение информационной безопасности в сфере открытого образования». В последнем документе, в частности, ставится задача обеспечения информационной безопасности образовательной инфраструктуры.

Согласно международным стандартам по информационной безопасности ISO 15408, 17799, 27001, ядро современной системы защиты информации — анализ и управление рисками, под которыми понимается процесс идентификации, устранения или уменьшения рисков безопасности, потенциально имеющих возможность воздействовать на информационную систему, при условии приемлемой стоимости защиты. В настоящее время определенную известность получили такие методики управления информационными рисками и основанное на них программное обеспечение, как Risk Watch (США), CRAMM (Великобритания), COBRA (Великобритания), ГРИФ, КОНДОР+ (Россия) и ряд других. Вместе с тем, эти продукты ориентированы, как правило, на коммерческие предприятия, поэтому для решения задач анализа и управления информационными рисками в вузе (в силу его особенностей) они не годятся.

1. ОСОБЕННОСТИ ВУЗА КАК ОБЪЕКТА ЗАЩИТЫ

С точки зрения обеспечения информационной безопасности, вуз обладает рядом особенностей:

- широкое внедрение средств вычислительной техники во все сферы учебного процесса и научных исследований, а также в управленческие структуры;
- огромные объемы информации, циркулирующие в учебном заведении;
- территориальная разобщенность отдельных объектов как внутри города, так и между филиалами и представительствами вуза в других городах;

• скопление большого количества людей на территории вуза;

• использование современных информационных технологий, включая электронный документооборот, средства инфотелекоммуникаций, распределенные базы данных, интернет-технологии и т. д.;

• развитие различных форм дистанционного обучения;

• значительные наработки в области интеллектуальной собственности, связанные с проведением госбюджетных и хоздоговорных научно-исследовательских работ (НИР), методическим обеспечением учебного процесса;

• потребность в постоянном притоке и обновлении информационных ресурсов и технологий как для студентов, так и для сотрудников и преподавателей вуза;

• сложность управления и контроля эффективности основного производственного процесса вуза — обучения.

Отличительной особенностью вуза также является молодой возраст основной массы пользователей информации, т. е. студентов. С точки зрения защиты информации, именно эта категория людей является наиболее уязвимой, так как она отличается:

• большей восприимчивостью новым идеям;

• повышенной психологической уязвимостью;

• негласной конкуренцией и борьбой за лидерство в своей среде;

• несформировавшимся сознанием и неустойчивостью личностных качеств.

Вышеперечисленные особенности приводят к неконтролируемому росту количества уязвимостей, увеличению числа угроз со стороны внешних и внутренних злоумышленников и, соответственно, трудно предсказуемым потенциальным материальным, финансовым, моральным и другим видам потерь.

Специфика образовательных учреждений создает дополнительные сложности при анализе и управлении рисками, поэтому необходимо разработать такой метод, который будет эффективен, несмотря на слабую формализованность объекта исследования, т. е. учебного и научного процессов с точки зрения информационной безопасности. Таким методом является моделирование процессов защиты информации с использованием нечетких когнитивных карт (НКК), сочетающих в себе преимущества нечеткой логики и нейронных сетей.

2. ОСНОВЫ ПОСТРОЕНИЯ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Нечеткие когнитивные карты (НКК) используются для решения широкого круга задач, связанных с моделированием плохо формализованных процессов, их прогнозированием и поддержкой принятия решений. Неоспоримыми их достоинствами по сравнению с другими методами являются возможность формализации численно неизмеримых факторов, использования неполной, нечеткой и даже противоречивой информации [1].

Чтобы построить НКК, объект исследования представляют в виде знакового ориентированного графа. Ключевые факторы объекта исследования располагаются в вершинах графа и называются концептами. Дуги графа отображают причинно-следственные связи между вершинами. Таким образом, НКК представляет собой кортеж множеств:

$$\text{НКК} = \{\text{C}_n, L_{ij}, Sg_{ij}, W_{ij}\}, \qquad (1)$$

где $\{C_n\}$ — множество вершин (концептов);

$\{L_{ij}\}$ — множество причинно-следственных связей между концептами;

$\{Sg_{ij}\}$ — множество знаков связей (+, -);

$\{W_{ij}\}$ — множество весов связей (сильно, средне, слабо и т. д.).

Каждый концепт C_i описывается одной или несколькими переменными состояния, которые характеризуют состояние концепта качественно или количественно. Связь L_{ij} описывает влияние изменения фактора C_i на фактор C_j. Если значение переменной состояния концепта C_j возрастает или убывает в зависимости от того, возрастает или убывает концепт C_i, то связь между ними положительная ($Sg_{ij} = +$). И наоборот, если значение переменной состояния концепта C_j при увеличении C_i уменьшается, а при уменьшении C_i увеличивается, то это отрицательная ($Sg_{ij} = -$) связь. Вес связи W_{ij} определяет силу влияния концепта C_i на концепт C_j и обычно определяется лингвистическими термами (например, сильно, средне, слабо).

В свою очередь, множество концептов $\{C_n\}$ можно разделить на следующие подмножества:

$$\{C_n\} = \{C_k^G, C_i^U, C_j^M, C_l^B\}, \qquad (2)$$

где $\{C_k^G\}$ — подмножество целевых факторов, состояние которых является критически важным для собственника информационной системы;

$\{C_i^U\}$ — подмножество дестабилизирующих факторов или угроз информационной безопасности;

$\{C_j^M\}$ — подмножество управляющих факторов, с помощью которых решается задача управления рисками;

$\{C_j^B\}$ — подмножество базовых факторов, к которым относятся все остальные промежуточные концепты.

Определение концептов, их переменных состояний и связей между ними является задачей, требующей высокой квалификации эксперта, осуществляющего построение и анализ НКК.

В теории НКК вводится понятие непрямых и полных причинных эффектов [1]. Некоторый путь от концепта C_i к концепту C_j, например, $C_i \to C_{k1} \to \ldots \to C_{kn} \to \to C_j$, считается непрямым эффектом. При этом если веса причинно-следственных связей заданы, можно вычислить значение непрямого эффекта. В простейшем случае оно равно

$$T(C_i \to C_{k1} \to \ldots \to C_{kn} \to C_j) = \\ = \min\{W_{i,k1}, W_{k1,k2}, \ldots, W_{kn,j}\}, \quad (3)$$

где W_{ij} — веса причинно-следственных связей между концептами (без учета знака).

В том случае, когда имеет место только один путь из C_i в C_j, то полный эффект влияния C_i на C_j сводится к непрямому эффекту. При наличии нескольких различных непрямых эффектов (путей из C_i в C_j), общий полный эффект вычисляется как

$$S(C_i \to C_j) = \max\{T_1, T_2, \ldots, T_N\}, \quad (4)$$

где T_k — непрямой эффект между C_i и C_j; N — число непрямых эффектов.

В случае задания весов связей W_{ij} в виде интервальных оценок или нечетких значений, при вычислении непрямого эффекта используется T-норма, а при вычислении полного пути — S-конорма [1]. Существуют также упрощенные алгоритмы по нахождению максимальных путей между различными концептами НКК [2].

3. МЕТОДИКА ИСПОЛЬЗОВАНИЯ НКК ДЛЯ АНАЛИЗА И УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Построение НКК производится экспертами соответствующей предметной области. Этот процесс похож на создание базы знаний экспертной системы. Процедура создания НКК для наиболее общего случая описана в [2], однако она имеет определенные особенности в зависимости от исследуемой области и задачи моделирования.

В данной работе в качестве объекта управления рассматриваются информационные риски, поэтому важным вопросом является то, как их оценивать и вычислять. Риск — это ожидаемые потери или возможный результат реализации угрозы при существовании уязвимости [3]. В общем случае при расчете риска используется формула:

$$R_{ij} = P_i^U \cdot P_{ij}^V \cdot A_j, \quad (5)$$

где R_{ij} — риск j-го информационного ресурса относительно i-й угрозы;

P_i^U — вероятность появления i-й угрозы;

P_{ij}^V — уязвимость защиты j-го ресурса по отношению к i-й угрозе;

A_j — ценность j-го ресурса.

Однако две первые составляющие риска (т. е. вероятность угрозы P_i^U и уязвимость защиты P_{ij}^V) обычно сложно определить, если речь идет об информационном ресурсе. Причинами этого, как правило, являются недостаточная статистика и сложность оценки вероятности угроз. Это стало одной из причин использования в данной работе нечетких когнитивных карт. Особенность когнитивных карт состоит в использовании нечетких лингвистических переменных для описания значений факторов, что делает этот метод пригодным для моделирования ситуаций, имеющих нечеткое описание. Математический аппарат НКК позволяет вычислить даже опосредованные влияния одних концептов на другие с помощью механизма непрямых и полных эффектов. Если использовать формулу (4) для прослеживания пути от i-й угрозы к j-му информационному ресурсу, то получится значение полного эффекта влияния угрозы на ресурс ($C_i^U \to C_j^G$). В таком случае значение полного эффекта дает приближенное значение произведения вероятности реализации угрозы и уязвимости защиты в отношении данного ресурса. Это можно использовать при вычислении риска:

$$R_{ij} = S(C_i^U \to C_j^G) \cdot A_j, \quad (6)$$

где $S(C_i^U \to C_j^G)$ — полный эффект влияния i-й угрозы на j-й ресурс (целевой фактор), вычисленный с помощью формулы (4);

A_j — ценность ресурса.

Формула (6) позволяет вычислить риск в случаях, когда сложно оценить вероятность

угрозы и уязвимость защиты: при отсутствии статистики угроз, большом количестве информационных потоков и т. д., что характерно для анализа и управления информационными рисками в вузе.

Учесть сложность информационной системы вуза можно и при построении НКК, для этого предлагается сделать ее интегративной. Это означает, что связь между любыми двумя концептами при желании можно также представить в виде нечеткой когнитивной карты, только более низкого уровня. При этом выявленное в ходе анализа этой НКК нижнего уровня наиболее сильное влияние (вычисляемое по формуле (4)) и передаст свое значение связи верхнего уровня. Соответствующий пример приведен на рис. 1: наиболее сильное влияние на концепт C_6 оказалось у концепта C_2, поэтому именно эта связь перешла на верхний уровень.

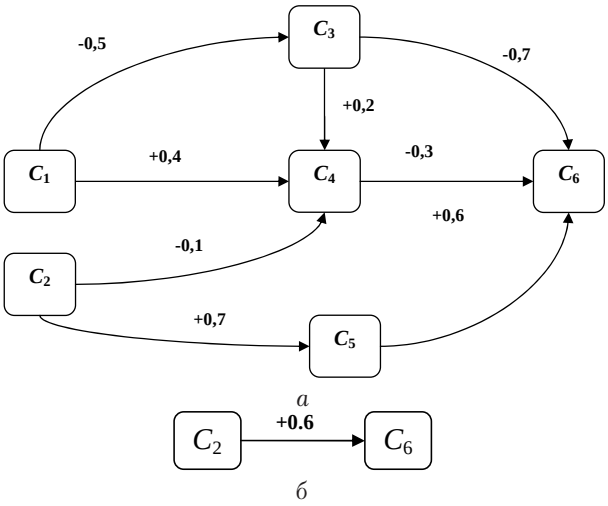

Рис. 1. НКК нижнего уровня (*а*) и эквивалентная ей связь верхнего уровня (*б*)

Интегративность позволит упростить нечеткую когнитивную карту, опустив менее важные, но все же значительные связи на нижний уровень, одновременно учтя их влияние.

Задача управления информационными рисками применительно к НКК состоит из двух этапов. На первом этапе требуется определить состояния целевых факторов $\{C_k^G\}$ при заданных начальных состояниях всех концептов $\{C_n\}$ (прямая задача управления или анализ рисков). Если по результатам первого этапа делается вывод о неприемлемости вычисленных величин рисков, то подразумевается переход ко второму этапу. На втором этапе необходимо найти такие управляющие факторы $\{C_i^U\}$, которые обеспечат желаемые изменения целевых факторов $\{C_k^G\}$ (обратная задача, или управление рисками). Решение обратной задачи может быть неединственным, поэтому возникает задача оптимизации, состоящая в нахождении такой комбинации управляющих факторов, которые будут максимально ослаблять влияние дестабилизирующих факторов.

В зависимости от характера управляющих воздействий, можно выделить несколько стратегий управления рисками [4]:

- *уменьшение риска*:

многие риски могут быть существенно уменьшены путем использования соответствующих способов и средств защиты. В этом случае в НКК будут введены управляющие факторы в виде множества барьеров $\{d_{ij}\}$, которые будут воздействовать на связи между дестабилизирующими факторами $\{C_i^U\}$ и остальными, снижая, таким образом, их влияние на информационную систему:

$$\{\mathrm{C}_n, L_{ij}, Sg_{ij}, W_{ij}\} => \\ => \{C_m, L_{ij}, Sg_{ij}, W_{ij}, d_{ij}, W_{ij}^d\}; \quad (7)$$

- *уклонение от риска*:

от некоторых классов рисков можно уклониться. Например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. На НКК данная стратегия выглядит в виде перегруппировки и изменения состава концептов и связей между ними:

$$\{C_n^1, L_{ij}^1, Sg_{ij}^1, W_{ij}^1\} => \{C_m^2, L_{ij}^2, Sg_{ij}^2, W_{ij}^2\}; \quad (8)$$

- *изменение характера риска*:

если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки. В этом случае управляющие факторы $\{C_j^M\}$ будут воздействовать не непосредственно на дестабилизирующие факторы $\{C_i^U\}$, а на некоторые из базовых факторов $\{C_l^B\}$:

$$\{C_j^M\} \to \{C_l^B\}; \quad (9)$$

- *принятие риска*:

многие риски не могут быть уменьшены до пренебрежимо малой величины. На практике после принятия стандартного набора контрмер ряд рисков уменьшается, но остается все еще значимым. В этом случае приходится решать оптимизационную задачу: что важнее —

бороться с рисками или с их последствиями. В этом случае управляющие факторы $\{C_j^M\}$ будут воздействовать непосредственно на дестабилизирующие факторы$\{C_i^U\}$:

$$\{C_j^M\} \to \{C_i^U\}. \qquad (10)$$

Возможности нечетких когнитивных карт позволяют описать любую из стратегий управления информационными рисками, в том числе такие сложноформализуемые, как принятие и уклонение от риска.

Таким образом, предлагаемая методика построения НКК для анализа и управления информационными рисками вуза состоит из следующих шагов:

1. Разработка экспертами по защите информации структуры знаний об объекте защиты, определение величины приемлемого риска, списка наиболее значимых факторов — базовых (характеризующих ситуацию) концептов. При этом, так как переменные состояния концептов практически невозможно описать точными значениями, их значения задаются в виде нечетких множеств, выделив среди концептов $\{C_n\}$:
   - целевые факторы $\{C_k^G\}$;
   - дестабилизирующие факторы $\{C_i^U\}$;
   - управляющие воздействия $\{C_j^M\}$.
2. Выявление связей между концептами $\{L_{ij}\}$ и их знака $\{\mathrm{Sg}_{ij}\}$.
3. Определение степени влияния $\{W_{ij}\}$ между каждой парой концептов $C_i \to C_j$ путем задания веса связи в виде числовой, интервальной оценки либо лингвистической термы.
4. Представление полученной информации в виде знакового ориентированного графа (НКК) и применение к нему известного математического аппарата. Для исследования когнитивных карт применяются нечеткая логика, теория графов и теория матриц;
5. На этапе анализа рисков выявляются максимальные пути между угрозами и целевыми факторами, производится расчет рисков по формуле (6), делается вывод о приемлемости существующих величин рисков.
6. На этапе управления рисками выбирается стратегия управления и изменения в соответствии с ней состава концептов, связей, их силы и знака. Перерасчет рисков с учетом внесенных изменений.
7. Интерпретация результатов исследования, выдача рекомендаций по повышению уровня защищенности объекта.

4. ПРИМЕР ИСПОЛЬЗОВАНИЯ НКК ДЛЯ АНАЛИЗА И УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ ПОДРАЗДЕЛЕНИЯ ВУЗА

В качестве объекта исследования было выбрано одно из ключевых подразделений в учебном процессе вуза — деканат. Основным видом деятельности в деканате является офисная, и задача защиты информации, таким образом, сводится к организации оперативного, прозрачного и защищенного документооборота. Утрата документов или подделка экзаменационной ведомости может иметь очень серьезные последствия — от нарушения работы деканата до снижения качества образования будущего выпускника, что может в перспективе негативно отразиться на реноме университета.

В целом, деканат как объект защиты имеет следующие особенности:

- объемный документооборот;
- многочисленность посетителей;
- ведение документации как в бумажном, так и в электронном виде;
- плохая эргономика рабочих мест;
- пульсация (неритмичность) рабочей нагрузки;
- относительно высокая численность персонала (как правило, 7–10 человек).

По результатам анкетирования сотрудников нескольких деканатов наиболее ценными информационными ресурсами признаны журналы успеваемости, зачетные и экзаменационные ведомости. Предварительно был определен допустимый уровень риска (0,5 тыс. руб.) в отношении сохранности этих документов. Заметим, что, по мнению многих экспертов, организация защиты документов значительно улучшилась бы с переходом на электронный документооборот.

Согласно методике, приведенной выше, был сформирован список концептов НКК, выявлены их взаимосвязи, оценены знаки и сила влияния концептов друг на друга, что позволило построить нечеткую когнитивную карту (НКК) для анализа и управления информационными рисками деканата (см. рис. 2).

В качестве целевого фактора НКК здесь выбрано качество образования, так как это основной показатель эффективности работы университета. В качестве дестабилизирующих факторов были выбраны наиболее общие угрозы безопасности информации, хранящейся в бумажном виде.

Рис. 2. НКК для анализа и управления информационными рисками деканата

В качестве базовых факторов, по изменениям которых можно судить о состоянии объекта защиты, выбраны: загруженность работников деканата, организация учебного процесса, адекватность документов и др. Под безопасностью ведомостей и журналов успеваемости понимаются их доступность, целостность и достоверность, а под адекватностью документов — степень соответствия записей в ведомостях и журналах результатам контроля знаний студентов. Значения переменных состояния всех вышеприведенных концептов оценивались экспертно, веса связей заданы термами лингвистических переменных.

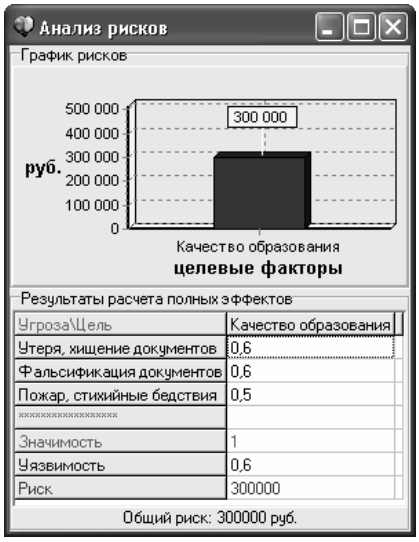

Рис. 3. Величина риска для целевого фактора «Качество образования»

На этапе анализа рисков проводится исследование НКК на ее адекватность, устойчивость по значению и по возмущению. По формуле (6) с помощью разработанного авторами программного продукта CognitiveRiskAnalyzer [5] были вычислены оценки величин информационных рисков в зависимости от разных угроз, а также совокупное значение риска (рис. 3).

Видно, что наибольшие потери для качества образования связаны с реализацией информационных угроз (утеря и фальсификация). Совокупное значение риска существенно превышает допустимое, отсюда делается вывод о необходимости управления рисками.

Рассмотрим возможность уменьшения риска путем применения соответствующих контрмер. На НКК (см. рис. 4) это отражается в виде введения барьеров d_{ij}, под которыми подразумеваются контрмеры, приведенные в табл. 1.

Предлагаемые контрмеры были выбраны из списка, составленного экспертами, с помощью программы CognitiveRiskManager [6]. Каждой контрмере поставлен в соответствие вес W_{ij}^{d}, характеризующий ее эффективность по отношению к угрозе. Если на одну угрозу вводится несколько таких мер, то совокупное их влияние будет средним арифметическим соответствующих весов.

Таблица 1

Предлагаемые контрмеры

Обозначение барьера	Название контрмеры	Вес, W_{ij}^{d}
d_1	Ведение более строгого учета экзаменационных ведомостей	0,8
d_2	Верификация реквизитов экзаменационной ведомости	0,9
d_3	Соблюдение правил пожарной безопасности	0,7

Рис. 4. НКК на основе стратегии снижения рисков

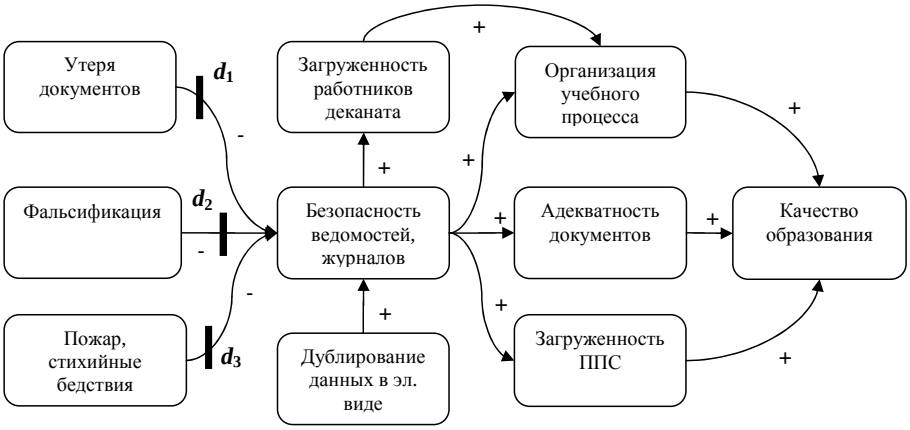

Рис. 5. НКК на основе стратегии изменения характера риска

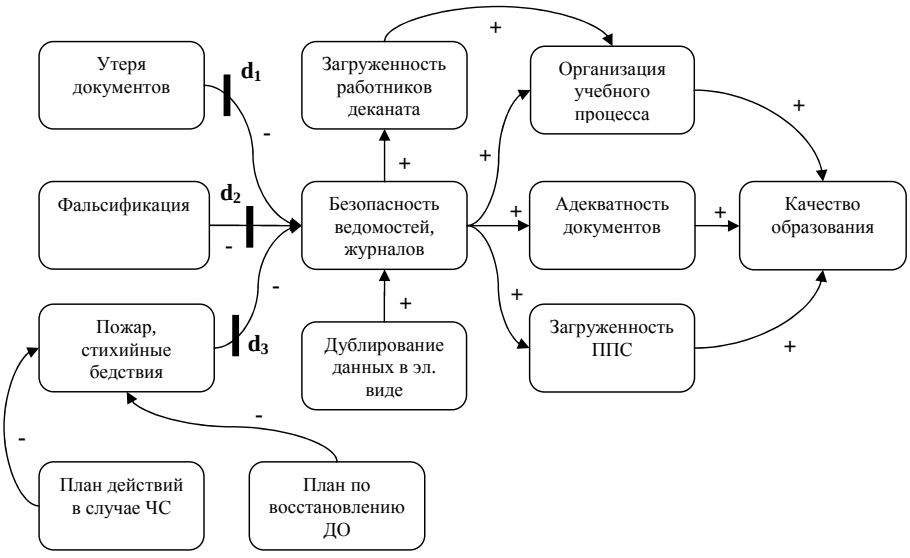

Рис. 6. НКК на основе стратегии принятия риска

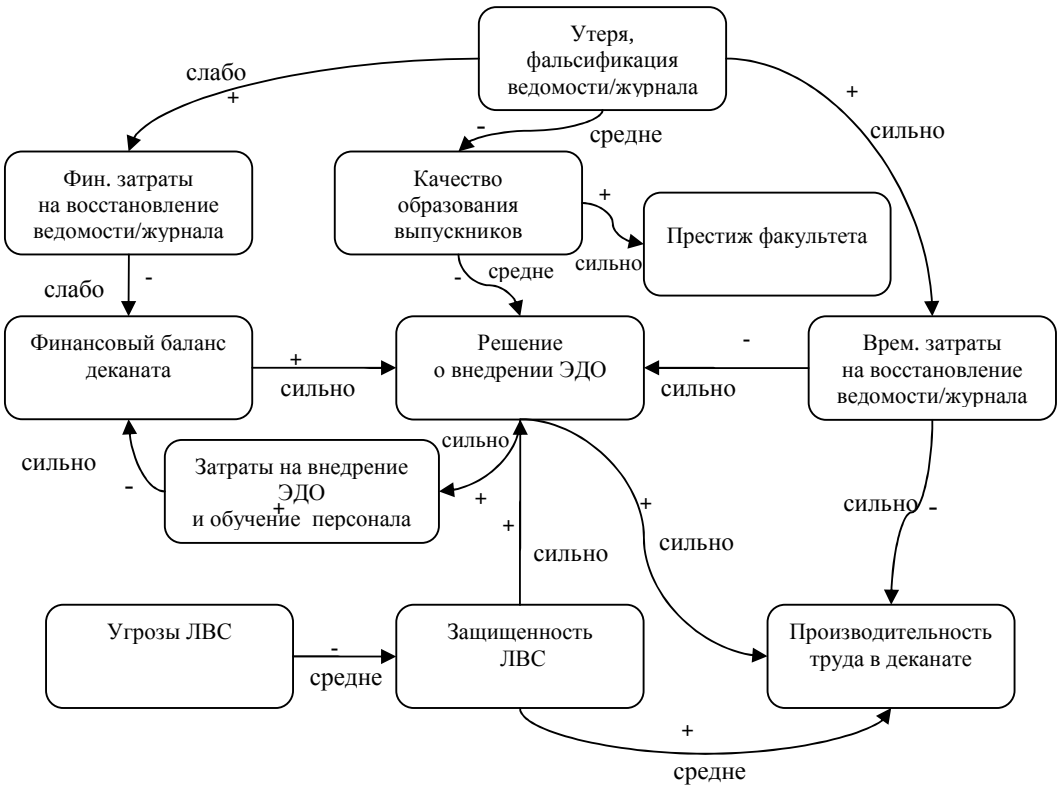

Рис. 7. НКК на основе стратегии уклонения от риска

Совокупная величина риска, полученная при повторном расчете риска с учетом введенных контрмер, уменьшилась на 70%, но она все еще выше допустимой величины вследствие влияния угроз «Утеря документов» и «Пожар/Стихийные бедствия».

Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки. Данная стратегия подходит для угрозы «Утеря документов». Так как это не снижение, а изменение характера риска, то управляющий фактор будет действовать не непосредственно на угрозу, а на базовый фактор (см. рис. 5).

С учетом данной меры защиты совокупная величина риска уменьшилась еще на 10%, однако, все еще остается существенной составляющая риска, связанная с возникновением пожара и стихийных бедствий.

Соблюдение правил противопожарной безопасности существенно уменьшит риск возникновения пожара, но не до нуля. Стихийные бедствия и вовсе непредсказуемы. В таком случае имеет смысл принять данные риски, что отразится на НКК частичной перегруппировкой факторов (см. рис. 6).

Можно уклониться от рисков, которым подвержены бумажные документы, путем переноса документооборота с бумажного на электронные носители. Оценить приемлемость данного решения можно с помощью НКК (см. рис. 7), построенной на основе предыдущей и включающей ее в качестве интегрированной карты нижнего уровня для связи между концептами «Утеря, фальсификация ведомости/журнала» и «Качество образования выпускников».

Целевыми факторами на данной НКК являются не только качество образования, но также производительность труда в деканате. В качестве управляющих факторов были выбраны «Решение о внедрении электронного документооборота» и «Защищенность ЛВС».

На рис. 7 приняты следующие сокращения: ЭДО — электронный документооборот, ЛВС — локальная вычислительная сеть.

Заметим, что НКК отражает, прежде всего, качественное влияние составляющих ее факторов друг на друга. Более детально характер этого влияния и динамику процессов отражает нечеткая когнитивная модель (НКМ), где связи НКК предстают в виде уравнений. Провести моделирование с помощью НКМ можно, используя стандартные существующие пакеты, например, Matlab.

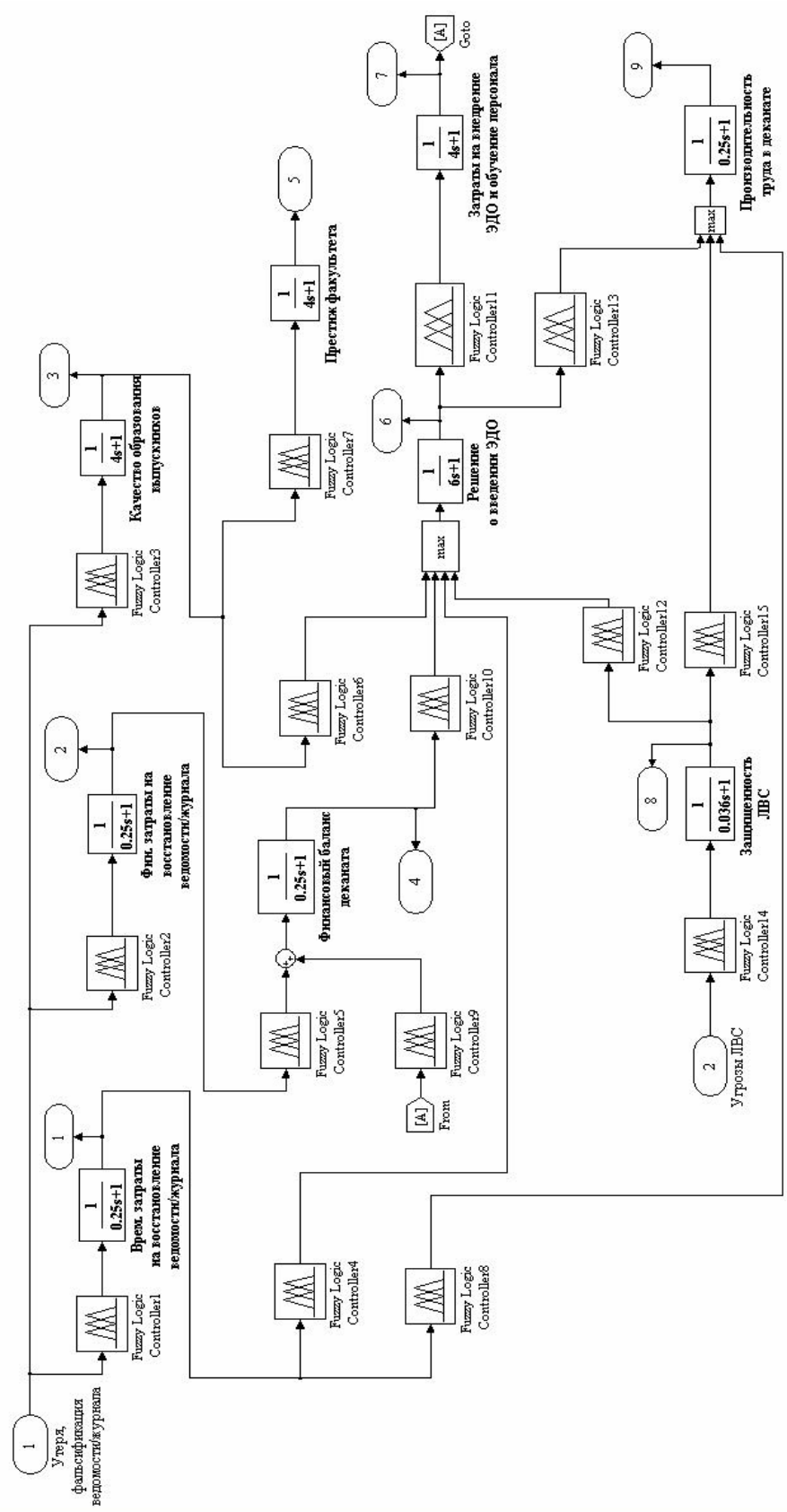

Рис. 8. Нечеткая когнитивная модель (НКМ) воздействия угроз на целевые факторы — «Качество образования», «Престиж факультета», «Производительность труда в деканате»

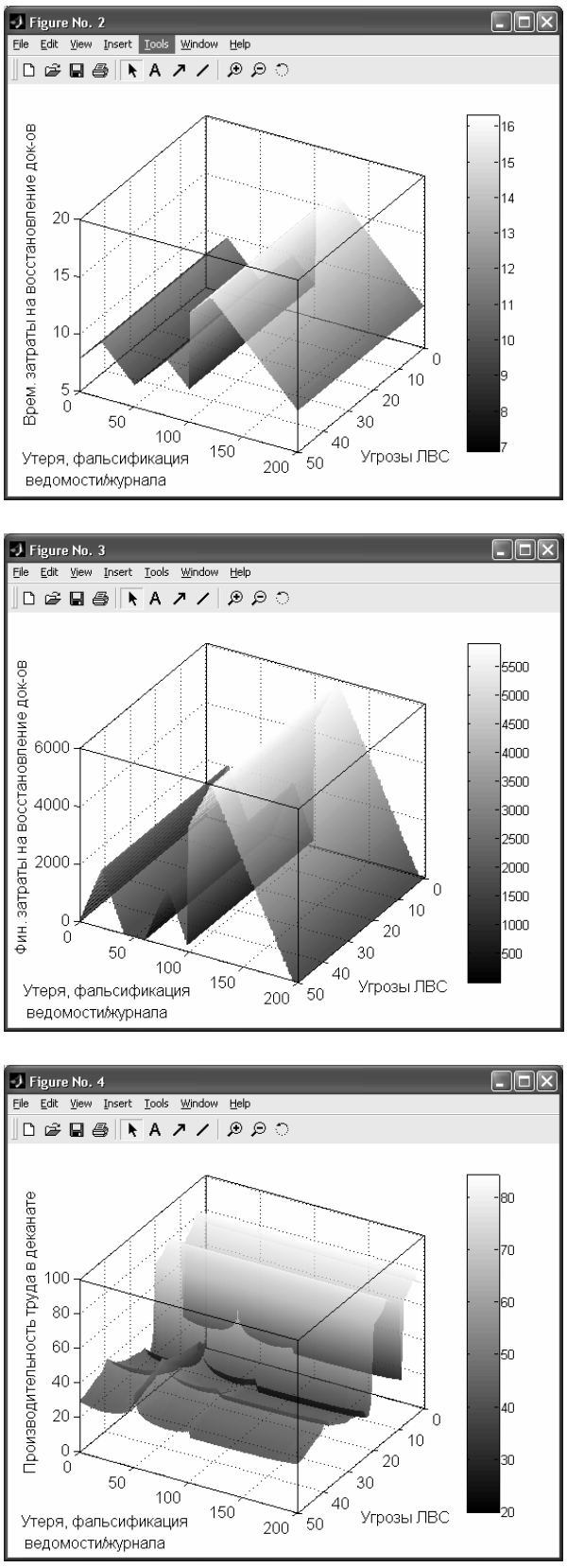

Рис. 9. Графики изменения состояния концептов

Использование приложения Simulink позволяет при этом получать наглядные графики изменения состояния концептов, а также варьировать параметры НКМ, добиваясь наиболее точного отображения моделируемой ситуации.

Для определения весов причинных связей в виде нечетких соотношений при моделировании в среде Matlab используется инструмент Fuzzy Logic Toolbox.

Результаты моделирования НКК, представленной на рис. 7, приведены на 3D-графиках (рис. 9).

Как видно из графиков, в результате совокупного воздействия угроз состояние каждого концепта ухудшилось, сильнее всего пострадала «Производительность труда в деканате». «Временные затраты на восстановление документов» при максимальном воздействии угрозы «Утеря, фальсификация ведомости/журнала» составляют 15 дней, а «Финансовые затраты на восстановление документов» — 6 тыс. рублей, шкала на рисунке показывает интервал изменения значения концепта в течение недели.

ЗАКЛЮЧЕНИЕ

Проблема анализа информационных рисков вуза значительно упрощается и формализуется при использовании нечеткого когнитивного подхода. Достоинством предложенного алгоритма анализа рисков на базе НКК является возможность построения адекватной модели воздействия угроз на защищаемые ресурсы и оценки их последствий при наличии неполной или даже противоречивой исходной информации.

Моделирование НКК в среде Matlab позволяет с достаточной достоверностью анализировать и прогнозировать состояние информационной безопасности вуза и его подразделений. Величина предсказанных рисков и характер изменения состояния целевых факторов позволяют при этом выбрать стратегию управления рисками и подобрать адекватные меры защиты для противодействия информационным угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. **Kosko, B.** Fuzzy Cognitive Maps / B. Kosko // Int. J. of Man-Machine Studies. 1986. Vol. 1. P. 65–75.
2. **Максимов, В. И.** Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач / В. И. Максимов, Е. К. Корноушенко. М. : ИПУ РАН, 1998. Вып. 2.
3. **Петренко, С. А.** Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. Компания АйТи; ДМК Пресс, 2005.

4. **Хрусталев, Е.** Когнитивные технологии в теории и практике стратегического управления (на примере оборонно-промышленного комплекса) / Е. Хрусталев, Д. Макаренко.
5. **Васильев, В. И.** CognitiveRiskAnalyzer. Программа для расчета и анализа рисков с применением нечетких когнитивных технологий. Свидетельство об официальной регистрации программы для ЭВМ № 2006612795 / В. И. Васильев, Р. Т. Кудрявцева, И. А. Савина. Зарег. в Реестре программ для ЭВМ 7.08.2006.
6. **Васильев, В. И.** CognitiveRiskManager. Программа управления информационными рисками. Свид. об офиц. рег. программы для ЭВМ № 2006612170 / В. И. Васильев, Р. Т. Кудрявцева, И. И. Шарипова. Зарег. в Реестре программ для ЭВМ 15.08.2006.

ОБ АВТОРАХ

Васильев Владимир Иванович, проф., зав. каф. выч. техн. и защ. инф. Дипл. инж. по промэлектронике (УГАТУ, 1970). Д-р техн. наук по сист. анализу и автом. управлению (ЦИАМ, 1990). Иссл. в обл. многосвязн., многофункц. и интел. систем.

Савина Ирина Александровна, асп. той же каф. Дипл. спец. по защ. инф. (УГАТУ, 2006). Готовит дис. в обл. инф. безопасности.

Шарипова Ирина Ильгизовна, асп. каф. ВТ и ЗИ. Дипл. спец. по защите информации по спец. «Комплексная защита объектов информатизации» (УГАТУ, 2006). Иссл. в обл. информационной безопасности.