ОТЗЫВ

официального оппонента Ходашинского Ильи Александровича на диссертационную работу **Наседкина Павла Николаевича**
«Модели и алгоритмическое обеспечение поддержки принятия решений по повышению эффективности системы защиты информации предприятия»,
представленную на соискание ученой степени кандидата технических наук
2.3.1 – Системный анализ, управление и обработка информации, статистика (технические науки)

Актуальность темы

Одним из приоритетов государственной политики является обеспечение информационной безопасности критических объектов инфраструктуры, оборонных объектов, объектов кредитно-финансовой сферы. Данное направление государственной политики фиксируется такими ключевыми документами как 1) Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 05.12.2016 № 646); 2) Стратегия развития информационного общества в Российской Федерации на 2017-2030 г.; 3) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Информационные системы занимают важное место в задачах управления производством, технологическими, социально-экономическими и иными процессами. Вмешательство в работу этих систем способно серьёзно осложнить работу организаций, компаний, нанести вред их деятельности или государству. Противодействие такому вмешательству сегодня – одно из актуальнейших направлений информационных технологий. Борьба с незаконным, несанкционированным вмешательством в работу информационных систем основана на применении методов системного подхода. Специалисты выделяют три главных составляющих защиты: организационно-управленческий, программно-аппаратный (программно-технический) и инженерно-технический. Важны все три уровня, но центральное место принадлежит программно-аппаратной составляющей. Организация системы защиты информации – это большая работа, требующая немалых финансовых затрат. От того, как будут распределены средства во многом зависят результаты защиты. Это важно для наиболее затратной – программно-технической составляющей. Сложность заключается в том, что разные аппаратные средства могут выполнять схожие функции, решая одну и ту же задачу, а могут дополнять друг друга. Это не может не отразится на их рациональном сочетании, и практический опыт специалистов необходимо дополнять соответствующими системами поддержки принятия решений. При

этом перед разработкой подобных программных средств должна быть проанализирована структура системы защиты в целом, выделены её элементы, установлены взаимосвязи между ними, оценена эффективность системы в различных конфигурациях, что невозможно сделать без глубокого и последовательного системного анализа данного предмета.

Диссертационная работа Наседкина П.Н. посвящена проблеме совершенствования сложной технической системы – программно-технической системы защиты информации организации. Автором разработана и реализована методика её совершенствования, опирающаяся на онтологическое моделирование предметной области с последующей постановкой и решением задач повышения эффективности системы при наличии финансовых ограничений. На основе разработанной методики создана система поддержки принятия управленческих решений.

Анализ содержания диссертационной работы

Диссертация содержит введение, четыре главы, заключение, список литературы из 183 наименований. Общий объем – 171 страница, включая 37 рисунков, 10 таблиц, 2 приложения.

Во введении обоснована актуальность темы исследования, сформулированы ее цель и основные задачи, научная новизна, практическая значимость результатов исследования. **В первой главе** представлен обзор существующих методик, методов и подходов к управления информационной безопасностью, оценке эффективности систем защиты информации. Большое внимание уделено рискам как основной методологии управления безопасностью (информационной, промышленной, пожарной и иными). Автор отмечает значительную степень субъективизма оценок на основе риска в условиях недостаточной статистики и ставит задачу снижения степени субъективизма за счёт перехода к другим методикам. В работе предлагается методика совершенствования подобных систем на основе онтологического моделирования с последующим построением оценок эффективности на основе анализа структуры и взаимосвязей компонентов системы с учётом пересечения и взаимодополнения их функций. **Во второй главе** представлены онтологические модели программно-технической системы защиты информации (программно-аппаратной подсистемы комплексной системы защиты информации) – основа всей авторской методики. Строятся как метаонтологии, так и онтологии систем более низкого уровня, описывается роль и назначение подсистем и компонентов, их взаимосвязи и защитные функции, которые они несут. Моделирование проведено на уровне лёгких

онтологий. Этого вполне достаточно для поставленных целей. **Третья глава** посвящена описанию способа построения модели оценки общей эффективности программно-технической системы защиты информации на основе онтологических моделей и постановке оптимизационных задач по повышению её эффективности в условиях финансовых ограничений. Автором строится трёхмерная матрица защиты «Угрозы-Активы-Комплексы средств защиты информации» и связанные с ней матрицы: эталонные значения «Объекты защиты в контексте подсистем»; «Угрозы-Комплексы средств защиты информации»; «Активы (Объекты воздействия)-Комплексы средств защиты информации» и матрица оценок аудитора. Описаны принципы построения функции оценки эффективности с отсылкой к материалам ФСТЭК России и описанием роли и назначения отдельных подсистем и комплексов. Эффективность вычисляется как показатель заполненности матриц по функциям, угрозам и объектам защиты с учётом состояния функциональных компонентов с точки зрения аудиторов. Оценки аудиторов – единственный элемент субъективного характера в методике. В этой же главе приведены постановки и решение двух задач оптимизации размещения денежных средств, направляемых на развитие и совершенствование системы. **В четвертой главе** описано разработанное программное обеспечение – системы «Агрегированное оценивание функциональной эффективности» (АОФЭ) и «Оптимальное распределение денежных средств» (ОРДС). Приведены блок-схемы алгоритмов, примеры интерфейсов и результаты работы программы. Описаны особенности и порядок работы с программами. В **заключении** соискателем изложены основные полученные результаты диссертационного исследования.

Несомненным достоинством рассматриваемой диссертации является полный цикл исследования: анализ результатов других авторов, постановка задачи, разработка модели, реализация модели в программном комплексе, проверка работоспособности и эффективности предлагаемых решений с последующим внедрением. Это позволяет заключить, что исследование является обоснованным и завершенным.

Новизна полученных результатов, выводов и рекомендаций

Научная новизна диссертационной работы заключается в создании новых моделей и алгоритмов для решения задач разработки и оценки эффективности систем принятия решений, которые позволяют обеспечить их защиту и улучшить технико-экономические характеристики.

1. Впервые разработана онтологическая модель программно-технической системы защиты информации, позволяющая систематизировать и структурировать данные о компонентах системы.

2. Впервые на основе метода линейного программирования разработаны модели оптимизации распределении денежных средств, направляемых на совершенствование программно-технической системы защиты информации.

3. Разработана методика агрегированного оценивания программно-технической системы защиты информации; отличительной особенностью методики является использование в её составе трехмерной матрицы «Угрозы – Активы – Комплексы средств защиты информации», онтологической модели, модели оптимизации эффективности, средств визуализации результатов оценивания.

Степень обоснованности и достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации

Основные научные положения и выводы, представленные в диссертационной работе, в достаточной степени обоснованы и интерпретированы. Автор корректно использует научные методы обоснования полученных результатов, выводов и рекомендаций. Обоснованность и достоверность научных положений, выдвигаемых автором, подтверждается использованием хорошо зарекомендовавших себя методов онтологического моделирования, линейного программирования, результатами опытной эксплуатации разработанного программного обеспечения на предприятии. Выводы логически вытекают из материалов исследований и в полном объеме отражают поставленные задачи.

Практическая значимость результатов работы

Практическая значимость полученных соискателем результатов подтверждается использованием их в текущей деятельности ООО «Янта» для обеспечения защиты информации и отказоустойчивости информационных систем предприятия. Результаты диссертационной работы могут быть использованы для построения систем принятия решений, работающих в иных предметных областях: экология, военное дело, пожарная и промышленная безопасность, противодействие преступности и так далее. Работа важна именно как исследование по системному анализу, потому что сходными принципами организации противодействия различным угрозам могут обладать и другие защитные системы в других направлениях.

Полнота опубликования результатов работы, соответствие автореферата содержанию диссертации

По теме диссертации опубликованы 12 работ, в том числе: четыре – в журналах из списка ВАК; шесть публикаций в сборниках трудов международных и российских конференций; два свидетельства о государственной регистрации программ для ЭВМ. Материалы диссертации достаточно полно изложены в опубликованных работах.

Автореферат в полной мере отражает содержание и основные положения диссертации.

Замечания по диссертации и автореферату

1. Вызывает недоумение пересказ на десяти страницах (стр. 22–31) содержание работы [179] без должного критического анализа.

2. На стр. 35-36 упоминается метод Дельфи, и в качестве «сложностей» применения этого метода указываются а) «*большое количество участников*», б) «*высокая субъективность оценок*». Во-первых, никакие количественные ограничения в упомянутом методе не задаются. Во-вторых, метод Дельфи – это метод экспертного оценивания, значит субъектность в методе заложена по определению, а использование обратной связи в процессе опроса позволяет значительно повысить объективность оценок экспертов. В-третьих, в научной работе следует избегать цитирования различных вики-блогов, речь о ссылке на источник номер 96.

3. В созданной онтологической модели комплекс К1 включает в себя средства защиты серверов и АРМ только под управлением операционных систем семейства Windows. При этом на стр. 59 диссертации указывается, что «данная модель может быть адаптирована и применена в различных предметных областях исследований, а также в области принятия управленческих решений по вопросам информационной безопасности». В связи с повсеместным импортозамещением возникает вопрос, каким образом модель будет адаптирована, если сервера и/или АРМ управляются операционными системами семейства Linux.

4. Исходя из описания функции комплекса К14 в таблице 2.1, место этого комплекса в модели весьма проблематично. Функции К14 практически совпадают с функциями К1, за исключением обеспечения целостности исполняемых файлов системного ПО, которое к прикладному не относится (а К14 представлен для защиты прикладного ПО). Возникают вопросы, в чём принципиальное отличие К1 от К14 и как К14 будет адаптироваться при внедрении в организации иных предметных областей.

5. На стр. 96 и 97 диссертации указано, что формулы (3.9), (3.10) и (3.11) являются линейными ограничениями. На самом деле указанные формулы всего лишь раскрывают содержание целевой функции, ограничения заданы другими формулами ниже.

6. *Оформление и аббревиатуры*.

6.1. Аббревиатура АСО вводится на стр. 8 автореферата, а расшифровывается на стр. 10. В тексте диссертации эта же аббревиатура впервые встречается на стр. 65, а расшифровывается на стр. 66.

Аббревиатура СУИБ вводится на стр. 35, а расшифровывается на стр. 43.

Аббревиатура КСЗИ вводится на стр. 38, а расшифровывается на стр. 55.

Аббревиатуре (ИБ) повезло гораздо больше, она вводится и расшифровывается в тексте диссертации ровно десять раз.

6.2. В списке литературы дважды упомянут один и тот же источник под номерами [136] и [137].

6.3. В диссертации присутствуют грамматические ошибки.

В целом замечания не снижают научной ценности и практической значимости проведенного исследования.

Заключение

Диссертация и автореферат Наседкина Павла Николаевича по содержанию и представленным результатам соответствует паспорту специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика (технические науки).

Научные и практические результаты, полученные при проведении диссертационного исследования, и полнота их освещения в публикациях соискателя позволяют считать, что диссертация Наседкина Павла Николаевича является законченной научно-квалификационной работой, содержащей решение актуальной научной задачи развития методов агрегированного оценивания сложных технических систем и разработки систем поддержки принятия решений по их совершенствованию.

Диссертация отвечает пункту 9 «Положения о присуждении учёных степеней», 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 (технические науки).

Я, Ходашинский Илья Александрович, даю согласие на обработку персональных данных.
Официальный оппонент:

Профессор кафедры компьютерных систем в управлении и проектировании факультета вычислительных систем федерального государственного автономного образовательного учреждения высшего образования "Томский государственный университет систем управления и радиоэлектроники", доктор технических наук, профессор

25 марта 2025г. _____/ Ходашинский Илья Александрович /

Полное наименование организации: федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»
Адрес: 634045, г. Томск, ул. Вершинина, д. 74
Телефон: +7 (3822) 70-15-15
Эл. почта: hodashn@rambler.ru

Подпись Ходашинского
УДОСТОВЕРЯЮ
Ученый секретарь
Е.В. Прокопчук