УТВЕРЖДАЮ:
Директор Института автоматики и процессов управления ДВО РАН, д.ф.-м.н., профессор, член-корреспондент РАН
_____ Ромашко Р.В.
«__8__» апреля 2025 г.

ЗАКЛЮЧЕНИЕ

ведущей организации – Института автоматики и процессов управления ДВО РАН по диссертационной работе 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 научной проблемы. Переход к цифровой экономике вывели на передний план вопросы защиты информации – основы пятого и шестого технологического укладов. Как правило, все значимые бизнес-процессы в организациях сопровождаются компьютерной обработкой информации, несанкционированное вмешательство в которую способно серьёзно навредить организации. При этом сама обработка невозможна вне информационной инфраструктуры, основой которой является программно-техническая система – соответствующий комплекс технических и программных средств.

Любая информационная система включает совокупность программных, технических, документальных и иных средств, необходимых для её функционирования. Соответственно, защита информации – это также комплексная проблема, важнейшей составляющей которой выступают программно-технические средства. Эффективное функционирование программно-технической системы (точнее, подсистемы) комплексной системы защиты информации (КСЗИ) предприятия – необходимое условие успешности КСЗИ в целом. В связи с этим, тема диссертационной работы П.Н. Наседкина безусловно актуальна.

Второй составляющей её актуальности является прикладное назначение исследования – разработка системы поддержки принятия решений по совершенствованию программно-технической системы защиты информации (ПТСЗИ). Ввиду сложности и комплексности проблемы, интуитивные решения здесь могут оказаться недостаточно эффективными и излишне затратными для организации. Решения, которые предлагаются в диссертации, позволяют снизить издержки и/или повысить общую результативность затрат на данные цели.

Наконец, важно и то, что диссертант попытался предложить свой, достаточно нетрадиционный путь решения проблемы, основанный на анализе трёхмерной матрицы «Угрозы – Активы – Комплексы средств защиты информации». Сегодня наиболее распространённые подходы к таким исследованиям опираются на понятие риска, определение которого, как отмечается в диссертации, является самостоятельной и непростой проблемой: из-за дефицита статистики риски часто оказываются субъективными. В результате, актуален поиск новых методов и приёмов в этой области.

Научная новизна исследований и полученных результатов заключается в следующем

1. Выполнено онтологическое моделирование КСЗИ предприятия применительно к её программно-технической реализации, что позволяет формировать исходные данные для вычисления показателей эффективности ПТСЗИ.

2. На основе п. 1 предложены методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ, использующие трехмерную матрицу защиты «Угрозы-Активы-Комплексы средств защиты информации», многомерный бинарный массив и модели эффективности системы, включая визуализацию результатов оценивания.

3. Решены вытекающие из пп. 1 и 2 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.

Значимость результатов диссертации для науки и производства. Результаты диссертационной работы представляют научный интерес и имеют практическую значимость для управления информационной безопасностью производственных предприятий и организаций.

Значимость для науки обусловлена оригинальностью и системностью авторского подхода к проблеме защиты информации, включающего шаги:

1. Выделения ПТСЗИ как ядра КСЗИ.
2. Онтологическое моделирование ПТСЗИ.
3. Разработка на основе онтологий метода агрегированного оценивания функциональной эффективности ПТСЗИ, использующего трёхмерную матрицу защиты «Угрозы-Активы-Комплексы средств защиты информации».
4. Постановка и решение на основе этого метода задач линейного программирования: задачи о повышении эффективности ПТСЗИ при заданных бюджетных ограничениях и задачи о минимизации суммарных затрат при заданном уровне эффективности ПТСЗИ.

Это заметно отличает результаты исследования от традиционных методов, опирающихся на понятие риска.

С прикладной стороны разработанная методика доведена до программно-алгоритмической реализации в виде двух программ: программы «Агрегированное оценивание функциональной эффективности» (АОФЭ) и программы «Оптимальное распределение денежных средств» (ОРДС) для принятия решений по повышению функциональной эффективности СЗИ предприятия в контексте функционирования её программно-технических компонентов. На обе программы автором получены соответствующие свидетельства.

Автором получен акт о внедрении результатов диссертации в деятельность предприятия ООО «ЯНТА». Опытная эксплуатация программных продуктов подтверждают обоснованность представленных в исследовании результатов и работоспособность предложенного подхода.

В целом, результаты диссертационного исследования Наседкина П.Н. имеют научную и прикладную значимость и могут найти применения в практической деятельности подразделений ИБ на предприятиях и в организациях различного типа и направленности, эксплуатирующих информационно-вычислительные системы.

Результаты диссертации могут также найти применение в учебном процессе, особенно при подготовке студентов и аспирантов в рамках укрупненной группы специальностей 10.00.00 «Информационная безопасность».

Степень обоснованности и достоверности научных положений, выводов и рекомендаций диссертации определяется корректным использованием онтологического моделирования, методов линейного программирования, а также результатами опытной эксплуатации разработанного программного обеспечения.

Результаты прошли хорошую апробацию в научной среде: докладывались на международных и всероссийских конференциях. Основные результаты опубликованы в 12 научных изданиях, включая издания из списка ВАК.

Структура диссертационной работы. Диссертация объемом 171 стр., состоит из введения, четырёх глав, заключения, списка сокращений, списка использованных источников и двух приложений. Основная часть работы изложена на 167 страницах машинописного текста, содержит 10 таблиц и 37 рисунков.

Во введении диссертации обоснована актуальность темы исследования, определена его цель, сформулированы задачи исследования и приводится общая характеристика диссертационной работы.

В первой главе работы выполнен анализ предметной области, касающейся оценки эффективности функционирования СЗИ предприятия. Анализ показал, что существующие методики имеют особенность – они ориентированы на оценку рисков с использованием экспертных методов, которые характеризуются известным субъективизмом при недостатке статистических данных. Для

корректного использования показателей ИБ в контексте повышения эффективности СЗИ автором предложено использовать онтологическое моделирование как инструмент для унификации терминологии, структурирования данных предметной области, а также интеграции знаний между системами и экспертами. В главе обоснована роль онтологий в повышении точности анализа, автоматизации управления безопасностью и принятия решений, что способствует снижению влияния субъективных факторов.

Во второй главе разработана система онтологий, которая положена в основу вычислительного алгоритма для оценки функциональной эффективности ПТСЗИ на предприятиях с различным уровнем зрелости в области ИБ. Предложенная система описывает компоненты, входящие в ПТСЗИ и связи между ними. Автор подчеркивает, что полученные в данной главе онтологические модели играют ключевую роль в процессе агрегированного оценивания эффективности функционирования КСЗИ. Определённые в рамках моделей концепты и их взаимосвязи служат основой для выбора показателей оценивания. Это позволило структурировать процесс измерения функциональной эффективности на всех уровнях системы, а также минимизировать влияние субъективных факторов за счёт формализации межкомпонентных связей. В рамках анализа выделены и описаны девять ключевых подсистем, каждая из которых интегрируется в общую архитектуру защиты. Онтологические модели ПТСЗИ получены впервые.

В третьей главе разработана методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ. Созданная на предыдущем этапе онтологическая модель обеспечила систематизацию объектов защиты, угроз и функций подсистем, что позволило построить кубическую матрицу «Угрозы – Активы – Комплексы средств защиты информации» и связанных с нею двумерные матрицы. Это сделало процесс оценки более объективным. В рамках данного подхода предложена модель повышения ИБ предприятия, охватывающая ПТСЗИ, и сформулированы две задачи ЛП об оптимальном распределении денежных средств. Здесь же представлен алгоритм агрегированного оценивания ПТСЗИ.

В четвёртой главе описаны созданные автором программные системы: программа «Агрегированное оценивание функциональной эффективности» (АОФЭ) и программа «Оптимальное распределение денежных средств» для повышения функциональной эффективности ПТСЗИ предприятия – «ОРДС». Здесь же представлены результаты опытной эксплуатации разработанного программного обеспечения на ООО «ЯНТА».

В заключении приводятся основные результаты работы.

Список литературы содержит 183 наименования.

Приложения включают свидетельство об использовании результатов работы в деятельности ООО «Янта» и свидетельства о регистрации программ для ЭВМ.

Рекомендации по использованию результатов и выводов диссертационной работы. Теоретические и экспериментальные результаты диссертации расширяют представление о возможностях использования интеллектуальных и вычислительных технологий в анализе КСЗИ, управлении информационной безопасностью с целью повышения её эффективности. Созданное программное обеспечение может найти применение в деятельности служб ИБ предприятий и организаций различного типа, в исследованиях научных коллективов, занимающихся данными вопросами, а также в учебных заведениях, осуществляющих подготовку в этой сфере. Подход достаточно общий и представляет интерес в том числе для анализа других сложных технических и социально-технических систем.

Основные результаты рекомендуется, в частности, передать для внедрения на следующих предприятиях:

– Восточно-Сибирская железная дорога – филиал ОАО «РЖД»;

– Забайкальская железная дорога – филиал ОАО РЖД;

– ФГБОУ ВО «Иркутский государственный университет путей сообщения».

Замечания по диссертации:

1. Недостаточно информации о ситуации на рынке с программно-техническими комплексами средств защиты информации. Нет сравнения выбранных методов с их аналогами.

2. Недостаточно полно используются возможности онтологического моделирования. В работе данный подход использовался только на этапе проведения системного анализа, а как программно-информационный компонент создаваемых программных систем, обеспечивающий их гибкую настройку и сопровождение, онтологии не используются.

3. Недостаточно освещены вклад работы в области теории обеспечения информационной безопасности и новизна подхода.

4. Не показаны план мероприятий или методика применения разработанного комплекса средств потребителями на практике в своих организациях.

В целом диссертационная работа производит впечатление завершённого научно-квалификационного исследования в области анализа и повышения эффективности систем защиты информации, в котором представлена совокупность научных положений и практических результатов, дающих существенный вклад в проблему управления информационной безопасностью на предприятиях и в организациях различной направленности. Решение данной проблемы имеет существенное значение для развития страны. В ходе работы автор Наседкин П.Н. продемонстрировал владение методологией системного анализа в одном из его прикладных аспектов.

На основании всего вышесказанного можно заключить, что по своей актуальности, научной и практической значимости диссертационная работа «Модели и алгоритмическое обеспечение поддержки принятия решений по

повышению эффективности системы защиты информации предприятия» отвечает требованиям пункта 9 абзац 2 «Положения о порядке присуждения ученых степеней», а соискатель Наседкин Павел Николаевич, достоен присуждения ученой степени кандидата технических наук по специальности 2.3.1 «Системный анализ, управление и обработка информации, статистика».

Отзыв обсужден и принят на заседании научного семинара лаборатории Интеллектуальных систем имени А.С. Клещева (№35) Института автоматики и процессов управления Дальневосточного отделения (протокол №318 от «8» апреля 2025 года).

Председатель научного семинара,
директор Института автоматики и процессов
управления ДВО РАН,
член-корреспондент РАН Р.В. Ромашко

Секретарь научного семинара
лаборатории интеллектуальных систем
имени А.С. Клещева (№35)
доктор технических наук Е.А. Шалфеева

690041, г. Владивосток, ул. Радио, 5
Тел.: +7(423)2310439
Официальный сайт в сети интернет: https://www.iacp.dvo.ru/

08.04.2025 г.