ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2014. Т. 18, № 3 (64). С. 253–260 http://journal.ugatu.ac.ru

УДК 004.056

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

В. И. Васильев[1], Р. Т. Кудрявцева[2], В. А. Юдинцев[3]

[1] vasilyev@ugatu.ac.ru, [2] cudrt@mail.ru, [3] yudintsev@rambler.ru

ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 17 апреля 2014 г.

Аннотация. В работе исследуются вопросы оценки информационных рисков на основе когнитивного моделирования информационной системы. Описывается программный продукт FCMBuilder, автоматизирующий процесс оценки рисков на основе построения нечеткой когнитивной карты.

Ключевые слова: информационная безопасность; информационные риски; когнитивное моделирование; нечеткая когнитивная карта.

Решение вопросов обеспечения информационной безопасности и управления защитой информации сегодня становится жизненно необходимым для существования и развития любой современной организации.

Разработанная в последнее время теория и практика информационной безопасности (ИБ), в том числе международная и отечественная нормативно-правовая базы, во многом облегчают решение задач обеспечения безопасности информационных систем (ИС). Вместе с тем многие вопросы анализа безопасности информационных систем и построения эффективной и оптимальной системы защиты информации (СЗИ), адекватной сложившимся угрозам, остаются недостаточно проработанными.

Сложность решения задачи анализа безопасности информационных систем состоит:

- в большой степени неопределенности и разнообразии возможных сценариев атак на ИС и модели поведения атакующих;
- сложности определения ущерба и последствий нарушения безопасности для ведения бизнеса и окружающей среды;
- недостаточной квалификации и снижения уровня лояльности сотрудников;
- обострении конкуренции, и как следствие – активизации промышленного шпионажа, роста числа хакерских атак и т. п.

Теория и практика информационной безопасности нашла отражение в международных и национальных стандартах нового поколения в области ИБ, учитывающих современное состояние информационных технологий и практические аспекты организации режима ИБ на предприятии. При этом основополагающим документом, определяющим цели, задачи и механизмы управления защитой информации на уровне организации (предприятия), является политика безопасности (security policy).

Анализ различных подходов к построению политики безопасности организации показывает, что центральное место при обеспечении режима ИБ занимает проблема оценки информационных рисков и управления рисками (Risk Management) [1, 2]. Риски ИБ представляют собой серьезную угрозу для бизнеса, так как приводят к возникновению потенциальной возможности финансовых убытков, потери репутации и доверия клиентов, невозможности выполнения основных бизнес-процессов и других видов ущерба. Поэтому анализ информационных рисков на сегодняшний день является актуальной задачей для современного бизнеса, позволяющей контролировать безопасность ведения бизнеса и принимать обоснованные решения.

Управление информационными рисками легло в основу стратегии и оперативного управления (менеджмента) в области защиты информации. Под управлением информационными рисками при этом понимается системный процесс идентификации, контроля и уменьшения информационных рисков в соответствии с целями и задачами, изложенными в политике безопасности предприятия для поддержания заданного уровня безопасности и непрерывности бизнеса. Основная задача оценки рисков –

идентифицировать и оценить наиболее значимые для бизнеса компании информационные риски. Кроме того, оценка информационных рисков позволяет оценивать эффективность использования внедренных средств защиты по критерию «эффективность – затраты».

В настоящее время известно более десятка различных стандартов и спецификаций, определяющих процедуры управления информационными рисками, такие как:

NIST SP 800-37:2010. Guide for Applying the Risk Management Framework to Federal Information Systems (Управление рисками ИБ в федеральных информационных системах);

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Однако существующие стандарты во многом носят декларативный характер, устанавливают не конкретные методы управления рисками ИБ, а только общий подход. Каждая организация должна определить свой собственный подход к управлению рисками, в зависимости от решаемых ею задач и специфики объекта защиты.

В соответствии с рекомендациями, изложенными в стандартах, управление информационными рисками любой компании предполагает следующие этапы:

- выбор системы оценок, разработка или выбор методики эффективной оценки рисков и соответствующего инструментария;
- проведение оценки рисков;
- выбор контрмер противодействия угрозам и управления рисками;
- выбор средств контроля и управления рисками, обеспечивающих режим ИБ;
- сертификация системы управления ИБ на соответствие стандартам безопасности (аудит ИБ).

Таким образом, оценка информационного риска является центральным звеном при определении уровня безопасности предприятия.

МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ

Как уже отмечалось, известные стандарты и опубликованные в открытой печати корпоративные документы, относящиеся к сфере ИБ, содержат только общие методики и рекомендации по анализу и управлению информационными рисками. Как правило, каждая компания сама разрабатывает собственную методику анализа рисков или заказывает ее специализированным организациям. Эти методики учитывают особенности деятельности компании, специфику ведения бизнеса, применяемых информационных технологий и другие факторы. Данные методики, как правило, относятся к разряду «know-how» и обычно не публикуются.

Большинство известных инструментальных средств программного обеспечения (ПО) анализа рисков разработаны в соответствии требованиями международного стандарта ISO/IEC 17799; их условно можно разделить на ПО базового уровня и ПО полного (детального) анализа рисков.

COBRA (ПО базового уровня фирмы C&A Systems Security Ltd) – анализ рисков производится на основе ответов на тематические «вопросники» (несколько десятков вопросов). После автоматической обработки ответов и некоторых соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению. При этом перечень учитываемых требований можно дополнить другими различными требованиями нормативно регулирующих органов.

RiskWatch – служит для идентификации и оценки уровней угроз, обнаружения уязвимостей, оценки соответствия требованиям нормативной базы, предсказания размеров возможных потерь и выработки контрмер. В качестве критериев для оценки и управления рисками при этом используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата (окупаемости) инвестиций (Return on Investment, ROI). Для выявления возможных уязвимостей используется опросник, включающий более 600 вопросов.

Метод **RA2 art of risk –** разработан фирмами AEXIS Security Consultants и XiSEC Consultants Ltd для оценки и управления информационными рисками коммерческих предприятий. Этот метод реализует простой для понимания процессный подход и позволяет создать систему управления информационной безопасности в соответствии со стандартами BS 7799-2 и ISO/IEC 17799. Для оценки и управления рисками используется информация, полученная из различных источников в организации.

Метод CRAMM (ПО полного анализа рисков) – наиболее распространенный метод анализа и управления рисками, относится к категории CASE-средств. В настоящее время имеется до

10 версий метода, рассчитанных на требования армии, государственных учреждений, финансовых структур, частных организаций. Оценка уровней дается по качественной шкале. Механизм вывода оценок риска – табличный.

ГРИФ (российская компания Digital Security) – анализ рисков ИС осуществляется путем построения моделей ИС компании, угроз, уязвимостей, злоумышленника, на основании которых проводится анализ защищенности каждого вида информационного ресурса. Для анализа используются экспертные оценки, рассчитывается риск от действия трех базовых угроз: угрозы конфиденциальности, целостности и отказа в обслуживании.

КОНДОР – ПО разработки и управления политикой безопасности ИС включает в себя систему ГРИФ. Производится оценка на соответствие требованиям стандартов безопасности ISO 17799, ISO 27001. Значения весов различных требований получаются на основе опыта экспертов и могут меняться в зависимости от специфики анализируемой компании.

Все рассмотренные выше методики имеют ряд недостатков:

- не обладают достаточной наглядностью («прозрачностью») принятых решений;
- имеют в основном качественный характер и сводятся к формальной проверке выполнения (или невыполнения) требований стандартов ИБ;
- в данных методиках плохо проработаны вопросы количественной оценки ущерба, вызванного воздействием угроз на информационные и материальные ресурсы (как правило, оценка этих ресурсов производится только по качественной шкале);
- трудно выявить чувствительность тех или иных оценок ущерба по отношению к основным дестабилизирующим факторам или уязвимостям ИС.

КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ

В последние годы для решения задач анализа и управления рисками все шире применяются методы когнитивного моделирования. Под когнитивным моделированием понимается моделирование некоторой предметной области в виде когнитивной карты, объектами которой являются понятия данной предметной области (концепты) и связи между ними, выраженные в соотношениях влияния (казуальные соотношения). В общем случае когнитивная карта – это математическая модель исследуемой системы, представленная в виде ориентированного взвешенного графа. Узлы этого графа представляют собой концепты, отображающие некоторые атрибуты, факторы, состояния системы, дуги – причинные (или каузальные) связи между ними, а веса этих связей определяют силу влияния концептов друг на друга [3].

Преимущества когнитивного моделирования заключаются в возможности моделирования слабоструктурированных (плохо формализуемых) систем, которые характеризуются неполнотой или неопределенностью знаний о них. Когнитивный анализ объекта исследования позволяет:

- увидеть общую картину анализируемой проблемы;
- прогнозировать направления развития системы (ситуации);
- выявить факторы, влияющие на развитие ситуации;
- выработать стратегию действий;
- предложить альтернативные варианты решения задачи;
- формализовать процессы принятия решений;
- получить как качественные, так и количественные характеристики рассматриваемой ситуации;
- повысить качество и обоснованность принимаемых решений.

Оценка информационных рисков, основанная на построении нечеткой когнитивной карты (НКК) применительно к ИС, позволит [4]:

- оценить текущее состояние ИБ и достаточность организационных, процедурных и технических средств защиты по заданию допустимого уровня рисков;
- выявить наиболее опасные угрозы и уязвимости, влияющие на ИС (бизнес-процессы);
- оценить возможный ущерб от действия угроз на ИС;
- дать оценку необходимых затрат на организацию мероприятий по обеспечению ИБ, обосновать размер необходимых финансовых вложений;
- адаптироваться к новым внешним и внутренним угрозам и информационным технологиям;
- дать эффективный и простой механизм принятия решений для служб, занимающихся обеспечением ИБ.

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ПО НКК

В общем случае нечеткая когнитивная карта, используемая для анализа информационных

рисков, представляет собой кортеж множеств [5]:

$$\text{НКК} = \{C, F, W\},$$

где C – множество вершин (концептов); F – множество связей между концептами; W – множество весов этих связей.

Все концепты, описывающие состояние ИБ можно разделить на следующие типы:

1) *информационные активы* $\{C^S_m\}$, нуждающиеся в защите, потеря которых может принести значительный ущерб;

2) *дестабилизирующие факторы* $\{C^U_i\}$, представляющие собой различные угрозы (опасности) ИБ;

3) *целевые факторы* $\{C^G_j\}$ – виды ущерба, критичные для успешного функционирования предприятия;

4) *управляющие факторы* $\{C^R_k\}$ – контрмеры, с помощью которых вносятся стабилизирующие воздействия в систему, оказывающие положительное влияние на уровень ИБ.

Для установления силы (веса) связей между концептами используются нечеткие отношения на шкале [0, 1], задаваемые экспертами с помощью функций принадлежности, т.е. в виде термов лингвистической переменной или с помощью числовых значений на той же шкале [0, 1] (рис. 1).

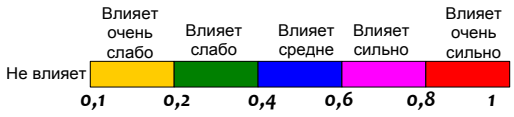

Рис. 1. Шкала для экспертной оценки взаимовлияния концептов

С позиции когнитивного моделирования целями анализа и управления информационными рисками является выявление и минимизация степени воздействия угроз (дестабилизирующих факторов) на базисные (информационные активы) и целевые факторы (ущерб).

Построенная НКК позволяет оценить влияние (эффект) как отдельной угрозы, так и совокупности угроз $\{C^U_i\}$ на тот или иной целевой фактор $\{C^G_j\}$ путем вычисления веса соответствующего пути с учетом весов входящих в него связей.

Оценка результирующего влияния входных концептов на выходные концепты НКК производится при этом с использованием операций алгебраического сложения и умножения T-норм (min) и S-норм (max).

Для вычисления общего эффекта от действия концепта C_i^U на концепт C_j^G необходимо найти матрицу достижимости:

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

где $W = \left\| W_{ij} \right\|_{n \times n}$ – матрица смежности НКК; W_{ij} – вес связи между i-м и j-м концептами НКК; n – число концептов. Для вычисления элементов матрицы $W^t = \left\| W_{ij}^{(t)} \right\|_{n \times n}$, характеризующих веса дуг для путей длины t, соединяющих произвольный концепт C_i с концептом C_j, используются формулы возведения матрицы W в t-ю степень. Например, элементы матрицы W^2 вычисляются по формуле:

$$W_{ij}^2 = \sum_{k=1}^{n} W_{ik} \times W_{kj}, \qquad (i, j = 1,2,...,n).$$

При нечетких значениях весов W_{ij} операции умножения и сложения необходимо заменить соответственно на операции нахождения минимума и максимума.

Для определения непрямого (т. е. местного) эффекта $T_k(C^U_i \rightarrow C^G_j)$ можно воспользоваться формулой:

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

где $\{W_{ij}\}$ – множество весов связей на пути между концептами C^U_i и C^G_j.

Полный (т. е. суммарный) эффект от воздействия C^U_i на C^G_j равен:

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

где T_k – непрямой эффект между угрозой C^U_i и целевым фактором C^G_j; N –число непрямых эффектов. Значение полного эффекта дает интегральную оценку вероятности реализации i-й угрозы и соответствующей уязвимости защиты в отношении j-го целевого фактора.

Риск j-го целевого фактора по отношению к i-й угрозе (R_{ij}) соответственно составляет:

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

где r_j – ценность (стоимость) j-го ресурса; $T(C^U_i \rightarrow C^G_j)$ – полный эффект воздействия C^U_i на C^G_j. Общий риск от воздействия всего множества угроз можно рассчитать по формуле

$$R = \sum_{i,j} \nu_j \cdot R_{ij},$$

где ν_j – значимость (вес) j-го целевого фактора.

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ FCMBUILDER

Описанное ниже программное средство **FCMBuilder** (Fuzzy Cognitive Maps Builder)

представляет собой универсальное решение для автоматизации анализа и управления рисками с использованием нечетких когнитивных карт [6].

Эта программа позволяет строить нечеткие когнитивные карты, проводить с их помощью анализ информационных рисков и обосновывать выбор состава необходимых контрмер. В результате работы программы строится диаграмма информационных рисков до введения и после введения контрмер, что наглядно отображает итоги работы с нечеткой когнитивной картой. Входной информацией в программе являются числовые и/или текстовые данные. Входными данными являются следующие характеристики НКК:

- типы факторов;
- наименования факторов;
- переменные состояния факторов;
- начальные и конечные состояния факторов.

Выходной информацией являются:

- нечеткая когнитивная карта, представленная в виде взвешенного ориентированного графа;
- матрица достижимости НКК;
- полные эффекты взаимовлияния концептов (до и после внедрения контрмер);
- информационные риски (до и после внедрения контрмер).

Программа позволяет задавать веса связей НКК в виде числовых значений и в виде лингвистических термов и соответственно на выходе получать эффекты взаимовлияния концептов в виде чисел или в виде значений лингвистических термов. Программа имеет удобный интерфейс, позволяющий отображать НКК и необходимую сопроводительную информацию по концептам и связям.

Всего выделено четыре вида концептов – дестабилизирующие факторы (ДФ), промежуточные факторы (информационные активы) (ПФ), целевые факторы (ЦФ) и управляющие факторы (УФ), которые для удобства и наглядности можно выделить цветом. После выбора типа концепта и нажатия мышкой по рабочей области окна программы появляется окно задания концепта, в котором необходимо задать название концепта, его текущее, начальное и предельные значения (рис. 2).

Для целевых факторов дополнительно необходимо задать стоимость в условных единицах и значимость (вес) концепта. Одновременно в рабочем поле автоматически появляется изображение концепта в виде кружка (который в дальнейшем можно перемещать мышкой) и все данные по концепту заносятся в таблицу «перечень концептов и их состояния», расположенную в нижней части окна.

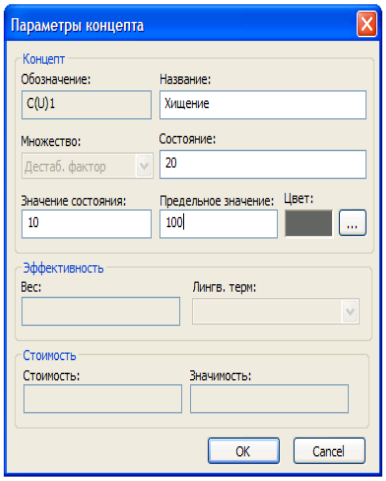

Рис. 2. Окно задания параметров концепта

Далее необходимо выбрать тип задания весов связей: числовые значения (в диапазоне 0 до 1) или лингвистические термы. В случае работы с лингвистическими термами необходимо задать шкалу вводимых переменных из готового списка или задать свою (рис. 3).

Для установления связей между концептами необходимо нажать на кнопку «Связь», расположенную на панели инструментов или в "Главном меню" → "Инструменты", затем соединить два нужных кружка мышкой. В результате получается стрелка в виде дуги, одновременно в таблицу «причинно-следственные связи между концептами», расположенную в нижней части рабочего окна программы, автоматически заносятся все значения связей.

На рис. 4 приведен пример построения НКК для отдела интеллектуальной собственности (ОИС) высшего учебного заведения.

При нажатии на кнопку «Матрица достижимости» можно посмотреть матрицу весов взаимного влияния всех концептов НКК. При нажатии кнопки «Полный эффект», расположенной на панели инструментов или в "Главном меню" → "Инструменты", появляется одноименное окно, в котором отображается полный эффект от всех дестабилизирующих факторов на каждый из заданных целевых факторов.

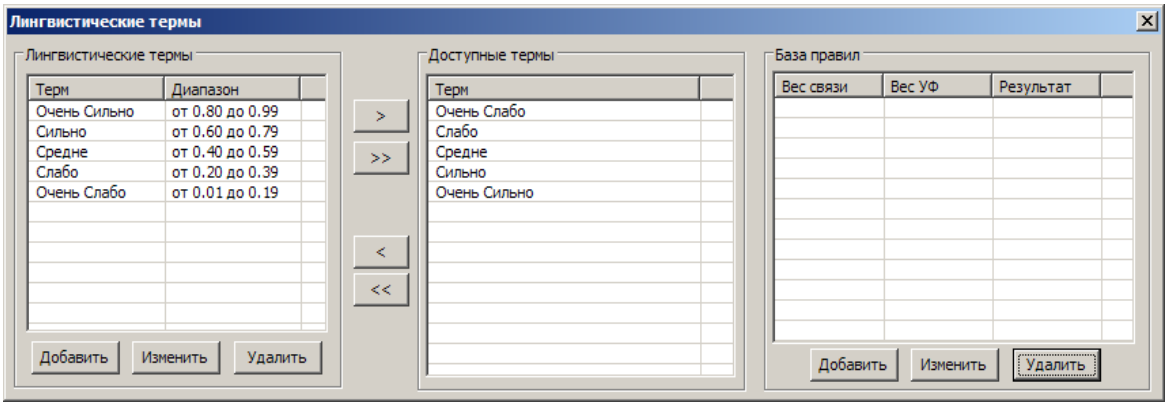

Рис. 3. Установка шкалы задания лингвистических термов

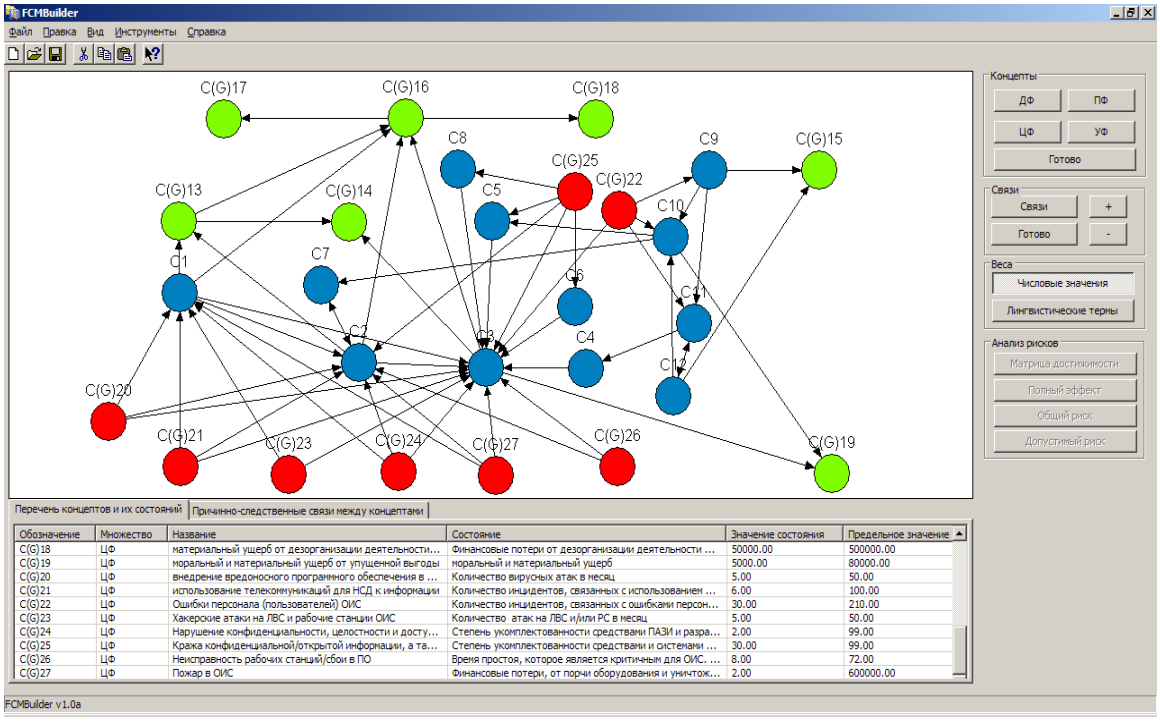

Рис. 4. Нечеткая когнитивная карта для ОИС

Для управления информационными рисками необходимо задать управляющие факторы (контрмеры), их ценность (стоимость) и базу правил для их выбора. Программа автоматически вводит в граф НКК управляющие факторы в виде барьеров, и после пересчета показателей «Полый эффект» и «Общий риск» строится новая диаграмма оценки информационных рисков «После внедрения контрмер», позволяющая визуально сравнить значение информационных рисков до внедрения и после внедрения контрмер.

На рис. 5 показано окно базы правил, в котором задаются правила влияния управляющих воздействий на силу соответствующих связей НКК при задании весов связей в виде значений лингвистических переменных.

Рис. 6 показывает вид построенной НКК с введенными управляющими воздействиями (контрмерами). На рис. 7 представлены результаты расчета рисков для НКК ОИС в условных единицах (у. е.) до и после внедрения контрмер. Первые 7 столбцов в каждом графике показывают уровень рассчитанных рисков от действия отдельно рассмотренных угроз для каждого из 7 заданных целевых факторов. Последний столбец показывает общий риск. Подводя курсор к каждому из столбцов, можно увидеть числовые значения рассчитанных рисков в условных единицах до и после внедрения контрмер, а для общего риска также значения предотвращенного ущерба и стоимость вводимых контрмер (защиты).

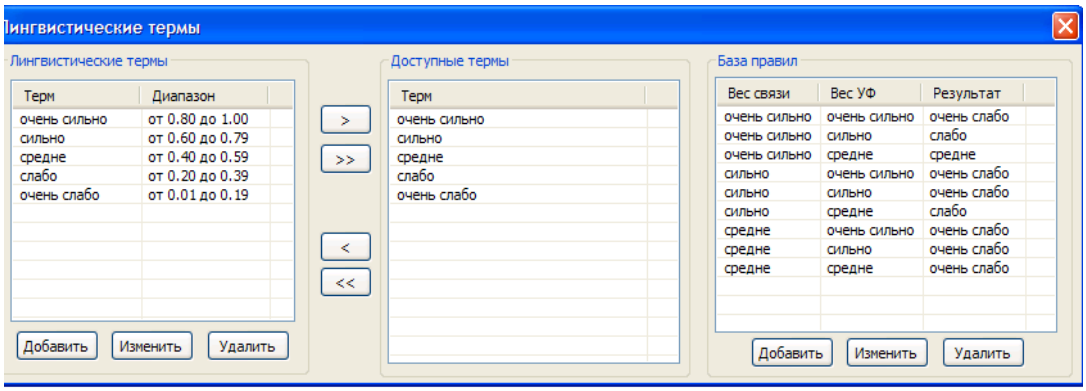

Рис. 5. База правил для управляющих воздействий НКК

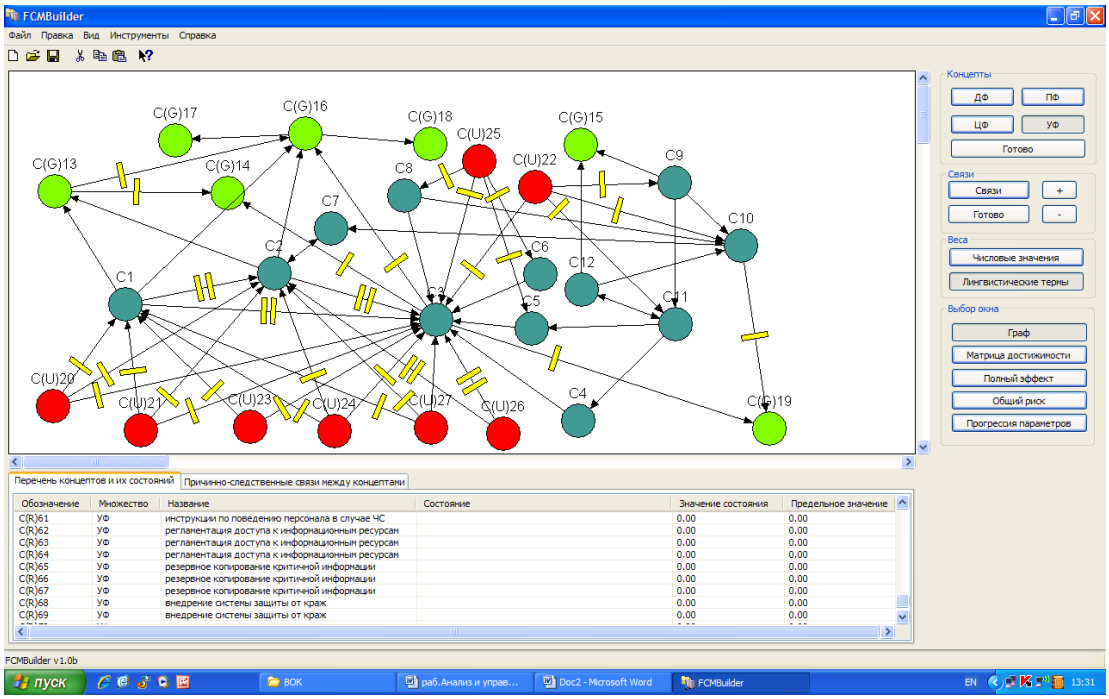

Рис. 6. НКК ОИС после введения управляющих факторов

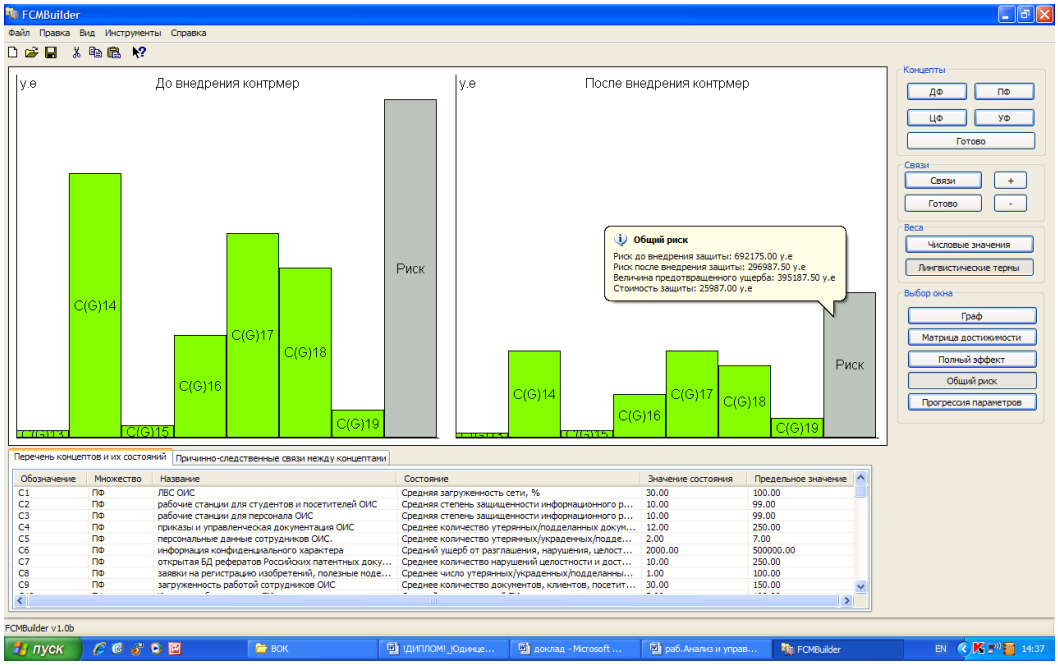

Рис. 7. Диаграмма оценки информационных рисков ОИС до и после внедрения контрмер

Зная значение риска до ($R1$) и после ($R2$) внедрения контрмер, можно сравнить его с допустимым значением риска $R_{\text{доп.}}$ и определить, во сколько раз произошло снижение риска:

$$K = \frac{R_1}{R_2},$$

где R_1 – значение риска до внедрения СЗИ, R_2 – значение риска после внедрения СЗИ.

Можно также рассчитать относительную эффективность принятых контрмер по формуле:

$$Э = \frac{R_1 - R_2}{R_1}.$$

ЗАКЛЮЧЕНИЕ

Таким образом, использование разработанной авторами программы **FCMBuilder** позволяет быстро и наглядно построить НКК, отображающую влияние основных факторов на ИБ. Произвести с ее помощью расчеты по оценке и анализу рисков, выявить наиболее опасные уязвимости в исследуемой ИС, в наглядной форме выявить и оценить эффективность внедренных мероприятий (контрмер) по защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. **Петренко С. А., Симонов С. В.** Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2005. 384 с. **[** S. A. Petrenko, S. V. Simonov, *Information Security Management. Economically safety*, (in Russian). Moscow: DMK Press, 2005. **]**

2. **ГОСТ Р ИСО/МЭК 27001-2006.** Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008. 32 с. **[** *Information technology. Security techniques. Information security management systems. Requirements*, (in Russian), Federal standard R ISO/IEC 27001-2006, Moscow, Standatrinform, 2008. **]**

3. **Борисов В. В., Круглов В. В., Федулов А. С.** Нечеткие модели и сети. М.: Горячая линия – Телеком, 2007. 284 с. **[** V. V. Borisov, V. V. Kruglov, A. S. Fedulov, "Fuzzy models and networks," (in Russian). Moscow: Goryachaya liniya-Telecom, 2007. **]**

4. **Васильев В. И., Кудрявцева Р. Т.** Анализ и управление информационной безопасностью вуза на основе когнитивного моделирования // Системы управления и информационные технологии. 2007. № 1 (27). С. 74–81. **[** V. I. Vasilyev and R. T. Kudryavtseva, "The analysis and management of information security of higher education institution on the basis of cognitive modeling," *Control systems and information technologies*, no. 1 (27), pp. 74-81, 2007. **]**

5. **Гузаиров М. Б., Васильев В. И., Кудрявцева Р. Т.** Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т. 5, № 4. С. 96–101. **[** M. B. Guzairov, V. I. Vasilyev, R. T. Kudryavtseva, "The system analysis of information risks with application of fuzzy cognitive maps, in Infocommunication technologies," vol. 5, no. 4, pp. 96-101, 2007. **]**

6. **Васильев В. И., Кудрявцева Р. Т., Юдинцев В. А.** Универсальное решение для автоматизации анализа и управления рисками с использованием нечетких когнитивных карт (Fuzzy Cognitive Maps Builder): свид. об офиц. рег. программы для ЭВМ № 2007613536 от 21.08.2007. **[** V. I. Vasilyev, R. T. Kudryavtseva, V. A. Yudintsev, "The universal decision for analysis and risk management automation with use of fuzzy cognitive maps (Fuzzy Cognitive Maps Builder)," The Certificate on official registration of the computer program, No. 2007613536, 21.08.2007. **]**

ОБ АВТОРАХ

ВАСИЛЬЕВ Владимир Иванович, проф. зав. каф. выч. техники и защиты информации. Дипл. инж. по промэлектронике (УАИ, 1970). Д-р техн. наук по сист. анализу и автом. управлению (ЦИАМ, 1990). Иссл. в обл. интел. систем инф. безопасности.

КУДРЯВЦЕВА Рима Тимиршаиховна, доц. той же каф. Дипл. инж.-э/мех. (УАИ, 1976). Канд. техн. наук по инф. безопасности (УГАТУ, 2008). Иссл. в обл. оценки рисков инф. безопасности.

ЮДИНЦЕВ Владимир Александрович. Дипл. спец. по защ. информации (УГАТУ, 2007). Иссл. в обл. инф. безопасности.

METADATA

Title: The automated process of information risks evaluation with use of fuzzy cognitive maps.

Authors: V.I. Vasilyev[1], R. T. Kudryavtseva [2], V. A. Yudintsev

Affiliation:

[1] Ufa State Aviation Technical University (UGATU), Russia.

[2] Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] vasilyev@ugatu.ac.ru, [2] cudrt@mail.ru.

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 18, no. 3 (64), pp. 253-260, 2014. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: This paper describes the questions of information risks evaluation on the basis of cognitive modelling. FCMBuilder software automating process for risks evaluation on the basis of fuzzy cognitive map is described.

Key words: information security; information risks; cognitive modeling; fuzzy cognitive map.

About authors:

VASILYEV, Vladimir Ivanovich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer of Electronic Engineering (1970). (UAI., 196x). Cand. of Tech. Sc. (USATU, 1975), Dr. of Tech. Sc (Eng.), (CIAM,, 1990).

KUDRYAVTSEVA, Rima Timirshaihovna, Acc. prof. of Computer Engineering and Information Security. Dipl. Engineer of Electronic Engineering (1976). Cand. of Tech. Sc. (USATU, 2008).

YUDINTSEV, Vladimir Alexandrovich, Dipl. Engineer of Information Security (USATU, 2007).