

На правах рукописи



АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ

АНАЛИТИЧЕСКОЕ И ПРОЦЕДУРНОЕ ОБЕСПЕЧЕНИЕ
ЭКСПЕРТНОЙ СИСТЕМЫ ОЦЕНКИ УСТОЙЧИВОСТИ
ФУНКЦИОНИРОВАНИЯ СЕТЕВЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ

Специальность 05.25.05 – Информационные системы и процессы

Автореферат диссертации
на соискание ученой степени кандидата технических наук

Тамбов – 2014

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Тамбовский государственный технический университет» (ФГБОУ ВПО «ТГТУ»), на кафедре «Информационные системы и защита информации».

Научный руководитель доктор технических наук, профессор
Дидрих Валерий Евгеньевич

Официальные оппоненты: *Скрыль Сергей Васильевич*,
доктор технических наук, профессор,
федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет им. Н. Э. Баумана» (Национальный Исследовательский Университет техники и технологий), профессор кафедры «Защита информации»

Лавлинский Валерий Викторович,
кандидат технических наук, доцент,
федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежская государственная лесотехническая академия», доцент кафедры «Вычислительная техника и информационные системы»

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет инженерных технологий»

Защита состоится 25 июня 2014 г. в 15 часов на заседании диссертационного совета Д 212.260.05 ФГБОУ ВПО «ТГТУ» по адресу: 392000, г. Тамбов, ул. Советская, д. 106, Большой актовывый зал.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБОУ ВПО «ТГТУ» www.tstu.ru.

Автореферат разослан 25 апреля 2014 г.

Ученый секретарь
диссертационного совета

Селиванова Зоя Михайловна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Понятие «сетевые информационные системы (СИС)» уже признано исследователями предметной области информационных систем и технологий. Оно базируется на понятии информационной системы (ИС), которое трактуется как совокупность программно-аппаратных средств, объединенных в систему информационными процессами, направленными на достижение конкретной цели в интересах, как правило, эргатического звена.

СИС предполагают обязательное использование информационных процессов, связанных с передачей информации и организацией распределенной работы пользователей.

На практике имеет место ряд негативных внешних воздействий (НВВ), которые существенно влияют на условия и качество функционирования СИС, снижая устойчивость, и при этом обладают параметрической неопределенностью, недетерминированным характером. Для нейтрализации этих НВВ разрабатываются и применяются средства парирования негативных внешних воздействий (СПНВВ).

Устойчивость функционирования СИС – свойство сохранять набор основных функциональных возможностей системы в различных условиях этого процесса, в том числе в условиях негативных внешних воздействий.

Анализ и оценка показателей этого свойства являются актуальной задачей в практике проектирования и эксплуатации СИС, поскольку на их основе возможно обеспечение заданного уровня устойчивости функционирования.

Степень разработанности темы. В работах российских и зарубежных ученых рассматриваются различные подходы для оценки свойств СИС, в том числе и устойчивости функционирования, влияющих на эффективность и защищенность этих систем, например, в работах: Ю. Ю. Громова, А. А. Малюка, Ж. С. Сарыпбекова, Ю. Е. Мельникова, А. Г. Додонова, В. М. Вишневецкого, Ю. Е. Малашенко, М. Г. Кузнецова, J. H. Dinitz, B. Hotmann, C. J. Colbourn, S. Tani и др. Предлагаемые ими подходы не учитывают при получении оценки риска и оценки опасности НВВ такие факторы, как важность ресурсов и ценность обрабатываемой информации; требуемый уровень устойчивости функционирования, учитывающий эти факторы; то, что тип исследуемой системы влияет на оценку показателя риска.

В настоящее время на практике используется множество похожих интеллектуальных информационных систем (ИИС), предназначенных для оценки защищенности информационных систем, однако не существует ИИС для проведения анализа и оценки устойчивости функционирования СИС при НВВ. Примерами наиболее известных ИИС являются: АванГард (Россия), Risk Watch (США), CRAMM (Великобритания). Анализ возможностей этих систем показывает, что они обладают следующими недостатками: не обеспечивают многофакторную оценку устойчивости через степень риска, зависящую от важности используемых ресурсов и ценности информации; не реша-

ют оптимизационных задач по выбору способов и средств парирования НВВ при построении оценок устойчивости СИС и др.

Таким образом, актуальная практическая задача заключается в построении экспертной системы (ЭС), позволяющей оценивать устойчивость функционирования СИС при НВВ с учетом важности ресурсов и ценности информации, а также генерировать рекомендации по ее улучшению.

В свою очередь – решаемая научная задача заключается в исследовании и разработке моделей информационных процессов в экспертной системе, учитывающих многофакторность условий функционирования СИС и оптимизирующих подбор СПНВВ при заданном уровне устойчивости.

Цель работы: обеспечение заданного уровня устойчивости функционирования СИС при НВВ на основе экспертной оценки риска ее нарушения и генерации рекомендаций.

Задачи исследования:

1. Провести анализ особенностей процесса функционирования СИС в аспекте устойчивости, построить структурную модель знаний для многофакторного оценивания устойчивости функционирования СИС.

2. Разработать аналитическую и процедурную модели оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ.

3. Синтезировать структуру экспертной системы оптимального выбора СПНВВ, обеспечивающую требуемую устойчивость функционирования СИС. Определить механизм формирования рекомендаций обеспечения устойчивости.

Объект исследования: процесс функционирования СИС.

Предмет исследования: модели информационных процессов в экспертной системе оценки устойчивости функционирования СИС.

Научная новизна результатов исследования:

1. Разработана структурная модель знаний для многофакторного оценивания устойчивости функционирования СИС, отличающаяся учетом факторов, которые характеризуют опасность НВВ и надежность защиты применением соответствующих средств и способов защиты, важность главным образом информационных ресурсов СИС, влияющих на устойчивость функционирования СИС.

2. Предложена аналитическая модель оптимальной оценки уровня устойчивости функционирования СИС при НВВ, отличающаяся использованием показателей ценности информации, важности ресурсов СИС и рисков от НВВ, получаемых экспертным путем.

3. Разработана процедурная модель оценки факторов устойчивости функционирования СИС при НВВ, отличающаяся использованием продукционных правил, определяющих ценность информации путем обработки нечетких характеристик важности ресурсов, опасности НВВ и надежности СПНВВ.

4. Синтезирована структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, отличающаяся модулем оптимизации затрат на реализацию СПНВВ в условиях заданных НВВ.

Теоретическая и практическая значимость работы:

1. Разработанные модели являются развитием методологического аппарата исследования сетевых информационных систем, функционирующих в условиях негативных воздействий и подбора эффективных средств парирования этих воздействий.

2. Полученные модели позволяют построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ, оптимизировать набор СПНВВ и выработать рекомендации по обеспечению заданного уровня устойчивости.

Реализация и внедрение результатов работы. Основные результаты исследований использованы: в учебном процессе по специальности «Информационные системы и технологии» на кафедре «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ»; в научных исследованиях и разработках по оценке свойств функционирования СИС ООО «КОНУС-ИТ» (Тамбов); в методических разработках регионального учебно-научного центра по безопасности информации и для исследования СИС, функционирующих в ФГБОУ ВПО «ТГТУ».

Методология и методы исследования.

Методология исследования основана на принципах системного анализа и общей теории систем. При решении поставленных задач в работе использованы методы: теории вероятностей, нечеткой логики, информационной безопасности, системного анализа, моделирования систем.

Диссертационная работа соответствует п. 1 «Методы и модели описания, оценки, оптимизации информационных процессов и информационных ресурсов, а также средства анализа и выявления закономерностей в информационных потоках» Паспорта специальности 05.25.05 «Информационные системы и процессы».

Положения, выносимые на защиту:

1. Достоверность оценки уровня устойчивости функционирования СИС зависит от полноты учета различных факторов, определяющих эту устойчивость, что обеспечивается применением разработанной структурной модели знаний для многофакторного оценивания.

2. Предлагаемая аналитическая модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ позволяет реализовать оптимальный выбор СПНВВ по заданному уровню устойчивости функционирования СИС или по минимальным затратам на их реализацию.

3. Разработанная процедурная модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ является основополагающей для построения экспертной системы многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ.

4. Применение многофакторной структуры знаний и модуля оптимизации затрат на реализацию СПНВВ в условиях заданных негативных воздействий позволило определить структуру экспертной системы оптимального выбора СПНВВ.

Степень достоверности и апробация результатов. Достоверность научных результатов обеспечивается полнотой системного анализа проблемы синтеза и повышения качества функционирования СИС и подтверждается корректным применением математического аппарата: теории систем, теории принятия решений, математического программирования, нечеткой математики. Для подтверждения достоверности научных выводов в работе проведена сравнительная оценка результатов, полученных с использованием разработанных моделей, с результатами, представленными в научных исследованиях других авторов.

Основные результаты работы обсуждались на всероссийских и международных научных конференциях: «Техника и безопасность объектов уголовно-исполнительной системы – 2011» (Международная научно-практическая конференция, г. Воронеж, 2011), «Актуальные проблемы деятельности подразделений УИС» (Всероссийская научно-практическая конференция, г. Воронеж, 2013), «Математические методы и информационно-технические средства» (VIII Всероссийская научно-практическая конференция, г. Краснодар, 2012), «Прикладная математика, управление и информатика» (Всероссийская научно-практическая конференция, г. Белгород, 2012), «Наука и образование для устойчивого развития экономики, природы и общества» (Международная научно-практическая конференция, г. Тамбов, 2013), «Информатика: проблемы, методология, технологии» (XIV Международная конференция, г. Воронеж, 2014); «Современные информационные технологии» (Международная научно-техническая конференция, г. Пенза, 2014); на научных семинарах кафедр «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ», «Прикладная информатика» Тамбовского филиала Московского государственного университета культуры и искусств.

Объем и структура работы. Диссертация, общий объем которой составляет 120 страниц, состоит из введения, трех глав, заключения, списка использованной научной литературы, включающего 132 наименования научных трудов на русском и иностранных языках. Диссертация содержит 24 иллюстрации и 21 таблицу.

Публикации. Результаты диссертационной работы отражены в 17 публикациях, в том числе в 4 статьях в научных журналах, рекомендованных ВАК.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение посвящается обоснованию актуальности выбранной темы, формулировке цели работы и задач исследования.

В главе 1 «Особенности процесса функционирования сетевых информационных систем в аспекте его устойчивости» по информации из доступных научных публикаций проведен анализ состояния и перспектив развития методологического аппарата оценки устойчивости функционирования СИС путем рассмотрения таких факторов, как: ценность обрабатываемой информации в СИС, характер негативных внешних воздействий, особенности способов

и средств парирования таких воздействий с учетом особенностей человеческого фактора, выявлены основные недостатки существующих подходов к анализу устойчивости СИС.

Многими авторами публикаций отмечается, что до настоящего времени не существует единых универсальных методик анализа свойства устойчивости функционирования СИС. Кроме того, автору не известна единая классификация негативных внешних воздействий из-за большого разнообразия классификационных признаков и типовых вариантов средств и методов их парирования, гарантирующих устойчивость функционирования СИС на требуемом уровне.

Основные недостатки существующих методик оценки устойчивости функционирования СИС связаны, прежде всего, с отсутствием:

- зависимости оценки опасности НВВ от предметного назначения систем (научно-технические, экономические и др.) и ценности обрабатываемой в них информации;
- должного внимания к важности системообразующих ресурсов СИС как существенному фактору при оценке рисков от НВВ;
- учета взаимовлияния элементов СИС в процедуре построения оценки показателей устойчивости в сочетании с экспертными оценками этих показателей.

В результате сформулированы цель работы и задачи исследования, решение которых даст возможность устранить выявленные недостатки.

В главе 2 «Разработка аналитической и процедурной моделей оптимальной многофакторной оценки устойчивости функционирования СИС при НВВ» предложена процедура проведения оценки свойства устойчивости функционирования СИС при НВВ, которая базируется на предложенной структурной модели знаний многофакторного подхода к исследованию оценки устойчивости СИС. Примеры объектно-ориентированных моделей структур знаний по отдельным факторам оценки приведены на рис. 1.

Процедурную модель аналитической оптимальной многофакторной оценки устойчивости функционирования СИС при НВВ предлагается представить следующими этапами:

1. Формирование классификатора (классификационного множества) негативных внешних воздействий:

$$Z_{in} = \begin{bmatrix} Z_G^D & Z_G^K & Z_G^Ц \\ Z_S^D & Z_S^K & Z_S^Ц \\ Z_D^D & Z_D^K & Z_D^Ц \end{bmatrix} \Rightarrow Z_{inj}^q \in Z; \quad Z_{out} = \begin{bmatrix} Z_G^D & Z_G^K & Z_G^Ц \\ Z_S^D & Z_S^K & Z_S^Ц \\ Z_D^D & Z_D^K & Z_D^Ц \end{bmatrix} \Rightarrow Z_{inj}^q \in Z,$$

где Z – множество источников негативных воздействий; in – внутренние негативные воздействия; out – внешние негативные воздействия; q – цель нарушения доступности (Д), конфиденциальности (К) и целостности (Ц); j – тип источника негативных воздействий; $j \in \{S, G, D\}$, S, G, D – множества антропогенных, техногенных и стихийных воздействий соответственно.

2. Формирование матрицы оценок важности ресурсов СИС:

$$U = \begin{bmatrix} U_{и}^д & U_{и}^к & U_{и}^ц \\ U_{ч}^д & U_{ч}^к & U_{ч}^ц \\ U_{ф}^д & U_{ф}^к & U_{ф}^ц \end{bmatrix} \Rightarrow U = U_{gi}^q,$$

где g – тип ресурса СИС (физические, информационные и человеческие); U_{gi}^q – совокупности оценок важности информационных, физических и человеческих ресурсов по цели нарушения доступности (Д, К, Ц), i – индекс ресурса.

3. Определение фактора влияния различных видов воздействий на типовой ресурс СИС:

– для внутренних воздействий

$$Z_{in}U = \{Z_j^q U_g^q \mid Z_j^q \in Z, U_g^q \in U\};$$

– для внешних воздействий

$$Z_{out}U = \{Z_j^q U_g^q \mid Z_j^q \in Z, U_g^q \in U\}.$$

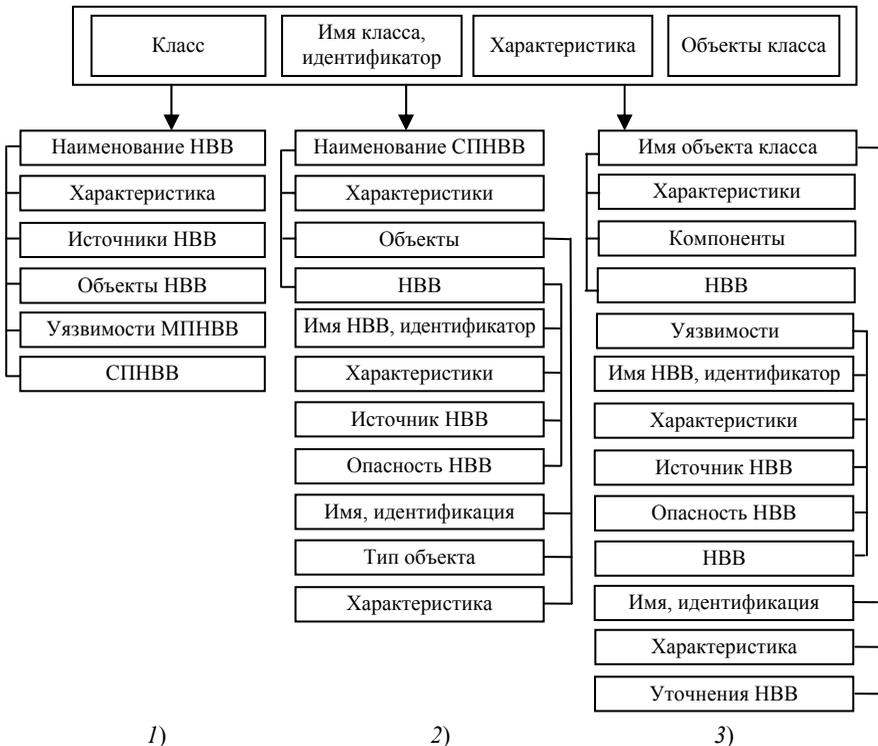


Рис. 1. Объектно-ориентированная модель структуры знаний для идентификации: 1 – НБВ; 2 – СПНБВ; 3 – ресурсы СИС

4. Определение фактора ценности информации: для лингвистических переменных «класс ценности информации», «важность ресурсов», «опасность НВВ», «надежность СПНВВ» и «экономические расходы на восстановление информации» методом экспертных оценок определяются параметры трапецидальной функции принадлежности. В оценках использованы термножества: критическая, важная, средняя, низкая.

Разработаны соответствующие производные правила определения нечетких оценок, факторов ценности информации.

5. Оценка свойства устойчивости функционирования СИС, основанная на анализе рисков от реализации предполагаемых НВВ.

$$P_{ji}^q = O_j^q V_i^q (1 - W_{1i}^q E_{1j}) \dots (1 - W_{di}^q E_{dj}),$$

$$E_{dj} = \begin{cases} 1, & \text{если } d\text{-е СПНВВ включен для } j\text{-го НВВ,} \\ 0, & \text{в противном случае,} \end{cases}$$

где P_{ji}^q – риск нарушения устойчивости при j -м воздействии, которое направлено на i -й ресурс с целью нарушения q ; O_j^q – оценка опасности j -го воздействия, которая характеризуется величиной ущерба и вероятностью появления; W_{di}^q – оценка надежности d -го средства парирования воздействия, которая характеризуется вероятностью их преодоления; V_i^q – оценка важности i -го ресурса по Д, К и Ц; E_{dj} – величина действующего временного парирования НВВ.

$$W_i^q = \frac{1}{x} \sum_{j=1}^x P_{ji}^q,$$

где W_i^q – риск нарушения устойчивости i -го ресурса по Д, Ц, К негативном воздействии; x – количество воздействий, направленных на этот же ресурс.

$$G_i^q = \min \left\{ 1, \frac{|1 - W_i^q|}{T_i^q} \right\},$$

где G_i^q – обобщенная оценка устойчивости функционирования i -го ресурса СИС в целом по Д, Ц, К; T_i^q – требуемый уровень устойчивости функционирования i -го ресурса СИС по Д, Ц, К.

$$T_i^q = V_i^q L,$$

где L – ценность обрабатываемой информации в СИС.

$$Q_s^q = \frac{\sum_{i=1}^n V_{is}^q G_{is}^q}{\sum_{i=1}^n V_{is}^q},$$

где Q_s^q – обобщенная оценка устойчивости функционирования s -го объекта по Д, Ц, К; V_{is}^q – оценка важности i -го ресурса s -го объекта по Д, Ц, К; G_{is}^q – оценка устойчивости i -го ресурса s -го объекта по Д, Ц, К.

$$W^q = \frac{\sum_{i=1}^n V_i^q G_i^q}{\sum_{i=1}^n V_i^q},$$

где W^q – обобщенная оценка устойчивости функционирования СИС в целом по К, Д, Ц.

Предлагаемая модель оценки свойства устойчивости позволила сформулировать две оптимизационные задачи по выбору СПНБВ.

Прямая задача. С целью обеспечения максимального уровня устойчивости функционирования каждого объекта СИС выбрать оптимальный состав средств и способов парирования негативных воздействий при ограничении на заданный уровень возможных затрат на реализацию такого парирования:

$$\left\{ \begin{array}{l} Q_s^q = \frac{\sum_{i=1}^n V_{is}^q G_{is}^q}{\sum_{i=1}^n V_{is}^q} \rightarrow \max; \\ \sum_{d=1}^k CN_s \leq C_z, \end{array} \right.$$

где суммарная стоимость всех реализаций средств и способов парирования для s -го объекта

$$CN_s = \sum_{d=1}^k CN_d E_{ds},$$

$$E_{ds} = \begin{cases} 1, & \text{если } d\text{-е СПНБВ включен для } s\text{-го объекта;} \\ 0, & \text{в противном случае,} \end{cases}$$

Важно отметить, что при этом уровень устойчивости функционирования будет не ниже требуемого T_i^q , что соответствует поставленной цели исследований.

Обратная задача. Оптимальным выбором средств и способов парирования негативных воздействий обеспечить минимум затрат на их реализацию при условии обеспечения устойчивости функционирования не ниже требуемой:

$$\left\{ \begin{array}{l} CN_s = \sum_{d=1}^k CN_d E_{ds} \rightarrow \min; \\ Q_s^q = \frac{\sum_{i=1}^n V_{is}^q G_{is}^q}{\sum_{i=1}^n V_{is}^q} \geq T_s^q. \end{array} \right.$$

Таким образом, использование многофакторной оценки устойчивости функционирования СИС в условиях НВВ в качестве целевой функции оптимального выбора СПНВВ дает основание считать эту оценку оптимальной в смысле возможности выбора лучшего варианта СПНВВ.

В главе 3 «Синтез структуры экспертной системы оптимального выбора СПНВВ и механизм формирования рекомендаций обеспечения требуемой устойчивости функционирования СИС» представлена разработанная структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, определен механизм формирования рекомендаций обеспечения устойчивости.

Для решения возникающих задач, характеризующихся неопределенностью и многофакторностью, предложен программный модуль экспертной (интерактивной) подсистемы формирования знаний, используемых как входные данные (рис. 2). Следует учитывать, что факторы отличаются друг от друга

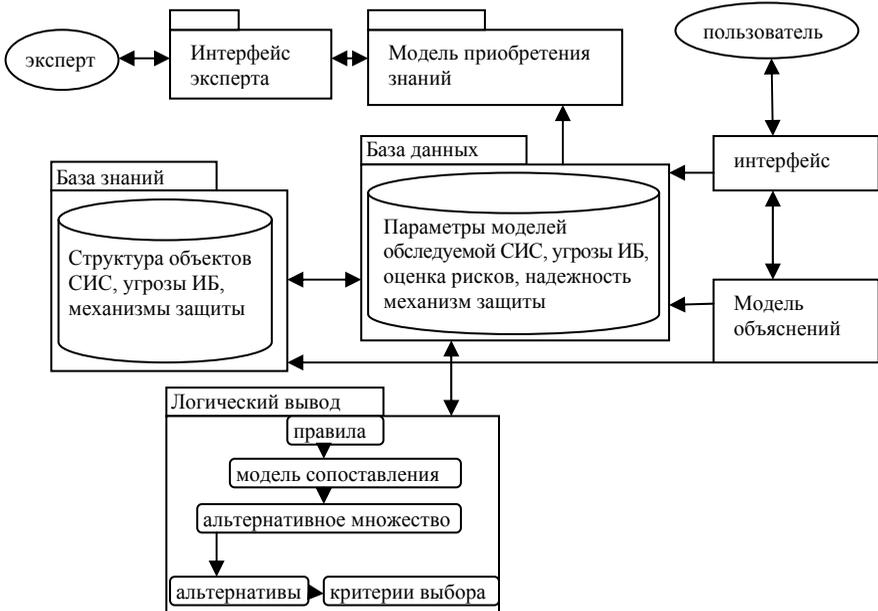


Рис. 2. Структура программного модуля подсистемы формирования базы знаний ЭС оценки устойчивости функционирования СИС при НВВ

уровнем влияния и зависят от типа исследуемой системы. Суть такой системы заключается в том, что она состоит из множества вопросов, которые содержат в себя факторы. Значимость (важность) каждого вопроса определяется типом системы. Вопросу соответствует несколько вариантов ответа. Каждый ответ имеет оценку в диапазоне 0...100%. Для получения важности ответа V каждого вопроса умножаем важность каждого вопроса Q на разницу диапазона ответа M и суммируем полученный результат с нижней границей A :

$$V_n = (Q_n M_n) + A,$$

где n – номер вопроса.

Для оценки влияния этого фактора на систему суммируем важность всех ответов и разделим сумму на их число по формуле:

$$T = \frac{1}{N} \sum_{n=1}^N V_i,$$

где T – общая оценка влияния фактора.

База знаний включает в себя совокупность данных о типах возможных систем, о ресурсах СИС, возможных внешних воздействиях, СПВВ и логические процедуры их обработки. Базы данных предназначены для хранения промежуточных решений или результатов общения системы с оператором экспертной системы.

Разбиение предметной области на множество типов систем и использование интерактивной системы формирования знаний дают возможность исследовать любую информационную систему, учитывая отличие между ними и отличие в уровне влияния одинаковых факторов на разные системы, и улучшить процесс решения возникающих задач, которые характеризуются неопределенностью и многофакторностью.

Построенная в работе диаграмма прецедентов отображает модель поведения системы для оценки функционирования СИС и позволяет описывать требования системы с точки зрения пользователя, который взаимодействует с ЭС. Диаграмма прецедентов предписывает прецеденты к пользователю и описывает взаимодействие между ними (исходящий поток от пользователя и поток откликов, исходящий от прецедентов).

На диаграмме деятельности (рис. 3) прецеденты имеют связь между собой и выполняются как последовательно, так и параллельно.

Работа оператора с экспертной системой описывается следующим алгоритмом:

- 1) задаются тип исследуемой системы и ценность обрабатываемой информации;
- 2) задается структура сегментов СИС из перечня типовых элементов и оценивается важность ресурсов системы;
- 3) задается множество действующих и возможных негативных воздействий на объекты системы;
- 4) задается множество реализуемых средств и способов парирования негативных воздействий для каждого объекта СИС;

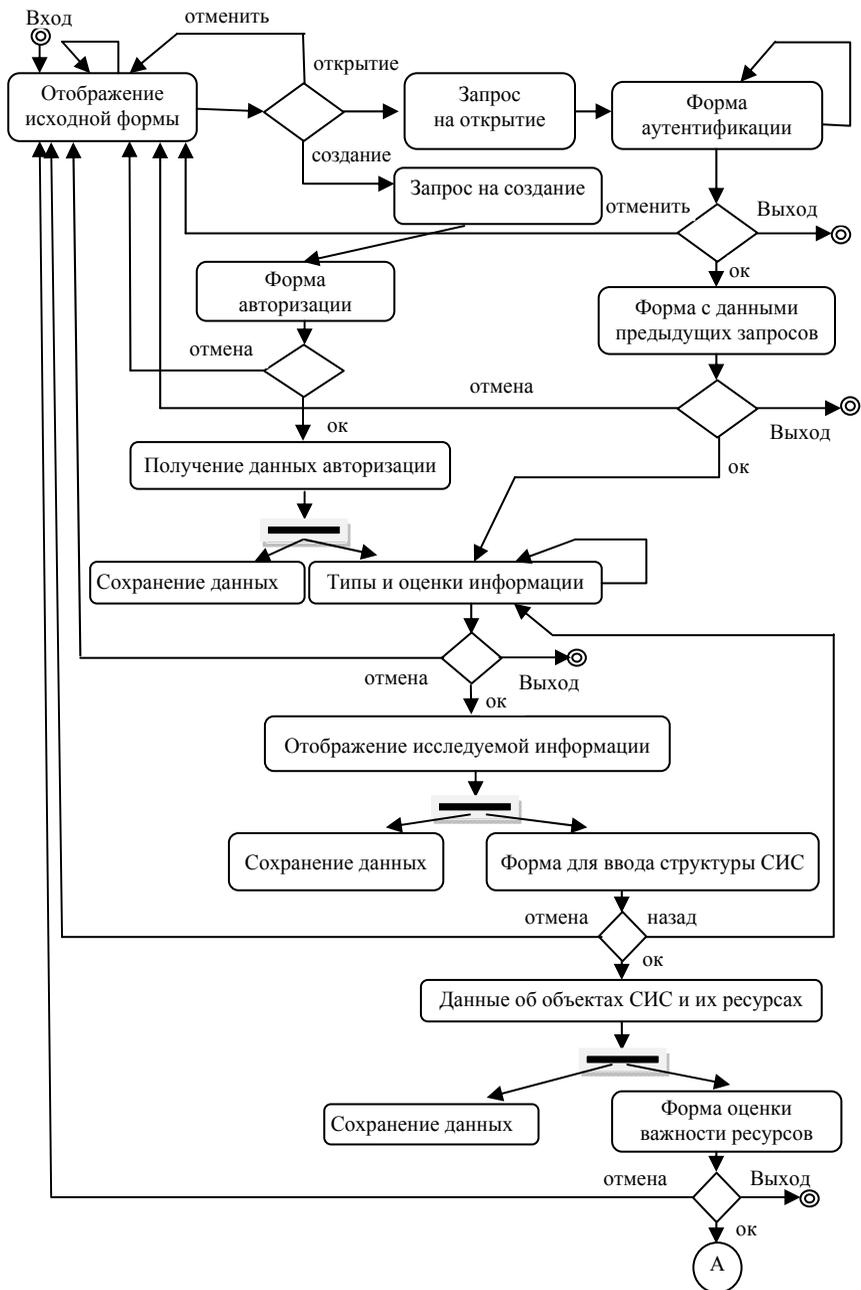


Рис. 3. Диаграмма деятельности процесса оценки устойчивости функционирования СИС

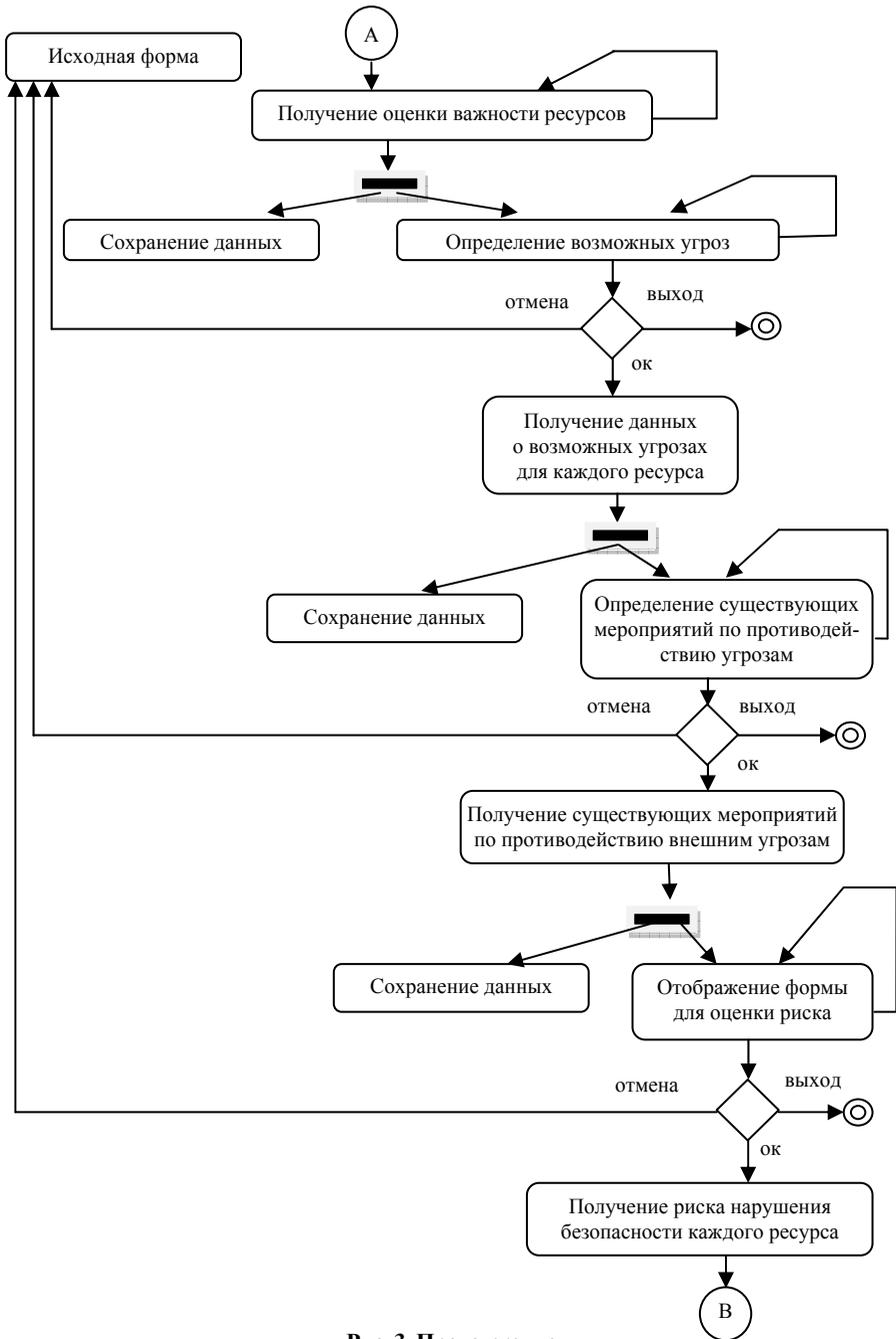


Рис. 3. Продолжение

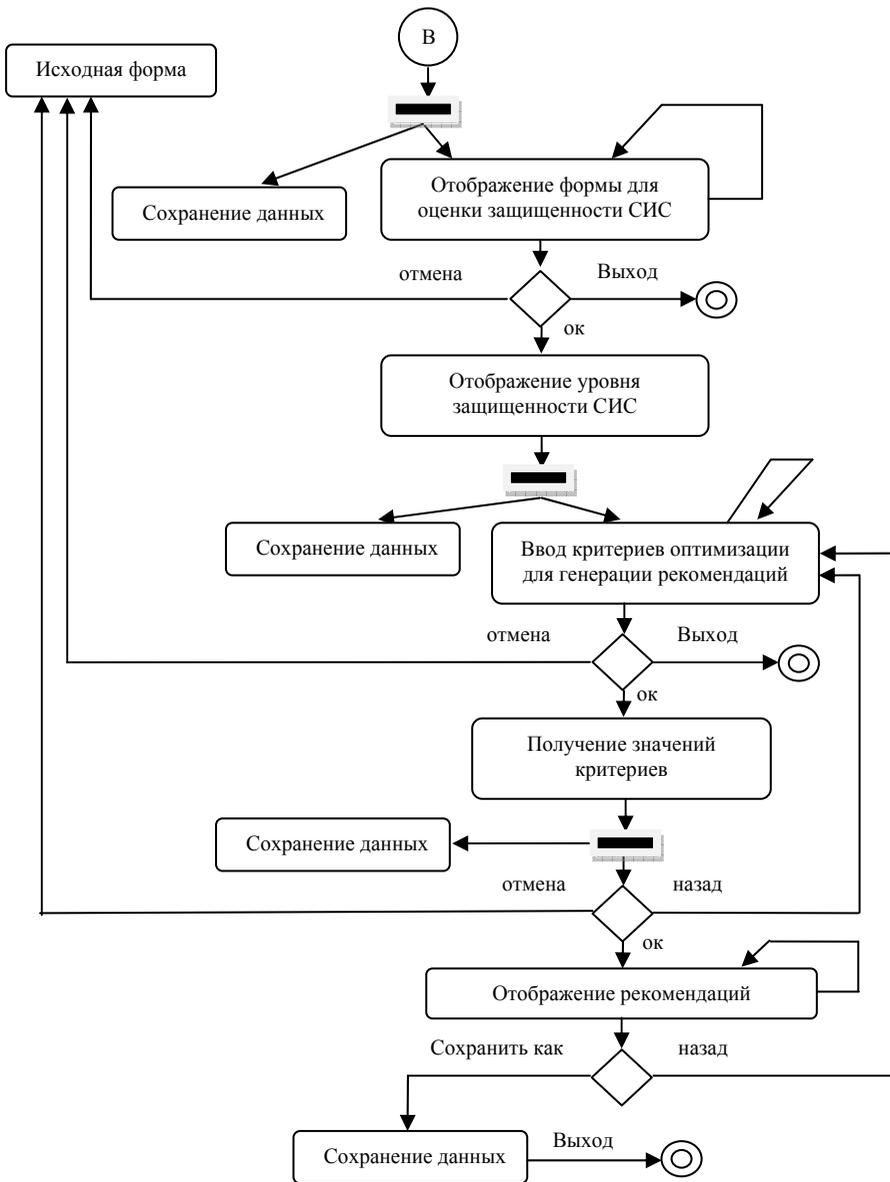


Рис. 3. Окончание

5) задается критерий оптимизации множества средств и способов парирования и рассчитывается уровень устойчивости функционирования.

Эмпирические исследования устойчивости проведены на примере СИС кафедры «Информационные системы и защита информации». Уровень устойчивости повышен на 23,5%, а затраты на поддержание заданного уровня устойчивости СИС снижены на 17,4%. Это позволяет сделать вывод о достижении поставленной цели исследования.

В заключении сформулированы основные результаты работы:

1. Построена структурная модель знаний для многофакторного оценивания устойчивости функционирования СИС, позволяющая разработать программный модуль формирования базы знаний с учетом различных факторов.

2. Предложена аналитическая модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ, позволяющая оптимизировать рекомендуемый набор СПНВВ по заданному уровню устойчивости функционирования или по минимальным затратам на их реализацию в данных условиях.

3. Предложена процедурная модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ, позволяющая построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ.

4. Синтезирована структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, на основе многофакторной структуры знаний и модуля оптимизации затрат на реализацию СПНВВ в условиях заданных НВВ.

5. Вычислительный эксперимент показал возможность улучшения показателей (оценки) устойчивости функционирования СИС на 23,5% и снижения затрат на реализацию оптимального набора СПНВВ на 17,4% .

Таким образом, в диссертационной работе решена научная задача разработки системы моделей информационных процессов в экспертной системе, учитывающих многофакторность условий функционирования СИС и оптимизирующих подбор СПНВВ при заданном уровне устойчивости.

Полученные результаты могут быть рекомендованы к использованию в системах, требующих оптимизации средств защиты от НВВ, обеспечивающих требуемый уровень устойчивости функционирования СИС.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях, рекомендованных ВАК РФ:

1. **Определение** групп негативных внешних воздействий каждого типа на сетевую информационную систему, максимизирующих значение функции ущерба / Ю. Ю. Громов, Ю. В. Минин, М. П. Аль Балуши, А. В. Клишина, А. С. Матвеева // Информация и безопасность. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013. – Ч. 2. – Т. 16. – С. 273 – 276.

2. **Кондратьев, Р. А.** Проблема выявления атак на сетевую информационную систему с использованием математического аппарата машины опорных векторов / Р. А. Кондратьев, К. В. Стародубов, М. П. Аль Балуши // Информация и безопасность. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013. – Ч. 2. – Т. 16. – С. 281 – 284.

3. **Определение** групп негативных внешних воздействий на сетевую информационную систему, максимизирующих значение функции ущерба / Ю. Ю. Громов, Ю. В. Минин, М. П. Аль Балуши, А. В. Клишина, М. А. Шахов // Информация и безопасность. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013. – Ч. 2. – Т. 16. – С. 269 – 272.

4. **Распознавание** негативных внешних воздействий на сетевую информационную систему / М. П. Аль Балуши, А. Ю. Гречушкина, В. Е. Дидрих, Д. В. Зайцев // Приборы и системы. Управление, контроль, диагностика. – 2014. – № 1. – С. 50 – 54.

Статьи и материалы конференций:

5. **Интеллектуальная** информационная система оценки устойчивости функционирования сетевых информационных систем / Н. Ю. Аль-Тамими, М. П. Аль Балуши, М. Ауад, Хак Д. Лыонг, Ю. В. Минин // Техника и безопасность объектов уголовно-исполнительной системы – 2011 : сборник материалов Международной научно-практической конференции : в 2 т. / ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж : ИПЦ «Научная книга», 2011. – Т. 1. – С. 382 – 388.

6. **Некоторые** аспекты интеллектуальной информационной системы оценки функционирования сетевых информационных систем / М. П. Аль Балуши, Н. Ю. Аль-Тамими, М. Ауад, Хак Д. Лыонг, Ю. В. Минин // Техника и безопасность объектов уголовно-исполнительной системы – 2011 : сборник материалов Международной научно-практической конференции : в 2 т. / ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж : ИПЦ «Научная книга», 2011. – Т. 1. – С. 388 – 394.

7. **Оценка** надежности средств парирования внешних воздействий / М. П. Аль Балуши, Н. Ю. Аль-Тамими, М. Ауад, Хак Д. Лыонг, Ю. В. Минин // Техника и безопасность объектов уголовно-исполнительной системы – 2011 : сборник материалов Международной научно-практической конференции : в 2 т. / ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж : ИПЦ «Научная книга», 2011. – Т. 1. – С. 394 – 399.

8. **Подход** к генерации T, S-норм на основе рядов Фурье / Д. В. Поляков, Л. В. Пучков, М. П. Аль Балуши, М. Ауад // Математические методы и информационно-технические средства : труды VIII Всероссийской научно-практической конференции, 22 – 23 июня 2012 г. – Краснодар : Краснодарский университет МВД России, 2012. – 278 с. – С. 165.

9. **К вопросу** проектирования вопросно-ответных информационных систем / А. А. Долгов, М. А. Хорохорин, Ю. В. Минин, М. К. Сила, М. П. Аль Балуши // Актуальные проблемы деятельности подразделений УИС : сборник материалов Всероссийской научно-практической конференции : в 2 т. – Воронеж : ИПЦ «Научная книга», 2013. – Т. 1. – С. 59 – 63.

10. **Процедура** принятия решений в информационной тренажерной системе при условии ограниченного времени прохождения / А. С. Моисеев, Хак Д. Лыонг, М. П. Аль Балуши, Ю.В. Минин // Актуальные проблемы деятельности подразделений УИС : сборник материалов Всероссийской научно-практической конференции : в 2 т. – Воронеж : ИПЦ «Научная книга», 2013. – Т. 1. – С. 106 – 109.

11. **Процедура** оценки надежности средств парирования внешних воздействий / М. П. Аль Балуши, В. А. Горин, А. А. Лебедев, В. Е. Дидрих // Актуальные проблемы деятельности подразделений УИС : сборник материалов Всероссийской научно-практической конференции : в 2 т. – Воронеж : ИПЦ «Научная книга», 2013. – Т. 1. – С. 91–92.

12. **Система** формирования знаний в интеллектуальной информационной системе оценки функционирования сетевых информационных систем / М. П. Аль Балуши, Н. А. Овчинников, В. В. Паладьев, В. Е. Дидрих // Актуальные проблемы деятельности подразделений УИС : сборник материалов Всероссийской научно-практической конференции : в 2 т. – Воронеж : ИПЦ «Научная книга», 2013. – Т. 1. – С. 93 – 95.

13. **Механизм** оценки устойчивости функционирования сетевых информационных систем / М. П. Аль Балуши, В. В. Паладьев, Н. А. Овчинников, В. Е. Дидрих // Актуальные проблемы деятельности подразделений УИС : сборник материалов Всероссийской научно-практической конференции : в 2 т. – Воронеж : ИПЦ «Научная книга», 2013. – Т. 1. – С. 96–97.

14. **Задача** оценки надежности средств парирования внешних воздействий / М. П. Аль-Балуши, С. В. Зайцев, С. А. Копылов, В. Е. Дидрих // Информатика: проблемы, методология, технологии : материалы XIV Международной конференции (6 – 8 февраля 2014 года) : в 3 т. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т. 3. – С. 68 – 71.

15. **Применение** аппарата нечеткой логики для оценки функционирования сетевых информационных систем / М. П. Аль Балуши, С. В. Зайцев, С. А. Копылов, В. Е. Дидрих // Информатика: проблемы, методология, технологии : материалы XIV Международной конференции (6 – 8 февраля 2014 года) : в 3 т. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т. 3. – С. 71 – 75.

16. **Задача** определения оценки устойчивости функционирования сетевых информационных систем / М. П. Аль Балуши, С. В. Зайцев, С. А. Копылов, В. Е. Дидрих // Информатика: проблемы, методология, технологии : материалы XIV Международной конференции (6 – 8 февраля 2014 года): в 3 т. – Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т. 3. – С. 75 – 78.

17. **Применение** аппарата нечеткой логики для оценки функционирования сетевых информационных систем / М. П. Аль Балуши, Е. В. Костерин, И. А. Елисеев, В. Е. Дидрих // Современные информационные технологии : труды Международной научно-технической конференции. – Пенза : Пензенский государственный технологический университет, 2014. – Вып. 19. – С. 24 – 27.

Подписано в печать 23.04.2014.
Формат 60×84/16. 0,93 усл. печ. л. Тираж 100 экз. Заказ № 208

Издательско-полиграфический центр ФГБОУ ВПО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14
Тел. 8(4752) 63-81-08. E-mail: izdatelstvo@admin.tstu.ru