ОТЗЫВ

официального оппонента
на диссертационную работу Аль Балуши Маджед Пир Бахш на тему «Аналитическое и процедурное обеспечение экспертной системы оценки устойчивости функционирования сетевых информационных систем», представленную на соискание ученой степени кандидата технических наук по специальности 05.25.05 - Информационные системы и процессы

В настоящее время известны интеллектуальные информационные системы, предназначенные для оценки защищенности информационных систем, однако нет информации о системах, обеспечивающих проведение анализа и оценки устойчивости функционирования сетевых информационных систем при негативных воздействиях.

Кроме того работы исследователей в области оценки надежности, в частности устойчивости функционирования информационных систем, и предлагаемые ими подходы не учитывают при получении оценки риска и оценки опасности негативных воздействий такие факторы как: важность ресурсов и ценность обрабатываемой информации; требуемый уровень устойчивости функционирования, учитывающий эти факторы; влияние типа исследуемой системы на оценку показателя риска.

Диссертационная работа Аль Балуши Маджед Пир Бахш посвящена исследованию в обозначенном актуальном направлении, а именно – обеспечению заданного уровня устойчивости функционирования сетевых информационных систем при негативных воздействиях на основе экспертной оценки риска ее нарушения и генерации рекомендаций.

Для достижения цели исследования автором в работе были поставлены следующие основные задачи:

– провести анализ особенностей процесса функционирования сетевой информационной системы в аспекте устойчивости, построить структурную модель знаний для многофакторного оценивания устойчивости функционирования системы;

– разработать аналитическую и процедурную модели оптимальной оценки рисков нарушения устойчивости функционирования сетевой информационной системы при негативных воздействиях;

– синтезировать структуру экспертной системы оптимального выбора средств парирования негативных воздействий, обеспечивающую требуемую устойчивость функционирования сетевой информационной системы. Определить механизм формирования рекомендаций обеспечения устойчивости.

В первой главе на основе анализа информации из доступных научных публикаций проведено исследование состояния и перспектив развития методологического аппарата оценки уровня устойчивости функционирования сетевой информационной системы путем рассмотрения таких факторов как: негативные воздействия, ценность обрабатываемой информации в сетевых информационных системах, средства парирования негативных воздействий; обнаружены ключевые слабости методов оценки и анализа устойчивости сетевых информационных систем.

Проделанный анализ позволил автору достаточно обосновано выявить цель работы и задачи исследования, решение которых дает возможность избавиться от недостатков в данной предметной области.

Вместе с тем главе используется множество понятий, в том числе и введенных самим автором, что не всегда оправдано.

Вторая глава диссертации посвящена разработке подхода к формализации процедуры оценки устойчивости функционирования сетевых информационных систем в условия негативных, в том числе и внешних, воздействий. Предложенная формализация учитывает возможные факторы, влияющие на устойчивость функционирования сетевой информационной системы. Предлагаемая модель оценки свойства устойчивости позволила сформулировать две (прямую и обратную) оптимизационные задачи по выбору средств парирования негативных воздействий. Использование многофакторной оценки устойчивости функционирования сетевой информационной системы в условиях негативных воздействий в качестве целевой функции оптимального выбора средств парирования дает основание считать эту оценку оптимальной в смысле возможности выбора

лучшего варианта средств.

В третьей главе работы определены необходимые пользователю функциональные требования, которые представлены для реализации в экспертной системе в виде описанных на естественном языке функций; на основе требований к функционалу синтезирована структура экспертной системы и описаны ее основные элементы и их особенности; объектно-ориентированными моделями в нотации *UML* описано поведение системы в конкретных ситуациях как реакция на действия эксперта/пользователя.

Экспериментальные исследования устойчивости проведены на примере сетевой информационной системы кафедры «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ». Проведенные эксперименты с использованием предлагаемых моделей позволили добиться улучшения показателей устойчивости функционирования системы на 23,5% и снижения затрат на реализацию оптимального набора средств парирования негативных воздействий на 17,4%, что весьма существенно в рассматриваемой предметной области.

В заключении подводятся итоги и делаются выводы, а также обсуждаются некоторые направления дальнейших исследований.

В приложения обосновано вынесены: материалы для проведения экспертного опроса; детальное описание диаграммы прецедентов; состав и структура системы для эмпирических исследований.

Основные научные результаты диссертации достаточно полно отражены в опубликованных автором 17 научных работах, в том числе 4-х статьях в ведущих рецензируемых журналах, а также получили апробацию на семинарах и конференциях различного уровня, включая международные.

Научной новизной, на мой взгляд, обладают все полученные в работе результаты, а именно:

– структурная модель знаний для многофакторного оценивания устойчивости функционирования сетевой информационной системы отличается учетом факторов, которые характеризуют опасность негативных воздействий и надежность защиты применением соответствующих средств и способов защиты, важ-

ность главным образом информационных ресурсов системы, влияющих на устойчивость функционирования системы;

– аналитическая модель оптимальной оценки уровня устойчивости функционирования сетевой информационной системы при негативных воздействиях отличается использованием показателей ценности информации, важности ресурсов системы и рисков от негативных воздействий, получаемых экспертным путём;

– процедурная модель оценки факторов устойчивости функционирования сетевой информационной системы при негативных воздействиях отличается использованием продукционных правил определения ценности информации путем обработки нечетких характеристик важности ресурсов, опасности негативных воздействий и надежности средств парирования;

– структура экспертной системы оптимального выбора средств парирования, обеспечивающая требуемую устойчивость функционирования сетевой информационной системы, отличается модулем оптимизации затрат на реализацию средств парирования в условиях заданных воздействий.

Практическая значимость работы заключается в программной реализации разработанных моделей, которые позволили построить экспертную систему многофакторной оценки устойчивости функционирования сетевых информационных систем в условиях различных негативных воздействий, оптимизировать набор средств парирования таких воздействий и выработать рекомендации по обеспечению заданного уровня устойчивости функционирования системы.

Достоверность представленных результатов обеспечивается корректными математическими формулировками, а также сравнительной оценкой результатов, полученных с использованием разработанных моделей, с результатами, представленными в научных исследованиях других авторов.

В качестве недостатков диссертации необходимо отметить следующее:

1. На стр. 46 автор предлагает классификацию показателя ценности информации, обрабатываемой в информационной системе, используя два класса: характер информации и степень конфиденциальности, хотя очевидно, что по-

добных классов может быть значительно больше. Однако автор не обосновал значимость именно введенных классов.

2. На стр.49 автор предлагает фрагмент модели базы знаний в форме продукционных правил. Остается не ясным, используются ли автором другие виды моделей представления знаний в системе и, почему именно продукционные правила использованы в данной разработке?

3. В работе излишне много внимания уделено аспекту экспертных оценок (подробное описание вопросников), что, на мой взгляд, несколько нивелирует ее научную ценность.

4. В работе автор в качестве базового понятия использует термин «негативные воздействия», но в материалах диссертации не приводятся конкретные примеры таких воздействий, под которые оптимизируются средства парирования.

Отмеченные недостатки не снижают существенно качества работы и не оказывают определяющего влияния на основные теоретические и практические результаты диссертации.

Тема и содержание диссертационных исследований соответствуют 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».

Текст диссертационной работы изложен математически достаточно строго и грамотно. Однако нельзя не отметить иногда встречающиеся в диссертации неудачные формулировки и фразеологические обороты, несколько снижающие общее впечатление о рукописи.

Автореферат соответствует содержанию диссертации и достаточно полно отражает решаемые автором задачи, методику исследований и полученные результаты. Актуальность темы, глубина проработки частных задач, обоснованность научных положений, научная и практическая значимость полученных в работе результатов позволяют сделать следующий вывод.

Вывод: диссертационная работа Аль Балуши Маджед Пир Бахш на тему «Аналитическое и процедурное обеспечение экспертной системы оценки устойчивости функционирования сетевых информационных систем» представляет собой доведенную до практической реализации, законченную научно-исследовательскую работу, имеющую определенную научную новизну и практическую значимость и содержащую решение актуальной научной задачи по разработке моделей информационных процессов в экспертной системе, учитывающих многофакторность условий функционирования информационных систем и оптимизирующих подбор средств парирования негативных воздействий при заданном уровне устойчивости.

Диссертация соответствует требованиям «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор, Аль Балуши Маджед Пир Бахш, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.25.05 – Информационные системы и процессы.

ОФИЦИАЛЬНЫЙ ОППОНЕНТ
Профессор кафедры «Защита информации»
ФГБОУ ВПО «Московский государственный технический университет им. Н.Э. Баумана» (Национальный Исследовательский Университет техники и технологий),
доктор технических наук, профессор

Скрыль Сергей Васильевич

«21» мая 2014 года

105005, Москва, 2-я Бауманская ул., д. 5, стр. 1
тел.: (495) 632-22-47
E-mail: zi@bstu.ru

Подпись профессора Скрыля С.В. заверяю:

ЗАМ. НАЧАЛЬНИКА УПРАВЛЕНИЯ КАДРОВ

А. А. ФЕДОТОВ

«21» мая 2014 года