ОТЗЫВ

официального оппонента Ризванова Дмитрия Анваровича на диссертацию Наседкина Павла Николаевича «Модели и алгоритмическое обеспечение поддержки принятия решений по повышению эффективности системы защиты информации предприятия», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика (технические науки)

Актуальность темы диссертации. Один из трендов современных информационных технологий – это системы автоматизированной поддержки принятия управленческих решений (СППР). Они облегчают управленческие задачи лицам, принимающим решения, и повышают качество решений. Сложность и важность их разработки определяется предметной областью как системой и поставленными задачами. Соискатель П.Н. Наседкин в качестве предметной области выбрал такой сложный технический объект как программно-техническую систему защиты информации (ПТСЗИ). Её целью является минимизация возможного ущерба от несанкционированного вмешательства в работу информационных систем предприятия.

Разработка моделей и алгоритмического обеспечения поддержки принятия решений в выбранной предметной области безусловно значима с прикладной точки зрения – защита информационных активов предприятий и организаций. В то же время эта работа иллюстрирует достаточно общую и отличную от традиционных методику принятия решений, основанную на глубоком структурном анализе средств защиты, выявлении их иерархии, взаимосвязей, оценки полноты реализации мер (в данном случае – программно-технических элементов защиты) с учётом спектра угроз и характера защищаемых ресурсов, эшелонированности защиты и других вопросов. Этот анализ автор положил в основу вычисления показателя эффективности системы защиты, поле чего перешёл к вопросам выработки рекомендаций по повышению уровня защищённости информационных ресурсов в условиях финансовых ограничений, – а это одна из центральных проблем, с которой сталкиваются практические работники независимо от вида защищаемых объектов: информационных, материальных, природных и т.д. Сегодня это делается, как правило, на основе понятия риска, в то время как соискатель избрал иной и, как представляется, достаточно перспективный путь, дополняющий методики, основанные на рисках.

Важно учесть, что рассмотренная система по целевому назначению – снижению ущерба от воздействия неблагоприятных факторов – похожа на многие другие защитные системы в других предметных областях. Причём они также характеризуются многокомпонентностью, иерархией, наличием функциональных элементов и групп элементов различного назначения, дополняющих и усиливающих друг друга, что обеспечивает комплексность и многоуровневость защиты. При этом, как показывает практика, разработка подобных СППР сопровождается изучением и моделированием предметной области, созданием специальных алгоритмов, опирающихся как на новейшие,

так и на классические исследования. Эта задача требует системного взгляда на проблему и потому разработка данных программных средств, вместе с соответствующими моделями, методами и алгоритмами – одна из отличительных особенностей специальности 2.3.1.

В целом, учитывая бесспорную прикладную значимость проведённых исследований и необходимость поиска новых подходов к решению подобных задач, считаю тему и результаты диссертационного исследования актуальными.

Структура и содержание диссертации. Диссертация объемом 171 стр., состоит из введения, 4 глав, заключения, списка сокращений, 2 приложений, списка использованных источников из 183 наименований. Основная часть работы изложена на 167 страницах машинописного текста, содержит 10 таблиц и 37 рисунков.

Во введении обосновывается актуальность работы, формулируется цель исследования, а также ставятся задачи, необходимые для ее достижения. Формулируются научная новизна и основные положения, выносимые на защиту. Определена теоретическая и практическая значимость полученных результатов. Приводится общая характеристика работы.

В первой главе работы проведён обзор предметной области. Освещены методы, методики, стандарты и модели, применяемых управления информационной безопасностью (ИБ). Авто отметил, что существующие методики как правило ориентированы на оценку рисков с использованием экспертных методов, которые характеризуются известным субъективизмом. Сделан вывод, что в рассматриваемой предметной области вместо рисков может быть применён системный подход с использованием онтологического моделирования. Показана значимость онтологий как инструмента для унификации терминологии, структурирования данных предметной области, а также интеграции знаний между системами и экспертами. Здесь же обоснована роль онтологий в повышении точности анализа, автоматизации управления безопасностью и принятия решений, что способствует снижению затрат и ограничивает влияние субъективных факторов.

В главе подчеркивается актуальность и необходимость разработки моделей и алгоритмического обеспечения СППР по повышению эффективности систем защиты информации (СЗИ) предприятий и дается развернутое определение понятию информационной системы (ИС) и ее компонентов, рассматриваются основные типы архитектур ИС, существующие методы управления их ресурсами. Проведен анализ современных исследований и описаны основные проблемы организации СЗИ такие как сложность и высокая стоимость внедрения.

Во второй главе разработана система онтологий, положенная в основу дальнейших действий. Представленная система формирует базу знаний предметной области, описывающую компоненты, входящие в ПТСЗИ и связи между ними. Отмечено, что онтологические модели играют ключевую роль в оценке эффективности функционирования СЗИ. Полученные в ней результаты

позволили структурировать процесс измерения функциональной эффективности на всех уровнях системы, а также минимизировать влияние субъективных факторов за счёт формализации межкомпонентных связей. Автором выделены девять ключевых подсистем ПТСЗИ, каждая из которых интегрируется в общую архитектуру защиты. Это подсистема контроля и управления доступом, подсистема регистрации и учёта, подсистема обеспечения целостности и другие. Выделены комплексы защиты такие как комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows, комплекс антивирусной защиты; комплекс резервного копирования и так далее. Всего пятнадцать комплексов. Отмечается, что предлагаемый подход позволяет оценивать их не по отдельности, а как взаимосвязанные компоненты, что обеспечивает всесторонний анализ и управление защитными мерами.

Подчёркивается, что полученные результаты могут быть адаптированы для предприятий в различных секторах экономики, когда требуется создать комплексную систему защиты информационных активов, провести минимизацию вероятностей киберугроз, а также сократить время реагирования на инциденты информационной безопасности.

В третьей главе разработана методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ, а также решены экстремальные задачи линейного программирования о повышении уровня защищённости ИС в условиях финансовых ограничений. В частности, представлена кубическая матрица защиты «Угрозы – Активы – Комплексы средств защиты информации» и связанные с нею двумерные матрицы. Матрицы легли в основу модели оценки функциональной эффективности системы, что, во-первых, сделало процесс оценки более объективным, во-вторых – позволило сформулировать экстремальные задачи повышения уровня защищённости информационных активов при финансовых ограничениях. Это способствовало автоматизации выработки рекомендаций по повышению эффективность защитных мер, обеспечивая их более рациональное распределение и управление в условиях ограниченных ресурсов.

Результаты третьей главы легли в основу разработанной и описанной в четвёртой главе СППР по повышению уровня эффективности ПТСЗИ при финансовых ограничениях. Соответствующий алгоритм, постановки и решения экстремальных задач описаны здесь же.

В четвертой главе автором приводятся сведения о разработанной СППР в виде программы «Агрегированное оценивание функциональной эффективности» (АОФЭ) и программы «Оптимальное распределение денежных средств» для повышения функциональной эффективности ПТСЗИ предприятия – «ОРДС». Обе программы внедрены в деятельность предприятия ООО «ЯНТА», что позволило не только оценить функциональную эффективность ПТСЗИ и её подсистем, но и определить долю угроз безопасности информации, которые покрываются комплексами

средств защиты информации в разрезе таких свойств, как конфиденциальность, целостность и доступность. Пользователями программ могут быть как специалисты, ориентированные на решение прикладных задач в области ИБ, так и руководство предприятия.

В главе в обобщённом виде представлены алгоритмы работы программ и приведены результаты их тестирования на базе ООО «Янта». Автором выполнено сравнение состояния ПТСЗИ предприятия до и после оптимизации. Для первой задачи показано, что эффективность системы защиты информации на предприятии возрастает с 0,63 до 0,98 при привлечении дополнительных денежных средств в размере 10 млн. руб. Решение второй задачи в свою очередь показало, что для обеспечения текущего для предприятия уровня функциональной эффективности 0,63, можно ограничится затратами всего 1,68 млн руб.

В заключении приводятся основные результаты работы.

Достоверность и обоснованность научных положений, выводов и рекомендаций работы подтверждается корректным использованием хорошо зарекомендовавших себя методов онтологического моделирования, линейного программирования, результатами опытной эксплуатации разработанного программного обеспечения. Основные результаты опубликованы в рецензируемых научных изданиях, апробированы на конференциях различного уровня, включая международный. Также получены два свидетельства на программу для ЭВМ.

Оценка научной новизны и практической значимости результатов. Признаками научной новизны диссертации имеют следующие результаты:

1. Онтологические модели применительно к программно-технической реализации СЗИ и модели определения исходных данных для вычисления показателей эффективности. Соответствует п. 5 паспорта специальности 2.3.1 «Системный анализ, управление и обработка информации, статистика».

2. Методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ, использующие трехмерную матрицу защиты, многомерный бинарный массив и модели эффективности, включая визуализацию результатов оценивания. Соответствует п. 11 паспорта специальности.

3. Две задачи линейного программирования (ЛП) об оптимальном распределении денежных средств на совершенствование ПТСЗИ, в первой из которых для заданного бюджетного ограничения максимизируется нижняя граница функциональной эффективности ПТСЗИ и всех её компонентов, а во второй минимизируются суммарные затраты для обеспечения заданного уровня функциональной эффективности ПТСЗИ и всех её компонентов. Соответствует п. 9 паспорта специальности.

Автор продемонстрировал глубокое знание предмета. Впервые разработаны онтологические модели такой сложной системы как ПТСЗИ; впервые предложена модель оценки эффективности на их основе, которая может использоваться и в других предметных областях; впервые решены

задачи о повышении эффективности ПТСЗИ при ограничениях на бюджет на основе разработанных моделей.

Практическую значимость ярче всего отражают результаты апробации СППР на конкретном предприятии: ООО «Янта» затратило на формирование СЗИ около 22 млн. рублей, применение же разработанной автором СППР и управленческие решения на этой основе позволили бы для достижения той же эффективности ограничиться 1,67 млн. руб.

Содержание работы и представленные результаты соответствуют пунктам 5, 9, 11 паспорта специальности 2.3.1 – «Системный анализ, управление и обработка информации, статистика».

Недостатки и замечания. К замечаниям по содержанию и оформлению диссертации можно отнести следующее:

1. В тексте диссертации на с.62 говорится «Важно отметить, что в данном исследовании предлагается анализировать возможность реализации угроз безопасности в отношении различных информационных активов предприятия. Это позволяет учесть особенности каждого актива и применить соответствующие меры защиты…». Вместе с тем, не совсем понятно, каким образом в моделях Задачи 1 и Задачи 2 учитываются особенности каждого актива. Например, если потенциальный ущерб от нарушения безопасности некоторого актива мал по сравнению с затратами, которые выделяются конкретно на его защиту, может и не стоит тогда его защищать?

2. Описание процессов формирования и использования онтологий носит ограниченный характер. В тексте диссертации не приводится информация о том, как создается и наполняется онтология, какими инструментами пользуется автор. Остается неясным, каким образом онтология проверяется на корректность и полноту.

3. Автор сделал акцент на практическую значимость разработанных методик, однако в работе не хватает полноценного анализа и рекомендаций по их внедрению. Как конкретно внедрить предложенные методики в практику предприятий, какие нужны дополнительные ресурсы и усилия.

4. В тексте диссертации имеются орфографические ошибки, а также ошибки, связанные с оформлением таблиц.

Заключение. Указанные замечания не снижают общей положительной оценки работы. Диссертация представляет собой завершенный научно-квалификационный труд на актуальную тему. Полученные результаты достоверны, имеют теоретическую и практическую значимость, причём не только в сфере защиты информации, но и для других организационно-технических, социально-экономических и иных подобных систем, управление которыми предполагает использование средств поддержки принятия управленческих решений.

Автореферат соответствует основному содержанию диссертации.

Оформление диссертации и автореферата отвечает требованиям ВАК России. В целом заключаю, что диссертационная работа по уровню и

значимости полученных результатов, стилю изложения, обоснованности выводов, широте и уровню апробации и опубликования соответствует требованиям п. 9 Положения «О порядке присуждении ученых степеней», утвержденного постановлением Правительства РФ от 24 сентября 2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени кандидата наук, а ее автор, Наседкин Павел Николаевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.1 – «Системный анализ, управление и обработка информации, статистика».

Официальный оппонент,
доктор технических наук
(05.13.10), доцент, профессор
кафедры вычислительной
математики и кибернетики
ФГБОУ ВО «Уфимский
университет науки и технологий» Ризванов Дмитрий Анварович

Адрес организации:
450076, Приволжский федеральный округ, Республика Башкортостан, г. Уфа, ул. Заки Валиди, дом 32

Тел.: +79174095406, e-mail: ridmi@mail.ru

Докторская диссертация защищена по специальности:
05.13.10 – Управление в социальных и экономических системах

Я, Ризванов Дмитрий Анварович, даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

«21» апреля 2025 г. _____ Д.А. Ризванов

Подпись Ризванова Д.А.
Удостоверяю «21» 04 2025 г.
Начальник общего отдела УУНиТ Ражеева Л.Р.