на правах рукописи

Наседкин Павел Николаевич

МОДЕЛИ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Специальность 2.3.1 – Системный анализ, управление и обработка информации, статистика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Иркутск – 2025

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Иркутский государственный университет путей сообщения»

Научный руководитель: **Аршинский Леонид Вадимович**, доктор технических наук, доцент, профессор кафедры «Информационные системы и защита информации» ФГБОУ ВО «Иркутский государственный университет путей сообщения», г. Иркутск

Официальные оппоненты: **Ходашинский Илья Александрович**, доктор технических наук, профессор, профессор кафедры компьютерных систем в управлении и проектировании ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники», г. Томск

Ризванов Дмитрий Анварович, доктор технических наук, доцент, профессор кафедры вычислительной математики и кибернетики ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа

Ведущая организация: ФГБУН «Институт автоматики и процессов управления ДВО РАН», г. Владивосток

Защита состоится 15 мая 2025 г. в 14:00 часов на заседании диссертационного совета 44.2.002.01, созданного на базе ФГБОУ ВО «Иркутский государственный университет путей сообщения» по адресу 664074, г. Иркутск, ул. Чернышевского, дом 15, аудитория А-803, тел.8(3952)63-83-94, e-mail: diss_sovet@irgups.ru.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Иркутский государственный университет путей сообщения» и на сайте https://www.irgups.ru.

Отзыв на автореферат в двух экземплярах, заверенный печатью учреждения, просим направлять по адресу: 664074, г. Иркутск, ул. Чернышевского, дом 15, аудитория А-803, ученому секретарю диссертационного совета 44.2.002.01.

Автореферат разослан «___» _____20____г.

Ученый секретарь
диссертационного совета
доктор технических наук, профессор А.В. Лукьянов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. С развитием информационных технологий и внедрением их в деятельность предприятий растёт необходимость совершенствования способов защиты предприятия от различных видов киберугроз, которые становятся все более сложными и разнообразными. С одной стороны происходит увеличение объема и значимости хранимой, передаваемой и обрабатываемой информации, что требует развития и совершенствования средств её защиты, с другой – предприятия функционируют в условиях ограниченных финансовых ресурсов, что усложняет проблему.

Изучение литературы показывает, что большинство исследований в области оценки и управления эффективностью систем защиты информации (СЗИ) посвящены вопросам оценки и управлению рисками информационной безопасности (ИБ). В то же время риск оценивается с использованием экспертных методов, которые характеризуются известным субъективизмом при недостатке статистических данных, когда вероятностный фактор риска рассчитывается исходя из следующего: вероятности реализации угрозы, вероятности использования уязвимости, размера ущерба.

Несмотря на общую результативность научных исследований и выработку стандартов в области управления ИБ, вопросы формализации оценок и измерения различных показателей безопасности всё ещё остаются недостаточно изученной областью знаний. В диссертационном исследовании рассматривается подход, основанный на онтологиях – специальной форме знаниевого моделирования предметной области, позволяющей отразить существующие в ней взаимосвязи. Исследования в области формализации знаний, касающиеся ключевых показателей ИБ, влияющие на свойства эффективности СЗИ описаны как в трудах российских учёных Г.Б. Петухова, Б.Е. Поклонова, Б.В.Черникова, В.И. Якунина и др., так и зарубежных авторов Г. Ковачича, К. Кормоса, Т. Кохонена, К. Пэйна, Ч. Робинсона, В. Рэйфорда, М. Свансона, М. Сэйко и др.

Вопросы онтологического моделирования и применения знаниевых моделей для поддержки принятия управленческих решений отражены как в трудах зарубежных авторов А. Гомес-Перес, Т.Р. Грубера, О. Корчо, М. Фернандеса-Лопеса и др., так и российских учёных И. Бубакара, М.Б. Будько, Т.А. Гавриловой, В.В. Грибовой, Ю.А. Загорулько, Л.В. Массель., С.В. Смирнова и др.

В контексте повышения эффективности функционирования СЗИ, применение онтологий позволяет достаточно точно определить компоненты и взаимосвязи предметной области и выполняемые ими функции, рассчитать агрегированные показатели соответствия СЗИ заявленным целям. Притом, что в прикладном плане необходимо не просто повысить эффективность СЗИ, а выполнить это с учётом возможных финансовых ограничений. Владельцы информационных активов должны решить задачу каким образом обеспечить максимальную функциональную эффективность СЗИ при ограничении на затраты, либо каким образом минимизировать затраты при ограничении на эффективность СЗИ (под функциональной эффективностью здесь и далее понимаем соответствие системы целям своего функционирования; под оценкой функциональной эффективности

– количественную меру такого соответствия).

Все вышеперечисленное обосновывает необходимость использования системного подхода при создании моделей и разработке алгоритмического обеспечения для повышения эффективности СЗИ. Это же определяет актуальность выбранной темы диссертационного исследования, позволяет определить его цель и задачи.

Целью диссертационной работы является повышение функциональной эффективности СЗИ предприятия на уровне программно-технических компонентов за счет разработки и применения моделей и алгоритмического обеспечения поддержки принятия решений с учётом возможных финансовых ограничений.

Для реализации поставленной цели необходимо решить следующие **задачи**:

1. Выполнить системный анализ предметной области, включая методики, методы и подходы, применяемые для оценки эффективности состояния информационной безопасности предприятия.

2. Используя методы системного анализа и онтологического моделирования, определить основные компоненты (объекты защиты, угрозы, комплексы средств защиты, подсистемы и функции подсистем) программно-технической СЗИ (ПТСЗИ) и их взаимосвязи.

3. Разработать алгоритмическое обеспечение агрегированного оценивания эффективности функционирования ПТСЗИ предприятия.

4. Разработать и программно реализовать задачу оптимизации распределения денежных средств, направляемых на повышение эффективности СЗИ предприятия в контексте функционирования программно-технических компонентов.

5. Разработать программу для реализации процедуры агрегированного оценивания и визуализации результатов оценивания.

Объектом исследования является ПТСЗИ предприятия в процессе его функционирования.

Предметом исследования является алгоритмическое обеспечение и программы, поддерживающие принятие управленческих решений для повышения эффективности СЗИ предприятия в контексте функционирования её программно-технических компонентов с учетом возможных финансовых затрат.

Методы исследования: для решения поставленных задач применены методы системного анализа и семантического моделирования, линейного программирования (симплекс-метод), а также методы для решения базовых задач визуальной аналитики.

Научную новизну диссертации представляют следующие положения, **выносимые на защиту**:

1. Онтологические модели применительно к программно-технической реализации СЗИ и модели определения исходных данных для вычисления показателей эффективности.

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

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.

Достоверность результатов, выносимых на защиту, подтверждается использованием хорошо зарекомендовавших себя методов онтологического моделирования, линейного программирования, результатами опытной эксплуатации разработанного программного обеспечения.

Соответствие диссертации паспорту научной специальности. Содержание диссертационной работы соответствует паспорту научной специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика: п.5. Разработка специального математического и алгоритмического обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта; п.9. Разработка проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; п.11. Методы и алгоритмы прогнозирования и оценки эффективности, качества, надежности функционирования сложных систем управления и их элементов.

Теоретическая значимость исследования определяется разработкой методики поддержки принятия решений по повышению эффективности СЗИ в контексте функционирования её программно-технических компонентов на основе: 1) созданных онтологических моделей для определения исходных данных с целью вычисления показателей функциональной эффективности ПТСЗИ предприятия; 2) методики и алгоритмического обеспечения агрегированного оценивания ПТСЗИ, использующих трехмерную матрицу защиты, многомерный бинарный массив и модели эффективности, включая визуализацию результатов оценивания с использованием 6 уровневой цветовой шкалы; 3) постановки и решения задач ЛП применительно к ПТСЗИ, позволяющих повысить эффективность принятия управленческих решений.

Практическая значимость результатов состоит в том, что 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. Созданные программы апробированы на различных исходных данных, характеризующих состояние СЗИ предприятия в контексте функционирования её программно-технических компонентов. По-

лучен акт о внедрении результатов диссертационной работы в деятельность предприятия ООО «ЯНТА».

Апробация материалов исследования. Основные результаты диссертационного исследования докладывались и обсуждались на следующих научных конференциях: межвузовской научно-практической конференции молодых ученых «Информационные технологии. Актуальные проблемы защиты информации» (г. Иркутск, 2019); межвузовской научно-теоретической конференции в рамках Сибирского форума «Информационная безопасность – 2021» (г. Новосибирск, 2021); VI-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Наука и молодежь» (г. Иркутск, 2020); VII-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных «Наука и молодежь» (г. Иркутск, 2021); VIII-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Наука и молодежь» (г. Иркутск, 2022); III-ей Всероссийской научно-практической конференции «Информационные Технологии, их приложения и информационное образование» (ИТПИО`22) (г. Гусиноозёрск, 2022); XI-ой Международной научно-практической конференции «Транспортная ин-фраструктура Сибирского региона» (г. Иркутск, 2020); XII-ой Международной научно-практической конференции «Транспортная инфраструктура Сибирского региона» (г. Иркутск, 2021); I-ой Всероссийской конференции с международным участием «Информационные технологии, их приложения и информационное образование» (ИТПИО'2020) (г. Иркутск, 2020); XXVII-ой Байкальской Всероссийской конференции с международным участием «Информационные и математические технологии в науке и управлении» (г. Иркутск, 2022).

Публикации. По теме диссертационного исследования опубликовано 12 научных работ. Из них 3 статьи в рецензируемых научных журналах из перечня ВАК по рассматриваемой научной специальности, а также: 1 статья в журнале, вошедшем в перечень ВАК в 2022 году, 2 свидетельства о государственной регистрации программ для ЭВМ и 6 статей в других изданиях.

Личный вклад автора. Постановка задачи выполнена совместно с руководителем. Результаты, составляющие новизну и выносимые на защиту, получены лично, либо в неделимом соавторстве. Конфликт интересов с соавторами отсутствует.

Объем и структура работы. 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выполняемой 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 выполнен системный анализ предметной области, касающейся оценки эффективности функционирования СЗИ от различных угроз. Исследование включает изучение методов, методик, стандартов и моделей, применяемых для оценки информационных рисков и управления информационной безопасностью (ИБ) на предприятии. Анализ показал, что существующие методики имеют особенность – они ориентированы на оценку рисков с использованием экспертных методов, которые характеризуются известным субъективизмом при недостатке статистических данных. Более того, отсутствует системообразующая модель, способная дать ответ на вопрос, как снизить влияние субъективных факторов на оценку эффективности СЗИ. В ходе анализа были выявлены важные показатели ИБ, применяемые к оценке рисков, зрелости, бенчмаркингу (контрольных точек и эталонов), процессов мониторинга производительности, обеспечению целостного управления кибербезопасностью. Для корректного использования показателей ИБ в контексте повышения эффективности СЗИ и непрерывной ее работы рассмотрен системный подход с использованием онтологического моделирования. Анализ современных подходов к онтологическому моделированию СЗИ показал значимость онтологий как инструмента для унификации терминологии, структурирования данных предметной области, а также интеграции знаний между системами и экспертами. В главе также обоснована роль онтологий в повышении точности анализа, автоматизации управления безопасностью и принятия решений, что способствует снижению затрат и влияния субъективных факторов.

В рамках данной главы закладывается основа для разработки системного подхода к оценке и совершенствованию СЗИ, подчеркивается актуальность и необходимость разработки моделей и алгоритмического обеспечения поддержки принятия решений по повышению эффективности СЗИ предприятия, что подтверждает сформулированные во введении цель и задачи диссертационного исследования.

Во второй главе, с учётом проведённого системного анализа, 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 формирует базу знаний предметной области, описывающую компоненты, входящие в ПТСЗИ и связи между ними. Онтологические модели играют ключевую роль в процессе агрегированного оценивания эффективности функционирования СЗИ. Определённые в рамках моделей концепты (например, подсистемы защиты, функции контроля доступа, антивирусной защиты и др.) и их взаимосвязи служат основой для выбора показателей оценки. Это позволяет структурировать процесс измерения функциональной эффективности на всех уровнях системы, а также минимизировать влияние субъективных факторов за счёт формализации межкомпонентных связей. В рамках анализа выделены девять ключевых подсистем, каждая из которых интегрируется в общую архитектуру защиты (рис. 1).

Для построения системы онтологий ПТСЗИ использовались методы онтологического моделирования, что позволило детализировать функции, выполняемые на уровне

каждой подсистемы. Это дало возможность структурировать комплексы средств защиты информации (СрЗИ) в рамках ПТСЗИ, такие как: К1 (комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows); К2 (комплекс антивирусной защиты); К3 (комплекс резервного копирования); К4 (комплекс защиты среды виртуализации); К5 (комплекс сбора, анализа и корреляции событий ИБ); К6 (комплекс встроенных средств АСО); К7 (комплекс резервного копирования конфигурационных файлов АСО); К8 (комплекс межсетевого экранирования); К9 (комплекс обнаружения вторжений); К10 (комплекс встроенных средств защиты систем хранения данных); К11 (комплекс централизованного управления СрЗИ); К12 (комплекс анализа защищенности); К13 (комплекс контроля целостности); К14 (комплекс встроенных средств защиты прикладного программного обеспечения (ППО)); К15 (комплекс контроля использования информационных ресурсов).

Рис. 1. Состав системы онтологий ПТСЗИ

Комплексы СрЗИ К1 … К15, несмотря на их внутреннюю сложность, рассматриваются в данном исследовании как функциональные элементы системы. Системный подход позволяет оценивать их не по отдельности, а как взаимосвязанные компоненты, что обеспечивает всесторонний анализ и управление защитными мерами. Разработанные онтологические модели ПТСЗИ не только формализуют знания о компонентах системы, но и служат методологической основой для разработки методики и алгоритмического обеспечения агрегированного оценивания её функциональной эффективности. Модели позволяют выделить ключевые показатели функциональной эффективности, структурировать их по уровням и обеспечить логическую взаимосвязь между компонентами системы. Это повышает объективность результатов и точность оценки.

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. Созданная во второй главе 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. Методика предусматривает использование системного подхода для оценки влияния киберугроз на конфиденциальность, целостность и доступность информации, учитывая особенности защищаемых объектов и функций ПТСЗИ. Такой подход позволяет детально анализировать и повышать эффективность защитных мер, обеспечивая их более рациональное распределение и управление в условиях ограниченных ресурсов.

Методика агрегированного оценивания ПТСЗИ реализована через следующий алгоритм:

Шаг 1. Используя данные с сайта ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx) формируется список объектов воздействия (защиты) в привязке к угрозам ИБ, содержащий n_0 элементов. Среди них базы данных, прикладное программное обеспечение, каналы связи, мобильные устройства и т.д.;

Шаг 2. В процессе формирования векторов и множеств использованы результаты онтологического моделирования из главы 2. Определённые в онтологической модели подсистемы, их функции и взаимосвязи между компонентами ПТСЗИ составляют основу структурирования данных, что обеспечивает единообразие при заполнении массивов. Например, концепты подсистем и их функций, описанные в онтологиях, стали основой для разбиения данных на множества, представленные в таблице 1. На основании онтологических моделей и компонентов ПТСЗИ, которые представлены во второй главе диссертационного исследования, формируются (см. табл. 1): 1) вектор V, состоящий из элементов v_i, каждый из которых показывает какое количество функций входит в *i*-ю подсистему; он имеет вид $V=(3,2,2,2,2,2,2,3,1)$; 2) множества M_i^j, содержащие номера комплексов, входящих в *j*-ю функцию *i*-й подсистемы.

Таблица 1. Комплексы СрЗИ в разрезе подсистем и выполняемых ими функций

Подсистемы	Функции подсистем	Множество M_i^j	Комплексы
Подсистема контроля и управления доступом (П1)	Контроль и управление доступом к защищаемым информационным ресурсам (А1)	M_1^1	К1, К4, К8, К10, К14, К15
	Контроль и управление доступом к внешним носителям информации и периферийным устройствам (А2)	M_1^2	К1, К15
	Контроль доступа к активному сетевому обору-	M_1^3	К6, К8

Подсистемы	Функции подсистем	Множество M_i^j	Комплексы
	дованию (АСО) (А3)		
Подсистема регистрации и учета (П2)	Регистрация и учет действий пользователей и процессов (Б1)	M_2^1	К1, К2, К4, К5, К6, К8, К9, К10, К12, К13, К14, К15
	Регистрация событий доступа к внешним устройствам и портам ввода-вывода (Б2)	M_2^2	К1, К15
Подсистема обеспечения целостности (П3)	Контроль целостности исполняемых и конфигурационных файлов СрЗИ, компонентов ОС и прикладного ПО (В1)	M_3^1	К1, К12, К13
	Контроль неизменности параметров встроенных СрЗИ и компонентов системного ПО (В2)	M_3^2	
Подсистема антивирусной защиты (П4)	Защита файловой системы от вирусов и вредоносных программ (Г1)	M_4^1	К2
	Потоковая защита межсетевого трафика от вирусов и вредоносных программ (Г2)	M_4^2	К8
Подсистема контроля использования информационных ресурсов (П5)	Контроль каналов утечек защищаемой информации (Д1)	M_5^1	К1, К15
	Обнаружение несанкционированного хранения конфиденциальной информации (Д2)	M_5^2	К15
Подсистема централизованного управления СрЗИ (П6)	Обеспечение возможности оперативного получения информации о состоянии защищенности (Е1)	M_6^1	К11
	Обеспечение автоматизации рутинных задач (Е2)	M_6^2	
Подсистема анализа защищенности (П7)	Предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению (Ж1)	M_7^1	К12
	Обеспечение инвентаризации узлов, выявление и идентификация уязвимостей (Ж2)	M_7^2	
Подсистема обеспечения сетевой безопасности (П8)	Межсетевое экранирование ЛВС (З1)	M_8^1	К8
	Обнаружение вторжений в ЛВС (З2)	M_8^2	К9
	Обеспечение безопасного функционирования сетевого оборудования (З3)	M_8^3	К6, К7, К8, К9
Подсистема обеспечения непрерывности функционирования (П9)	Резервное копирование конфигурационных файлов СрЗИ и восстановление данных из резервных копий в случаях сбоев (И1)	M_9^1	К3, К7

Шаг 3. Для связи объектов воздействия с подсистемами, функциями и комплексами конкретного предприятия нужно заполнить бинарный четырехмерный массив D, состоящий из элементов δ_{ijkp}, $i=\overline{1,9}$, $j=\overline{1,v_i}$, $k \in M_i^j$, $p=\overline{1,n_0}$, заданными по правилу

$$\delta_{ijkp} = \begin{cases} 1, \text{ если для } j\text{-й функции } i\text{-й подсистемы} \\ \quad k\text{-й комплекс связан с } p\text{-м объектом воздействия;} \\ 0, \text{ в противном случае.} \end{cases}$$

Шаг 4. С использованием бинарного массива D и на основе разработанных онтологий вычисляются:

1) доля N^1_{ijk} связей для каждого комплекса одного типа, реализующего j-ю функцию i-й подсистемы с выбранными для оценки объектами защиты, к общему числу связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты по формуле:

$$N^1_{ijk} = \begin{cases} \dfrac{\sum\limits_{p=1}^{n_o} \delta_{ijkp}}{\sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{ijsp}}, \text{ если } \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{ijsp} \neq 0, \\ 0, \text{ если } \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{ijsp} = 0, \end{cases} \quad i = \overline{1,9},\ j = \overline{1,v_i},\ k \in M_i^j; \qquad (1)$$

2) доля N^2_{ij} общего числа связей всех комплексов разного типа для каждой j-ой функции, входящей в i-ю подсистему с выбранными для оценки объектами защиты к общему числу связей всех комплексов разного типа i-й подсистемы по выбранным объектам защиты по формуле:

$$N^2_{ij} = \begin{cases} \dfrac{\sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{ijsp}}{\sum\limits_{t=1}^{v_i} \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{itsp}}, \text{ если } \sum\limits_{t=1}^{v_i} \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{itsp} \neq 0, \\ 0, \text{ если } \sum\limits_{t=1}^{v_i} \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{itsp} = 0, \end{cases} \quad i = \overline{1,9},\ j = \overline{1,v_i}; \qquad (2)$$

3) доля N^3_i общего числа связей всех комплексов разного типа i-ой подсистемы с выбранными объектами защиты к общему числу связей всех комплексов разного типа всех подсистем уровня ПТСЗИ по выбранным объектам защиты по формуле:

$$N^3_i = \begin{cases} \dfrac{\sum\limits_{t=1}^{v_i} \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{itsp}}{\sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp}}, \text{ если } \sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp} \neq 0, \\ 0, \text{ если } \sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp} = 0, \end{cases} \quad i = \overline{1,9}. \qquad (3)$$

Шаг 5. Вычисляется эффективность каждого уровня j-ой функции i-й подсистемы по формулам

$$Э_{ij} = \sum_{k \in M_i^j} N_{ijk}^1 \cdot d_{ijk}\ ,\quad i = \overline{1,9},\ j = \overline{1,v_i}\ , \tag{4}$$

где d_{ijk} – оценки аудиторов по шкале от 0 до 1. Оценка «1» означает, что k – й комплекс полностью задействован в обеспечении j-ой функции i-й подсистемы, и удовлетворяет требованиям регуляторов по ИБ. Оценка «0» означает, что k – й комплекс либо не участвует в обеспечении j-ой функции i-й подсистемы, либо не удовлетворяет требованиям регуляторов по ИБ. Промежуточные значения отражают частичную функциональность комплекса. При этом на оценку аудиторов могут влиять такие факторы как: уровень компетенции экспертов в области ИБ и результаты вычислений уязвимостей по интерактивному калькулятору, размещенному на сайте ФСТЭК (https://bdu.fstec.ru/calc31).

Затем определяется функциональная эффективность каждого уровня подсистемы по формуле

$$Э_i = \sum_{j=1}^{v_i} N_{ij}^2 \cdot Э_{ij}\ ,\quad i = \overline{1,9}. \tag{5}$$

и вычисляется оценка функциональной эффективности ПТСЗИ по формуле

$$Э = \sum_{i=1}^{9} N_i^3 \cdot Э_i\ . \tag{6}$$

Оценка функциональной эффективности ПТСЗИ принимает значения от 0 до 1, где 1 означает, что все компоненты ПТСЗИ задействованы в полном объёме в реализации процессов обеспечения защиты информации и эксплуатации технологий безопасности информации, а «0» или любое число меньшее единицы – что ПТСЗИ, соответственно, полностью или частично не функционирует, либо не соответствует требованиям регуляторов по ИБ.

Модель информационной безопасности предприятия формализована в виде следующих двух задач ЛП.

Задача 1 (о максимизации нижней границы функциональной эффективности ПТСЗИ и всех её компонентов для заданного бюджетного ограничения W).

$$\min\left\{Э_{ij}^*, Э_k^*, Э^*\right\} \to \max\,, \tag{7}$$

где $i = \overline{1,9}$, $j = \overline{1,v_i}$, $k = \overline{1,9}$

и с линейными ограничениями

$$Э_{ij}^* = \sum_{k \in M_i^j} N_{ijk}^1 \cdot d_{ijk}^*\,,\qquad i = \overline{1,9},\ j = \overline{1,v_i}\,, \tag{8}$$

$$Э_i^* = \sum_{j=1}^{v_i} N_{ij}^2 \cdot Э_{ij}^*\,,\qquad i = \overline{1,9}\,. \tag{9}$$

$$Э^* = \sum_{i=1}^{9} N_i^3 \cdot Э_i^* . \qquad (10)$$

$$c_{ijk} = \frac{-c_{ijk}^{дост} \cdot d_{ijk}}{1-d_{ijk}} + \frac{c_{ijk}^{дост}}{1-d_{ijk}} \cdot d_{ijk}^*, \quad i=\overline{1,9},\ j=\overline{1,v_i},\ k \in M_i^j, \qquad (11)$$

$$d_{ijk} \le d_{ijk}^* \le 1, \qquad i=\overline{1,9},\ j=\overline{1,v_i},\ k \in M_i^j, \qquad (12)$$

$$\sum_{i=1}^{9} \sum_{j=1}^{v_i} \sum_{k \in M_i^j} c_{ijk} \le W, \qquad (13)$$

$$d_{ijk}^* \ge 0,\ c_{ijk} \ge 0,\ i=\overline{1,9},\ j=\overline{1,v_i},\ k \in M_i^j, \qquad (14)$$

где c_{ijk} – затраты, обеспечивающие соответствующие ожидаемые оценки d_{ijk}^* аудиторов после будущей модернизации ПТСЗИ; $c_{ijk}^{дост}$ – затраты, достаточные для обеспечения текущего режима полного функционирования комплекса, при котором все его компоненты используются и работают без нарушений; $Э_{ij}^*$, $Э_i^*$, $Э^*$ – ожидаемые оценки функциональной эффективности.

Для (7) используя известный приём[1], введена нижняя граница ожидаемой функциональной эффективности всех компонентов ПТСЗИ, и она максимизируется целевой функцией

$$r \to \max, \qquad (15)$$

с линейными ограничениями (8) – (14) и

$$Э_{ij}^* \ge r,\ i=\overline{1,9},\ j=\overline{1,v_i}, \qquad Э_i^* \ge r,\ i=\overline{1,9}, \qquad Э^* \ge r, \qquad (16)$$

где r – неотрицательная переменная, играющая роль нижней границы ожидаемой функциональной эффективности всех компонентов ПТСЗИ.

Задача ЛП с целевой функцией (15), линейными ограничениями (8-13), (16) и условиями неотрицательности переменных (14), эквивалентна задаче (7), (8-14). Решение задачи (8) – (16) даёт ответ на вопрос, как распределить имеющуюся сумму W, чтобы максимизировать функциональную эффективность ПТСЗИ и всех её компонентов.

Задача 2 (о минимизации суммарных затрат для обеспечения заданного уровня $U \in [0,1]$ функциональной эффективности ПТСЗИ и всех её компонентов).

Сформулирована задача ЛП с целевой функцией

[1] Носков С.И. Технология моделирования объектов с нестабильным функционированием и неопределенностью в данных. – Иркутск: Облинформпечать, 1996. – 321 с.

$$\sum_{i=1}^{9}\sum_{j=1}^{v_i}\sum_{k\in M_i^j} c_{ijk} \to \min, \qquad (17)$$

с линейными ограничениями (8) – (12), (14) и

$$Э_{ij}^{*} \ge U,\ i=\overline{1,9},\ j=\overline{1,v_i}, \qquad Э_{i}^{*} \ge U,\ i=\overline{1,9}, \qquad Э^{*} \ge U. \qquad (18)$$

Решение задачи ЛП (8) – (12), (14), (17), (18) даёт ответ на вопрос, какие затраты необходимы и как их распределить, чтобы обеспечить заданный уровень функциональной эффективности *U* для ПТСЗИ и всех её компонентов.

В четвёртой главе описаны и апробированы созданные программы: программа «Агрегированное оценивание функциональной эффективности» (АОФЭ) и программа «Оптимальное распределение денежных средств» для повышения функциональной эффективности ПТСЗИ предприятия — «ОРДС». Программа «АОФЭ» позволила для предприятия ООО «ЯНТА» 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. Блок-схема алгоритма программы «АОФЭ» представлена на рис.2. Пользователями программы «АОФЭ» и «ОРДС» могут быть как специалисты в области анализа данных, так и исследователи, ориентированные на решение прикладных задач.

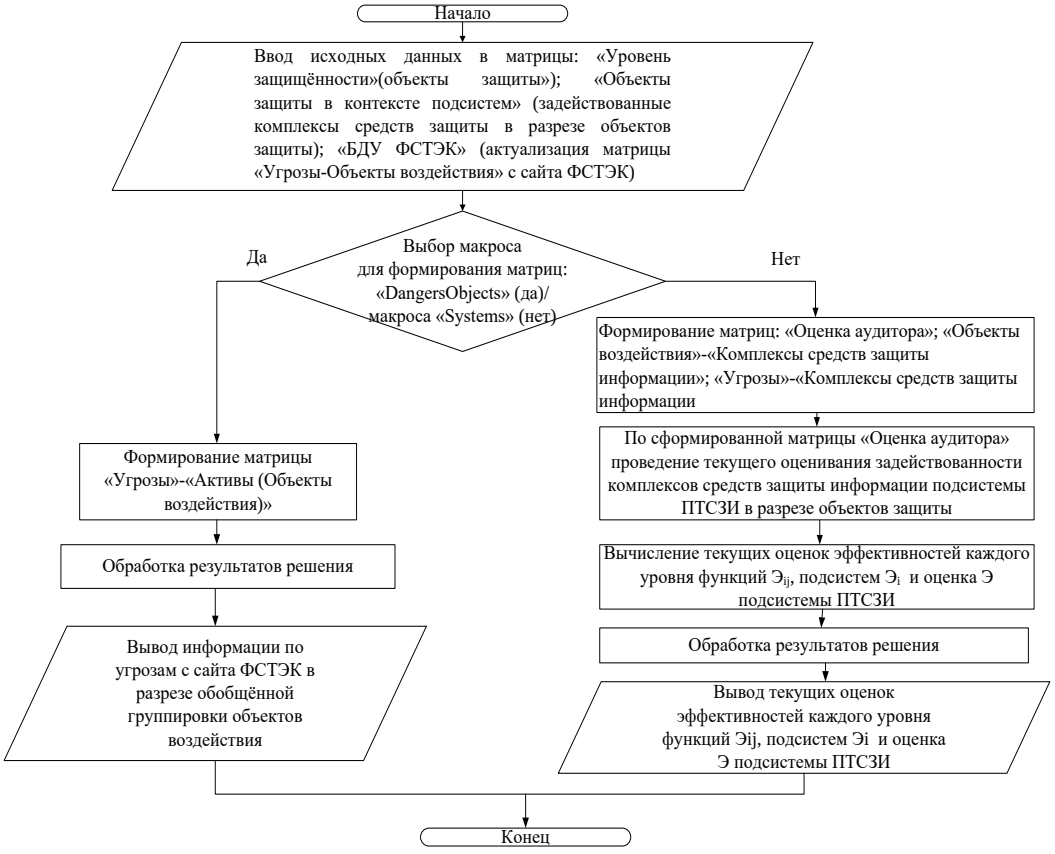

Рис. 2. Блок-схема алгоритма программы «АОЭФ»

Формирование матриц, используемых в программе «АОФЭ», основано на концептах и взаимосвязях, определённых в онтологической модели ПТСЗИ (глава 2). Это поз-

волило в рамках рассматриваемой главы автоматизировать создание двумерных матриц с помощью макросов «DangersObjects» и «Systems», обеспечив согласованность данных и корректность расчётов. Также эта программа обеспечивает визуализацию всех задействованных компонентов в матричной форме, используя 6 уровневую цветовую шкалу. Это упрощает анализ и интерпретацию данных.

Исходными данными для «АОФЭ» послужили сведения об информационных активах (объектах воздействия), подсистемах и комплексах СрЗИ ПТСЗИ предприятия ООО «ЯНТА». С учётом исходных данных и с помощью программы «АОФЭ» была получена оценка текущей функциональной эффективности ПТСЗИ с учётом максимальной (значение «1» по вкладке «Оценка аудитора») аудиторской оценки.

Блок-схема алгоритма программы «ОРДС» представлена на рис.3. Программа «ОРДС» реализована с использованием решателя LPSolve IDE v5.5.2.12 и ориентирована на рациональное распределение ресурсов для улучшения защитных мер.

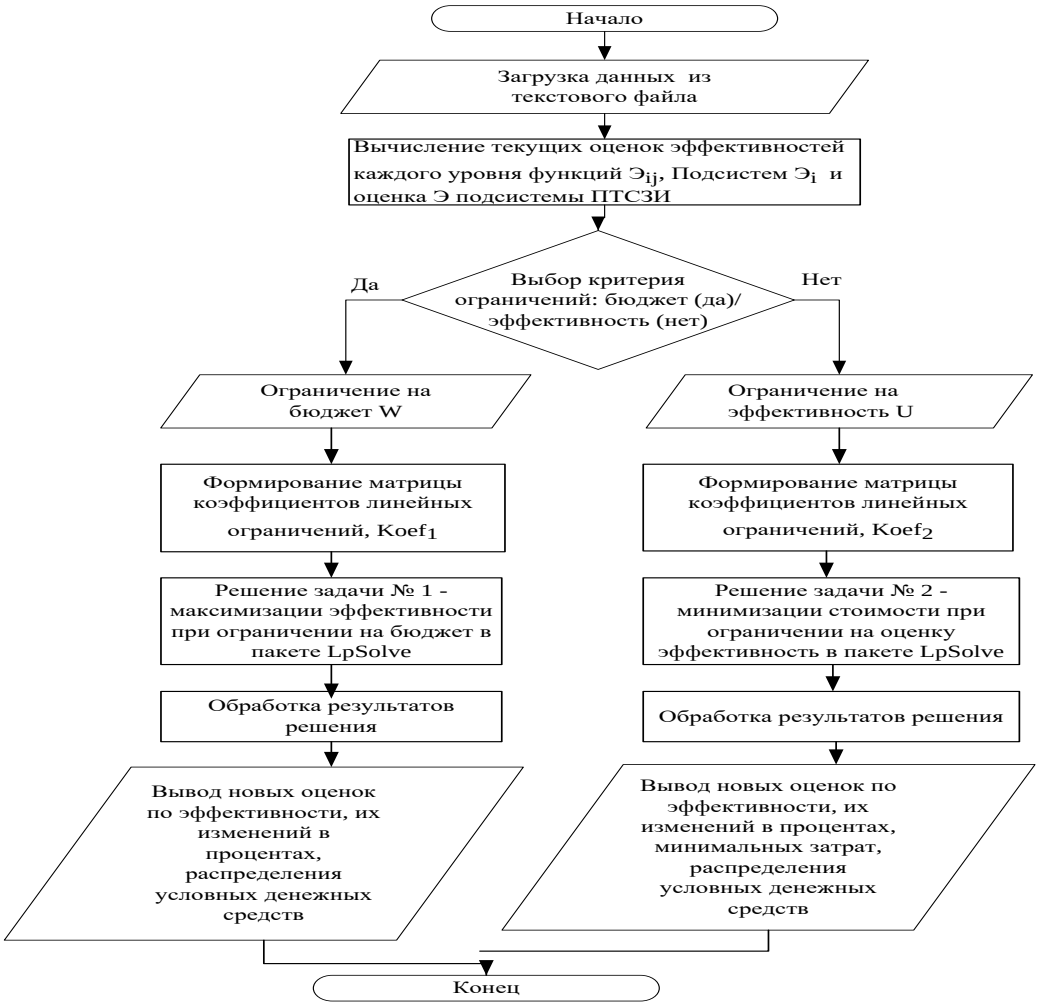

Рис. 3. Блок-схема алгоритма программы «ОРДС»

Программно-алгоритмическая реализация «АОФЭ» и «ОРДС» протестирована на исходных данных предприятия ООО «ЯНТА». Получен акт внедрения. Результаты, приведенные в таблице 2, демонстрируют увеличение показателя функциональной эффективности ПТСЗИ на предприятии ООО «ЯНТА» с коэффициента 0,63 до 0,98, что стало

возможным благодаря привлечению дополнительных финансовых инвестиций в размере 10 млн руб.

Как следует из таблицы 2, общая эффективность (Э) ПТСЗИ до оптимизации составляла 0,63, что отражет недостаточную сбалансированность и результативность применения отдельных подсистем ПТСЗИ. Кроме того, таблица содержит оценку функциональной эффективности отдельных подсистем ПТСЗИ «до» (текущая эффективность) и «после» оптимизации.

Таблица 2. Результаты расчётов по программе «ОРДС»

Оценка функциональной эффективности ПТСЗИ			Оценка функциональной эффективности подсистем ПТСЗИ		Распределение финансовых средств для повышения эффективности функционирования подсистем ПТСЗИ	
Символ	При текущих затратах в 22 млн. руб.	При W=10 млн. руб. (привлечение финансовых инвестиций)	Эффективность	При текущих затратах в 22 млн. руб.	При W=10 млн. руб. (привлечение финансовых инвестиций)	
Э	0,63	**0,98**	$Э_1$	0,73	**0,98**	**1 794 662,59**
			$Э_2$	0,5	**0,98**	**2 339 112,01**
			$Э_3$	0,33	**0,98**	**177 111,25**
			$Э_4$	0,99	**0,99**	**0**
			$Э_5$	0,5	**0,98**	**87 497,87**
			$Э_8$	0,69	**0,98**	**1 401 718,76**
			$Э_9$	0,5	**0,98**	**4 199 897,52**

Для большинства подсистем (например, $Э_1$, $Э_2$, $Э_3$, $Э_5$, $Э_8$, $Э_9$) текущая эффективность составляла от 0,33 до 0,73, указывая на наличие "узких мест" в защите информации. Для выполнения мероприятий по повышению функциональной эффективности ПТСЗИ и её компонентов было установлено ограничение на привлечение дополнительных финансовых инвестиций в размере 10 млн рублей с целью решить задачу по перераспределению финансовых ресурсов так, чтобы устранить неэффективные элементы, максимизировав при этом общую эффективность ПТСЗИ. В результате, после перераспределения средств: 1) эффективность каждой подсистемы была доведена до значений 0,98, за исключением подсистемы $Э_4$, чья эффективность и «до» оптимизации была на высоком уровне 0,99; 2) эффективность (Э) ПТСЗИ возросла до 0,98, что близко к максимально возможному значению.

Решение второй задачи ЛП для обеспечения минимизации затрат при заданном уровне функциональной эффективности U = 0,63 ПТСЗИ для этого предприятия показало, что минимальные затраты на обеспечение указанного уровня функциональной эффективности составят 1,68 млн руб.

В заключении приводятся основные результаты работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе получены следующие результаты.

1. Выявлены недостатки существующих методов и показателей ИБ. Особое внимание уделено проблеме получения достоверных исходных данных при экспертном оценивании, учитывая разные типы организаций. Проведён анализ современных подходов к онтологическому моделированию СЗИ. Показана значимость онтологий как инструмента унификации терминологии, структурирования данных, повышения качества анализа с точки зрения выбора наилучших решений в области затрат на ИБ и снижения влияния субъективных факторов.

2. На основе результатов системного анализа, разработана подробная онтологическая модель ПТСЗИ и её составляющих компонентов. Эта модель не только формализует знания о компонентах системы, но и служит методологической основой для разработки алгоритмического обеспечения и методики агрегированного оценивания эффективности её функционирования. Созданные модели определения исходных данных позволили выделить ключевые показатели функциональной эффективности, структурировать их по уровням и обеспечить логическую взаимосвязь между компонентами системы.

3. Разработано алгоритмическое обеспечение агрегированного оценивания эффективности функционирования ПТСЗИ предприятия через систематизацию её компонентов (объектов защиты, угроз, комплексов средств защиты, подсистем и функций подсистем), что позволило построить: кубическую матрицу «Угрозы – Активы – Комплексы средств защиты информации»; связанные двумерные матрицы и модели эффективности, включая визуализацию результатов оценивания.

4. Сформулированы две задачи ЛП: а) задача максимизации нижней границы функциональной эффективности ПТСЗИ и всех её компонентов при заданном ограничении на бюджет; б) задача минимизации бюджетных затрат для обеспечения заданного уровня функциональной эффективности ПТСЗИ. Это позволяет повысить эффективность соответствующих управленческих решений.

5. Созданы две программы: программа «АОФЭ» для реализации методики агрегированного оценивания и визуализации компонентов ПТСЗИ, а также программа «ОРДС» для принятия решений по повышению функциональной эффективности ПТСЗИ предприятия.

6. Используя программы «АОФЭ» и «ОРДС» на предприятии ООО «ЯНТА» проведена оценка состояния ПТСЗИ и выработаны рекомендации по повышению её функциональной эффективности с учётом бюджета. Получен акт внедрения.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

В журналах из Перечня ВАК

1. Наседкин, П. Н. Оценка состояния комплексной системы защиты информации на основе онтологий / **П. Н. Наседкин,** Л. В. Аршинский // Информационные и

математические технологии в науке и управлении. – 2023. – № 1(29). – С. 158-177. – DOI 10.38028/ESI.2023.29.1.014. (**К2**)

2. Наседкин, П. Н. Методика оценки уровня защищённости программно-технических решений комплексной системы защиты информации предприятия / **П. Н. Наседкин**, М. П. Базилевский // Современная наука: актуальные проблемы теории и практики. Серия “Естественные и технические науки”. – 2023. – № 3. – С. 87-93. – DOI 10.37882/2223-2966.2023.03.27. (**К3**)

3. Базилевский, М. П. Формализация модели информационной безопасности предприятия в виде многокритериальной задачи линейного программирования / М.П. Базилевский, **П.Н. Наседкин**, // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11, № 3(42). – С. 10-11. – DOI 10.26102/2310-6018/2023.42.3.021. (**К2**)

4. Глухов, Н.И. Аналитика внутренних угроз информационной безопасности предприятий / Н. И. Глухов, **П. Н. Наседкин** // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2021. - Т. 24, № 1. - С. 33-41. - DOI 10.21293/1818-0442-2021-24-1-33-41. (К2, входит по шифру научной специальности 2.3.1. с 2022)

Свидетельства о государственной регистрации программы для ЭВМ

5. Свидетельство о государственной регистрации программы для ЭВМ № 2023618996 от 03.05.2023 : Создание матрицы по укрупнённой группировке объектов воздействия со стороны угроз безопасности информации и построение с учётом прототипа онтологической модели Комплексной Системы Защиты Информации (КСЗИ) корреляционных взаимосвязей: «Объект воздействия Комплексы СрЗИ», «Угрозы – Комплексы СрЗИ», «Угрозы – Объекты воздействия» / **П.Н. Наседкин**, В.А. Сверкунов ; правообладатель ФГБОУ ВО ИрГУПС. – Зарегистрировано Федеральной службой по интеллектуальной собственности. – Бюл. № 5. – 03.05.2023. – URL: https://fips.ru/EGD/f48eda73-9720-4660-886e-a862b643bb43 (дата обращения: 20.10.2024).

6. Свидетельство о государственной регистрации программы для ЭВМ № 2024616201 от 18.03.2024 : Программа оптимального распределения денежных средств для принятия решений по повышению эффективности программно-технических комплексов защиты информации предприятия / **П.Н. Наседкин**, М.П. Базилевский ; правообладатель ФГБОУ ВО ИрГУПС. – Зарегистрировано Федеральной службой по интеллектуальной собственности. – Бюл. № 3. – 18.03.2024. – URL: https://fips.ru/EGD/eecb6fa2-1c4e-4c2c-80b2-697999608ae6 (дата обращения: 20.10.2024).

Статьи в сборниках трудов конференций

7. Наседкин, П.Н. Применение нечёткого присоединённого логического вывода в оценке эффективности функционирования комплексной системы защиты информации предприятий / **П. Н. Наседкин**, Л. В. Аршинский, Н. И. Глухов // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности : Материалы межвузовской научно-теоретической конференции (в рамках Сибирского

форума "Информационная безопасность - 2021"), Новосибирск, 29 ноября - 03 2021 года / Под редакцией А.В. Ефимова, Т.И. Монастырской, И.В. Балабан. - Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. - С. 42-52.; URL: https://www.elibrary.ru/item.asp?id=47474022 (дата обращения: 28.05.2023).

Статьи в рецензируемых журналах и сборниках научных трудов

8. Глухов, Н.И. Онтологические модели в процессе управления информационными рисками и информационной безопасности хозяйствующих субъектов / Н. И. Глухов, **П Н. Наседкин**// Информационные технологии и математическое моделирование в управлении сложными системами. – 2020. – № 2(7). – С. 24-31. – DOI 10.26731/2658-3704.2020.2(7).24-31.

9. Милько Д.С. Экспертная система оценки угроз безопасности информации. Формальное представление объектов воздействия / Д.С. Милько, **П.Н. Наседкин** // Молодая наука Сибири. – 2021. – № 2(12). – С. 280-292.

10. Глухов, Н. И. Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности / Н. И. Глухов, **П.Н. Наседкин**, Д. С. Милько // Информационные технологии и математическое моделирование в управлении сложными системами. – 2021. – № 3(11). – С. 59-66. – DOI 10.26731/2658-3704.2021.3(11).59-66.

11. Глухов, Н.И. Разработка элементов онтологии комплексной системы защиты информации предприятия / Н. И. Глухов, **П. Н. Наседкин**, // Информационные технологии и математическое моделирование в управлении сложными системами. – 2021. – № 1(9). – С. 35-42. – DOI 10.26731/2658-3704.2021.1(9).35-42.

12. Наседкин, П. Н. Анализ востребованности компонентов уровня программно-технических решений КСЗИ предприятия с точки зрения обеспечения базовых требований по информационной безопасности / **П.Н. Наседкин** // Информационные технологии и математическое моделирование в управлении сложными системами. – 2022. – № 2(14). – С. 50-64. – DOI 10.26731/2658-3704.2022.2(14).50-64.