ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

На правах рукописи

Полтавцева Мария Анатольевна

АДАПТИВНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ ПРОМЫШЛЕННЫХ СИСТЕМ НА ОСНОВЕ СИСТЕМОЛОГИЧЕСКОГО ПОДХОДА

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени доктора технических наук

Санкт-Петербург
2021

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО СПбПУ) в Институте кибербезопасности и защиты информации.

Научный консультант:
доктор технических наук, профессор РАН, профессор Зегжда Дмитрий Петрович.

Официальные оппоненты:
доктор технических наук, профессор Будзко Владимир Игоревич, федеральный исследовательский центр «Информатика и управление» Российской Академии Наук (ФИЦ ИУ РАН), заместитель директора по научной работе.

доктор технических наук, профессор Ныркov Анатолий Павлович, федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», профессор.

доктор технических наук, профессор Хомоненко Анатолий Дмитриевич, федеральное государственное образовательное бюджетное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», И.О. заведующего кафедрой Информационные и вычислительные системы.

Ведущая организация:
ФГБОУ ВО «Российский государственный гидрометеорологический университет»

Защита состоится «05» октября 2021 года в ____ ч. на заседании диссертационного совета У.05.13.19 федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (195251, г. Санкт-Петербург, ул. Политехническая, д. 29, Главный корпус, ауд. 175).

С диссертацией, авторефератом можно ознакомиться в библиотеке и на сайте www.spbstu.ru федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Автореферат разослан «___» _____ 2021 года.

Ученый секретарь
диссертационного совета У.05.13.19,
кандидат физико-математических наук  Шенец Николай Николаевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Расширение функций систем обеспечения безопасности, их автоматизация и интеллектуализация привели к необходимости создания и совершенствования специального класса комплексов контроля, обнаружения и исследования инцидентов безопасности. Задачами современных систем мониторинга информационной безопасности являются:

– выявление нарушений информационной безопасности, причин и механизмов их возникновения;

– анализ рисков, перспективы ликвидации последствий и возможность предупреждения атак, разработка сценариев проактивной защиты;

– прогноз состояния безопасности, выявления трендов новых атак, разработка сценариев антиципационного реагирования и предупреждения деструктивных воздействий.

В цифровизированных промышленных объектах решение перечисленных задач базируется на разнообразных технологиях искусственного интеллекта. К ним относятся: нейронные сети, методы анализа временных рядов на основе статистического и спектрального анализа, метод разладки и другие. Эти решения строятся на базе технологий Больших данных для структурирования и оптимизации обработки большого объема разнородной информации с целью обеспечить адаптивное управление безопасностью и снизить риски.

Современные работы в области мониторинга информационной безопасности (МИБ), направлены, в основном, на развитие отдельных методов решения задач безопасности и обеспечение устойчивого функционирования киберфизических систем (КФС) в условиях киберугроз. Проблеме обеспечения методов анализа исходными данными, сохранению полноты и оперативности оценок в условиях изменений объекта и внешней среды, уделяется меньше внимания. Исходные данные для решения задач безопасности должны быть структурированы и обладать должной полнотой для каждого типа объекта защиты и метода анализа, что обеспечивается соответствующими моделями, методами и инструментами. При этом возникают следующие противоречия:

– Различные задачи и методы требуют различной глубины мониторинга, режимов сбора, подготовки и анализа данных, что значительно усложняет создание универсальных систем.

– Применяемые методы анализа требуют различной структуры и характеристик входных данных. Возникает необходимость использования разных моделей и методов (иногда многоэтапных) обработки информации.

– Стремление к увеличению числа измеряемых параметров, уровней иерархии, снижение интервалов измерений для обеспечения точности зачастую не приводят к повышению точности оценок, вызывая дополнительные трудности и увеличивая требования к вычислительным ресурсам.

Таким образом, для повышения достоверности оценки прогноза и управления безопасностью объектов КИИ, возможности антиципационной оценки рисков и повышения точности представления объекта защиты системы мониторинга информационной безопасности должны создаваться как интеллектуальные комплексы с распределенным адаптивным управлением на основе технологий Больших данных, обладающие гибкой архитектоникой и способностью к адаптивной саморегуляции и самообучению. Возникает необходимость всестороннего анализа задач МИБ и поиска путей его совершенствования, для чего автор предлагает системологический подход, основанный на адаптивном управлении МИБ, заключающемся в установлении соответствия между целями и задачами мониторинга, методами обработки, режимом сбора данных и представлением объекта исходя из конкретики объекта защиты и требуемой степени информированности о его состоянии.

Степень разработанности темы исследования. Созданию систем мониторинга безопасности, в том числе на сложные промышленные КФС (ПКФС), посвящено значительное число работ. Среди них – работы таких ученых, как А. Окутан, В. Хоа, Э.Кнапп, А. Колетта, Ю. Янг, Ф. Харроу, С.А. Петренко, И.В. Котенко, Д.Н. Бирюков, О.И. Шелухин, И.Б. Саенко. Ряд работ посвящен разработке методов и подходов к управлению данными в системах мониторинга. К ним также относятся работы Семенова В.В., Т. Класа, Ю. Гертнера, К. Брандауэра, Т.Е. Фарранда, А. Саджи, С. Маршала, Г. Маногарана. В диссертационной работе обобщаются методы и архитектурные решения этих исследований и формируется целостный подход к решению задачи адаптивного мониторинга информационной безопасности.

Объектом исследования являются системы мониторинга информационной безопасности промышленных киберфизических систем. Под ПКФС понимаются промышленные системы с развитой сетевой инфраструктурой, в отношении которых реализуются компьютерные атаки.

Предметом исследования являются методы мониторинга безопасности, включая методы адаптивного управления, сбора, подготовки и анализа данных,

как основа технологии интеллектуального адаптивного управления безопасностью ПКФС.

Цель исследования состоит в обеспечении и поддержании полноты, достоверности и оперативности информирования об инцидентах безопасности КФС в условиях эволюционных изменений объекта защиты и среды его функционирования путем создания системологического подхода и методологии адаптивного управления мониторингом информационной безопасности промышленных КФС на основе отображения множеств задач безопасности, методов их решения и данных объекта защиты, а также технологий, основанных на данных.

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

1. Провести анализ систем мониторинга информационной безопасности, специфики современных КФС как объекта защиты, выполнить систематизацию задач МИБ и постановку задачи адаптивного мониторинга информационной безопасности КФС (АМИБ).
2. Разработать принципы системологического подхода к адаптивному мониторингу информационной безопасности КФС на основе общей теории систем и системного анализа и построить модель, определяющую взаимосвязь АМИБ с системой управления информационной безопасностью;
3. Разработать методологию управления АМИБ, позволяющую обеспечить полноту мониторинга ПКФС путем взаимного отображения множеств возможных задач безопасности, методов их решения и наборов данных, включая:

– построение взаимного отображения множеств задач безопасности, методов их решения и наборов данных объекта защиты;

– разработку метода интеллектуального управления АМИБ промышленных КФС на основе поиска оптимальной схемы мониторинга;

– разработку подхода к оценке характеристик мониторинга ПКФС на основе теории управления.

4. Разработать модель объекта защиты, адаптивную к различным способам структурной и функциональной организации объекта мониторинга и позволяющую описать ракурсы рассмотрения объекта мониторинга, соответствующие подходу системного анализа, включая:

– построение метамодели промышленной КФС для обеспечения взаимодействия управления АМИБ и подсистемы управления данными [1] на основе концепции универсального решателя системных задач (УРСЗ);

– разработка основанной на данных (Data-driven) модели объекта мониторинга с использованием связанных графов.

5. Разработать методы обработки данных и управления Большими данными в системе мониторинга безопасности КФС, включая:

– формализацию структур данных в задачах адаптивного мониторинга информационной безопасности КФС;

– разработку методов обработки данных, включая методы одномерной и многомерной агрегации потоковых данных самоподобных процессов и метод интеллектуального анализа гетерогенных данных на основе паттернов;

– разработку метода управления Большими данными при адаптивном мониторинге информационной безопасности промышленных КФС для реализации управления мониторингом.

6. Разработать макет системы адаптивного мониторинга информационной безопасности ПКФС, провести практическое исследование методов управления мониторингом и экспериментальную оценку методов управления и обработки данных.

Научная новизна результатов:

1. Предложен новый системологический подход к адаптивному мониторингу информационной безопасности ПКФС, включающий принципы целостности, конвергенции и иерархической связности. Подход состоит в выборе взаимного отображения между множествами задач мониторинга информационной безопасности, методов их решения и наборов данных объекта защиты, а также адаптации подсистемы обработки данных мониторинга к выбранным методам.

2. Разработан метод интеллектуального управления адаптивным мониторингом информационной безопасности, основанный на решении задачи оптимального выбора схемы мониторинга.

3. Сформулированы условия достаточности и не избыточности взаимных отображений задач безопасности, методов их решения и наборов данных объекта защиты. Сформулированы условия, при выполнении которых показано, что методология управления адаптивным мониторингом при

[1] Под управлением данными понимается вся деятельность, целью которой является определение, создание, хранение, поддержка данных, включая механизмы доступа и манипулирование информацией.

системологическом подходе позволяет обеспечить полноту, достоверность и оперативность мониторинга.

4. Разработаны метамодель промышленной киберфизической системы как объекта адаптивного мониторинга безопасности и модель объекта мониторинга на основе данных (Data-driven) с использованием связанных графов. Предложенные метамодель и модель обладают полнотой в отношении решения задач безопасности и отличаются адаптивностью к различным способам структурной и функциональной организации объекта защиты.

5. Предложены новые методы обработки данных для управления информацией в системах адаптивного мониторинга безопасности КФС, включая:

- методы одномерной и многомерной агрегации потоковых данных самоподобных процессов, отличающиеся введением иерархических (PCR – Parent-Child-Relation) временных связей;
- метод анализа гетерогенных данных об объекте защиты в условиях неполноты исходных данных на основе представления систем как набора объектов и их свойств («bag of objects») и анализа паттернов;
- метод управления Большими данными мониторинга, использующий двухэтапную предварительную обработку данных, сочетание потоковой и пакетной обработки информации и миграцию данных между разными типами хранилищ;

6. Предложен подход к оценке параметров мониторинга на основе теории управления путем выражения характеристик полноты, достоверности и оперативности мониторинга через характеристики наблюдаемости и идентифицируемости технических систем.

Теоретическая значимость работы заключается в создании нового системологического подхода к адаптивному мониторингу информационной безопасности КФС, основанного на принципах целостности, конвергенции и иерархической связности. В рамках созданного подхода разработаны:

1. Методология управления адаптивным мониторингом информационной безопасности промышленных киберфизических систем, включая:
   - метод интеллектуального управления адаптивным мониторингом информационной безопасности промышленных КФС на основе оптимального выбора схемы мониторинга;
   - метамодель объекта защиты на основе универсального решателя системных задач;

- модель объекта защиты на основе данных с использованием связанных графов, отражающая иерархию рассмотрения объекта защиты.
- подход к оценке мониторинга КФС на основе теории управления, выражающий характеристики полноты, достоверности и оперативности МИБ через характеристики наблюдаемости и идентифицируемости объекта управления.

2. Методы обработки и управления данными ПКФС в АМИБ, включая:
   - метод управления Большими данными при адаптивном мониторинге информационной безопасности промышленных КФС обеспечивающий поддержку управления мониторингом;
   - методы одномерной и многомерной агрегации потоковых данных самоподобных процессов;
   - метод интеллектуального анализа гетерогенных данных на основе паттернов.

Практическая значимость работы определяется возможностью использования разработанных подхода, методов и моделей для построения систем адаптивного мониторинга информационной безопасности промышленных КФС. Результаты работы позволяют:

– обеспечить полноту решения задач безопасности и полноту исходных наборов данных для методов анализа при адаптивном мониторинге информационной безопасности ПКФС за счет интеллектуального управления адаптивным мониторингом и модели объекта защиты, основанной на данных;

– обеспечить оперативность решения задач безопасности при мониторинге информационной безопасности промышленных КФС за счет интеллектуального управления адаптивным мониторингом путем генерации оптимальной схемы мониторинга безопасности;

– снизить время одномерной и многомерной агрегации потоковых данных самоподобных процессов и сократить объем данных, хранимых в оперативной памяти, используя разработанные методы агрегации потоковых данных;

– реализовать поддержку принятия решений в условиях неполноты и гетерогенности описаний исходных объектов и систем путем прецедентного анализа с использованием подхода «bag of objects», в том числе при мониторинге угроз и оценке защищенности КФС.

Методы исследования. Для решения поставленных задач в диссертационной работе использовались методы математического моделирования, имитационного моделирования на основе данных, дискретной

многокритериальной оптимизации, дискретной и вычислительной математики, теории графов, теории обработки и управления данными, прецедентного анализа данных, теории защиты информации, теории управления, системного подхода и теории систем.

Положения, выносимые на защиту:

1. Системологический подход к адаптивному мониторингу информационной безопасности, включающий принципы целостности, конвергенции и иерархической связности и обеспечивающий полноту решения задач безопасности АМИБ в условиях эволюции объекта защиты и внешней среды.
2. Методология управления АМИБ на основе отображения множеств задач безопасности, методов их решения и наборов данных объекта защиты.
3. Метамодель объекта защиты на основе универсального решателя системных задач и модель ПКФС на основе данных, обеспечивающие полноту рассмотрения объекта защиты при решении задач безопасности.
4. Метод управления Большими данными в системах адаптивного мониторинга включающий схему предварительной двухэтапной иерархической обработки данных и три типа хранилищ данных для обеспечения полноты решения задач безопасности.
5. Методы потоковой агрегации данных использующие иерархическую связь между наборами самоподобных данных и метод интеллектуального анализа гетерогенных данных в условиях неполноты и неточности описаний объектов при решении задач безопасности в АМИБ.

Соответствие специальности научных работников. Полученные научные результаты соответствуют следующим пунктам паспорта специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность»: теория и методология обеспечения информационной безопасности и защиты информации (п. 1); модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования (п. 6); модели и методы оценки защищенности информации и информационной безопасности объекта (п. 9); принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (п.13).

Степень достоверности результатов исследования подтверждается их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе, корректностью применения апробированных современных теоретических положений и математических методов совокупности с экспериментальными исследованиями, а также апробацией результатов в научных публикациях и докладах на конференциях.

Внедрение результатов работы. Полученные основные научные результаты диссертационной работы использованы при выполнении гранта Президента Российской Федерации для государственной поддержки ВНШ Российской Федерации по теме «Управление безопасностью и устойчивым функционированием киберфизических систем с адаптивной топологией» (соглашения № 075-02-2018-504, № 075-15-2019-1066 на 2018-2019 г.), исследованиях: «Разработка технологии высокопроизводительной обработки и визуализации больших массивов данных в крупномасштабных сетях электронных потребительских устройств (Internet of Things)» (ФЦП, соглашение № 14.575.21.0100 шифр заявки «2014-14-576-0149-013»); «Исследование и разработка технологии автоматического управления кибербезопасностью в крупномасштабных коммуникационных сетях беспилотного транспорта на базе суперкомпьютерных эластичных вычислений» (ФЦП, уникальный идентификатор Соглашения RFMEFI57816X0224 шифр заявки «2016-14-579-0009-011»); «Предотвращение сетевых атак на основе технологии больших данных и высокопараллельного эвристического анализа сверхвысоких объемов трафика в магистральных сетях Интернет» (ФЦП, уникальный идентификатор проекта RFMEFI57817X0231 шифр заявки «2017-14-579-0002-001»). А также, в проектной деятельности АО «НПО «Эшелон», ОАО «НИИ «Рубин», ЗАО «Институт телекоммуникаций», в проектной деятельности Санкт-Петербургского отделения Российской инженерной академии и в учебном процессе Института кибербезопасности и защиты информации ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» при организации дисциплин «Высокопроизводительные системы анализа данных», «Методы анализа данных и естественно языковых текстов», «Системы управления базами данных» в виде методических рекомендаций по проведению лекционных, практических и лабораторных занятий, а также для сопровождения научной деятельности аспирантов и докторантов по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», что подтверждается соответствующими актами о внедрении.

Апробация работы. Основные результаты исследований и научных разработок докладывались и обсуждались на следующих конференциях: научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2016-2020), межрегиональная конференция «Региональная информатика и информационная безопасность» (Санкт-Петербург, 2017), международная конференция «Security of Information and Networks» (Джапур (Индия), 2017), международная конференция «Industrial Cyber-Physical Systems» (Санкт-Петербург, 2018), международная конференция «Управление развитием крупномасштабных систем» (Москва, 2018-2020), международная конференция «Intelligent Systems Conference» (Лондон (Великобритания) 2018), международная конференция «International Black Sea Conference on Communications and Networking» (Сочи, 2019), международная конференция «Ivannikov Memorial Workshop» (Новгород, 2019), Всероссийское совещание по проблемам управления ВСПУ-2019 (Москва, 2019), международный семинар «Nonlinear phenomena in complex systems» (Минск (Беларусь), 2019-2020), международная конференция «Engineering & Telecommunication» (Московская обл., г. Долгопрудный, 2020), международная конференция «Технологическая трансформация: новая роль человека, машин и управления» (Санкт-Петербург, 2020), международная конференция «Открытая конференция ИСП РАН им. В.П. Иванникова» (Москва, 2020). Результаты работы победили в 2020 году в конкурсном отборе по выделению грантов аспирантам и молодым ученым на исследования, которые направлены на обеспечение информационной безопасности для задач цифровой экономики (конкурс «Грант ИБ»).

Публикации по теме диссертации. Результаты диссертационной работы отражены в 63 публикациях, в том числе в 18 публикациях в рецензируемых журналах из перечня ВАК, рекомендованных для работ по специальности 05.13.19, 23 изданиях, индексируемых Scopus и Web of Science, монографии и разделе в монографии, двух свидетельствах о регистрации программы для ЭВМ, патенте РФ на изобретения.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованных источников из 274 наименований. Общий объем работы составляет 296 страниц, в том числе 81 рисунок и 20 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулирована цель, определены основные задачи, научная

новизна и практическая значимость полученных результатов, а также положения, выносимые на защиту. Представлены сведения по апробации работы и приведено краткое содержание диссертации по главам.

В первой главе проведен анализ развития систем МИБ, выделены такие тенденции, как: ориентирование на обработку и анализ Больших данных; эволюция методов мониторинга в сторону интеллектуализации; использование особых свойств данных и трафика (в частности, самоподобия и мультифрактальности). Ключевым фактором является изменение роли МИБ от инструмента оценки соответствия в сторону постоянного процесса наблюдения и анализа результатов регистрации событий безопасности для выявления нарушений, угроз и уязвимостей. В связи с этим, в работе отмечается значительное расширение задач безопасности, решаемых при МИБ, а также повышение требований к степени автоматизации и рабочим характеристикам, таким, как достоверность и оперативность систем МИБ.

В главе представлена специфика ПКФС как объекта защиты с точки зрения задач мониторинга, заключающаяся в: гетерогенности составляющих и технологий, включая большое число низко-ресурсных составляющих; распределенной организации; динамической структуре, эволюционирующей в процессе функционирования. Защита КФС осложняется их связью с физическим процессом и требованием устойчивости, то есть, сохранения целостности физического процесса во времени в условиях кибератак. Показано, что в современной концепции МИБ система мониторинга предоставляет информационное обеспечение для всех этапов управления информационной безопасностью и, таким образом, является одним из ключевых компонентов кибербезопасности промышленных КФС.

Приводится систематизация современных задач и методов МИБ, выделяются такие обобщенные группы задач, как: оценка защищенности включая детализацию и оценку рисков; обнаружение аномалий в функционировании, идентификация компьютерных атак и комплекс задач по управлению инцидентами; управление конфигурацией (структурой и настройкой) КФС для поддержания устойчивого функционирования, где МИБ используется как источник информации для принятия решения. Показано, что в каждой из групп задач присутствует несколько различных подходов и широкий набор конкретных методов решения, которые должны обеспечиваться данными со стороны системы мониторинга. Выбор конкретного метода осуществляется в условиях неопределенности и затруднен целым рядом факторов, связанных со

спецификой как самих методов, так и их реализаций. Показано, что это обусловлено особенностями и ограничениями самих методов.

Сформулированы требования к АМИБ, такие как требование адаптивности и требование обеспечения полноты, достоверности и оперативности мониторинга. Выполнена постановка задачи АМИБ промышленных КФС, заключающаяся в реализации расширяемого набора решаемых задач безопасности и методов их решения с возможностью коррекции набора задач и используемых методов в процессе функционирования на основе динамического представления объекта защиты.

Во второй главе описан системологический подход к адаптивному мониторингу информационной безопасности промышленных киберфизических систем. Основой подхода являются фундаментальные положения теории систем и системного анализа. Рассматривается представление объекта защиты – промышленной КФС – как системы, с выделением таких свойств как иерархичность, интегрированность и связность. Сформулированы основные особенности представления КФС с точки зрения системного анализа при управлении безопасностью: целенаправленность, требование контекста, оценка ресурсов и требование конвергентности. Сформулированы принципы системологического подхода к АМИБ ПКФС.

Принцип целостности подразумевает целостное рассмотрение объекта защиты, промышленной КФС, как системы, в отношении всех задач безопасности, которые должны быть реализованы над ней.

Принцип конвергенции отражает взаимосвязь между различными компонентами системы и с внешней средой, обуславливая необходимость соответствия системы МИБ текущему режиму работы объекта защиты, включая пул доступных параметров, перечень задач безопасности и набор доступных методов их решения.

Принцип иерархической связности акцентирует особенности декомпозиции как ПКФС, так и ракурсов рассмотрения объекта при АМИБ. Он обуславливает возможность декомпозиции и/или агрегации компонентов КФС в отношении любого построенного среза общего представления объекта защиты, где элементы каждой иерархии можно соотнести с другими иерархическими срезами.

В главе дано определение *схемы мониторинга* как набора методов обработки и анализа данных объекта защиты и порядка их применения над группами входных данных. Приведена высокоуровневая модель АМИБ ПКФС, реализующая принцип целостности и задающая взаимосвязь между функциями

МИБ и управлением информационной безопасностью КФС. Представленная модель АМИБ при помощи обобщенных функций мониторинга информационной безопасности промышленных КФС формализует взаимосвязь между управлением информационной безопасностью объектов этого типа и техническими требованиями к мониторингу.

Показано, что для реализации АМИБ в рамках системологического подхода для реализации принципа конвергенции необходимо решить задачу взаимного отображения между задачами безопасности, методами решения и наборами данных. Заданы: $I = \{i_1, \dots, i_I\}$ – множество задач безопасности, определенных со стороны внешней среды как требование к системе управления безопасностью, и, следовательно, АМИБ; $M = \{m_1, \dots, m_M\}$ – множество методов решения задач безопасности, потенциально применимых к данной ПКФС; $D = \{d_1, \dots, d_D\}$ – множество наборов данных в системе АМИБ, как собираемых со стороны объекта защиты, так и преобразованных от них в процессе выполнения процедур мониторинга. Их взаимосвязь описывается отображениями:

$F_{ID}: I \to D$ – отображение задач безопасности на множество наборов данных объекта защиты. Обратное отображение $F_{ID}^{-1}: D \to I$ показывает, какая задача решается при помощи конкретных данных.

$F_{IM}: I \to M$ – отображение задач безопасности на множество методов их решения. Обратное отображение $F_{IM}^{-1}: M \to I$ показывает, какую задачу решает заданный метод.

$F_{MD}: M \to D$ – отображение методов решения задач безопасности на множество наборов данных объекта защиты. Обратное отображение $F_{DM}^{-1}: D \to M$ показывает, какой метод использует указанные данные.

В общем случае отображение F_{ID} между задачами безопасности и наборами данных и транзитивное отображение вида $F_{MD}(F_{IM})$ не эквивалентны, также как и обратные: $F_{ID}^{-1} \not\equiv F_{IM}^{-1}(F_{MD}^{-1})$. Это различие обуславливается возможным отсутствием методов решения задачи и/или невозможностью сбора требуемых данных. Сформулированы условия достаточности и не избыточности отображений задач безопасности, методов их решения и наборов данных мониторинга безопасности при построении схемы АМИБ, чтобы исключить изначально не реализуемые или явно избыточные схемы мониторинга, соответствующие указанным ситуациям.

Условие достаточности: если для каждой задачи безопасности $i \in I$ существует подмножество наборов данных $D_i \subseteq D$ от объекта защиты, собираемых и проходящих предварительную обработку, и существует

подмножество методов решения этой задачи $M_i \subseteq M$; такие, что этих данных достаточно для применения этих методов, а методы полностью решают задачу безопасности, тогда в системе АМИБ для данного объекта данная задача может быть решена.

Условие не избыточности: если для каждого набора данных $d \in D$ существует использующее этот набор не-пустое подмножество методов задач безопасности $M_d \subseteq M$ и для каждого из этих методов существует связанная задача (или подмножество задач $I_d \subseteq I$) которую он решает, тогда в системе АМИБ отсутствуют явно избыточные компоненты: все собираемые данные востребованы методами решения задач безопасности, каждый из которых связан с актуальной задачей.

В главе представлена схема АМИБ ПКФС в соответствии со системологическим подходом. Определены основе этапы адаптационного процесса:

1. Оценка состояния, включая оценку выполнения всех целей и задач безопасности, условий достаточности и не избыточности.
2. Процесс корректировки и фиксации множества задач безопасности.
3. Определение допустимых методов решения задач безопасности. При их отсутствии – переход на более высокоуровневую корректировку или задач безопасности, или параметров системы, включая технические возможности по сбору данных и граничные условия на основе ресурсов.
4. Формирование новой схемы мониторинга, включая оценку временных характеристик методов и подготовки данных для них, оценку комплекса прочих граничных условий, решение задачи поиска оптимальной схемы мониторинга.
5. Корректировка схемы сбора и предварительной обработки данных в соответствии с новой схемой мониторинга.

Дано формальное описание схемы мониторинга информационной безопасности как кортежа вида $S = \langle (I^{Cur}, M^{Cur}, D^{Cur}), F_{IM}, F_{MD} \rangle$, включающего текущий набор задач безопасности I^{Cur}, методы их решения M^{Cur} и требуемые ими наборы данных D^{Cur}, а также отображения между задачами, методами и данными F_{IM}, F_{MD}.

Предлагается метод интеллектуального управления АМИБ на основе принципов целостности и конвергенции, заключающийся в решении задачи оптимального выбора схемы МИБ. Исходными данными являются: множество задач безопасности I^{Cur}, множество возможных методов решения M и множество наборов данных D. Множество возможных схем мониторинга S_0

формируется на основе возможных сочетаний задач, методов и данных $R_0 = I^{Cur} \times M \times D$ и последовательно сокращается.

Сначала проводится редукция множества S_0 на основе условий достаточности и не избыточности до множества $S \subseteq S_0$.

Далее формализуется множество параметров схем мониторинга, применимых для каждой схемы $s \in S$:

$$Par = \begin{Bmatrix} pr_q | \forall (i_j \in I^{Cur}, m_k \in M^{Cur}, D_k^{Cur} \subseteq D^{Cur}) \\ \exists Fpr_q(i_j, m_k, D_k^{Cur}) \in \mathbb{R} \end{Bmatrix} \quad (1)$$

где i_j – задача безопасности, m_k – некоторый метод ее решения, D_k^{Cur} – наборы данных, для метода $m_k.Fpr_q(i_j, m_k, D_k^{Cur})$ – целевая функция параметра pr_q, определенная на множестве $\mathbb{R}$ вещественных чисел.

На основе максимизируемых целевых функций параметров схемы (1) определяется общая целевая функция -й схемы s_i МИБ как многопараметрическая функция вида: $F_{s_i}^{\Sigma} = F\left(\sum\left(Fpr_q | q \in [1, |Par|]\right)\right) \to max$, определенная над целевыми функциями параметров. Дальнейшая редукция множества S выполняется на основе набора граничных условий, определенных как $B = \{b_h | b_h = \langle Name, Value \rangle, Value \in \mathbb{R}, h \in [1, H]\}$, где H – общее число граничных условий . Выполнение граничных условий над схемой определяется правилом:

$$\forall b_h \in B \exists pr_q \in Par\left[\left(pr_q.Name = b_h.Name\right) \wedge \left(Fpr_q > b_h.Value\right)\right] \quad (2)$$

В результате редукции по условию (2) формируется множество возможных (потенциально применимых в данных граничных условиях) схем мониторинга $S^{Imp} \subseteq S$. Над потенциально применимыми схемами МИБ S^{Imp} задается отношение доминирования: схема s_x доминирует над s_y ($s_x \succ s_y$) если для всех Fpr_q выполняется неравенство $Fpr_q^{s_x} \geq Fpr_q^{s_y}$ и существует по крайней мере один параметр pr_j, для которого $Fpr_q^{s_x} > Fpr_q^{s_y}$. Эквивалентными считаются схемы мониторинга s_x, s_y ($s_x = s_y$) если для всех Fpr_q значение $Fpr_q^{s_x} = Fpr_q^{s_y}$. Из множества потенциально применимых схем мониторинга удовлетворяющих граничным условиям S^{Imp} исключаются все схемы, для которых в этом множестве существует доминирующая или эквивалентная схема. Таким образом формируется множество оптимальных схем $S^{Opt} = \left\{s_l \middle| (s_l \in S^{Imp}) \wedge \left(\nexists\left(s_g \in S^{Imp}\right) \middle| s_g \succ s_l\right)\right\}$. Показано, что $S^{Opt} \neq \emptyset$. Если $|S^{Opt}| = 1$, то можно говорить что для $S^{Opt} = \{s_l\}$ схема s_l является единственным оптимальным решением и оптимальной схемой МИБ. Показано, что при

$|S^{Opt}| > 1$ множество S^{Opt} является оптимальным по Парето и нуждается в сокращении до единственного решения. Поиск оптимальной схемы мониторинга путем сокращения S^{Opt} в данном случае предлагается проводить на основе приоритезации.

Приведена схема работы метода и показано, что методология управления адаптивным мониторингом при системологическом подходе к АМИБ позволяет обеспечить требования полноты, достоверности и оперативности при выполнении двух *условий*:

1. Полноты и достоверности (адекватности) модели объекта защиты в системе мониторинга и достоверности методов анализа;
2. Отсутствия искажений при передаче данных в систему мониторинга.

Приведен подход к оценке характеристик мониторинга КФС на основе теории управления, проводящий аналогии между объектом управления в управлении техническими системами и КФС как объектом управления информационной безопасностью. На основе этого представления определяются характеристики МИБ (полнота, достоверность, оперативность) через характеристики объекта управления (наблюдаемость, идентифицируемость).

В третьей главе сформулированы требования к модели ПКФС в АМИБ, такие как: адаптивность, универсальность, иерархическая организация и полнота, а также факторы, затрудняющие создание модели: неполнота данных; структурная динамичность и сложность объекта. Рассмотрены подходы к моделированию ПКФС и показано, что модели в рамках подхода на основе данных (Data-driven моделирование) в наибольшей степени отвечают поставленной задаче.

Представлена метамодель промышленной КФС, как объекта мониторинга информационной безопасности, на основе иерархии систем универсального решателя системных задач (УРСЗ), соответствующая принципам целостности и иерархической связности системологического подхода (рисунок 1).

Рисунок 1 – Метамодель промышленной КФС а основе иерархии систем УРСЗ

Показано соответствие между элементами метамодели (порождающими системами и метасистемой) и методами решения задач безопасности согласно принятой схеме мониторинга.

Приведена модель объекта защиты на основе данных в виде набора ассоциированных графов построенная на базе принципов целостности, конвергенции и иерархической связности. В ее основе находится базовая модель объекта защиты в виде орграфа $G_0(V_0, E_0)$. Вершины графа $v_{0,i} \in V_0$ ассоциированы с компонентами КФС и представляют собой структуры данных, описывающие известную информацию о компоненте и его состоянии, включая наборы полученных от него сведений. Ребра $e_{0,k} \in E_0$ в графе $G_0(V_0, E_0)$ представляют собой связи между компонентами системы и формируются на основе коммуникационной информации КФС. Для каждого ребра в графе определена входная и выходная вершины на основании отображения $F: V \to V$, зависимость между вершинами и ребрами графа определяется как: $\forall e_{0,(i,j)} \in E_0 \exists v_{0,i} \in V_0, v_{0,j} \in V_0 \left[Fin\left(e_{0,(i,j)}\right) = v_{0,i} \wedge Fout\left(e_{0,(i,j)}\right) = v_{0,j} \right]$. Тогда любой процесс $p_k \in P$ объекта защиты можно представить в виде маршрута на орграфе $G_0(V_0, E_0)$, заданного как последовательность вершин и ребер: $p_k = \left\{ v_{0,1}, e_{0,(1,2)}, v_{0,2}, \dots e_{0,(n-1,n)}, v_{0,n} \right\}$.

Описан процесс построения частных моделей промышленной КФС для создания целостной модели объекта защиты, на основе базовой модели по требованию задач безопасности с использованием связанных графов. Каждая структурная, функциональная или иная иерархия, описывающая объект защиты

в соответствии с принципом иерархической связности, определяется как дерево T_I, узлы которого представляют собой агрегации подграфов нижележащего уровня модели объекта с заданными функциями обобщения, а ребра отражают наследственные (PCr - Public Child relation) отношения между узлами. Каждый уровень такого дерева представляет собой граф вида $G_L(V_L, E_L)$, где L – это уровень соответствующего дерева. В свою очередь каждый узел также может быть описан подграфом $G_i(V_i, E_i)$, представляющим обобщенный фрагмент нижележащего графа, где $i \in [0, I]$, а I – число узлов соответствующего уровня. Установлено соответствие систем концептуального представления УРСЗ и элементов модели на основе данных.

Приведен пример построения модели КФС для решения задачи обеспечения ее устойчивости. Порождающие элементы выше лежащего графа задаются как связь $\overset{PCr}{\longrightarrow}$ родитель – потомок от вышележащей (более общей) вершины к нижележащей: $v_v \overset{F^V_{0,v}}{\longrightarrow} v_0$, а между ребрами как $e_v \overset{F^E_{0,v}}{\longrightarrow} e_0$ для первого уровня и $v_{v,i} \overset{F^V_{0,v}}{\longrightarrow} v_{i-1}$, $e_{v,i} \overset{F^E_{0,v}}{\longrightarrow} e_{i-1}$ для -го уровня (рисунок 2). G_0 представляет собой граф базовой модели, а вышележащие графы – уровни функциональной декомпозиции целевого процесса КФС от более детализированного G_v к менее детализированному G_{v1} в соответствии методом решения задачи.

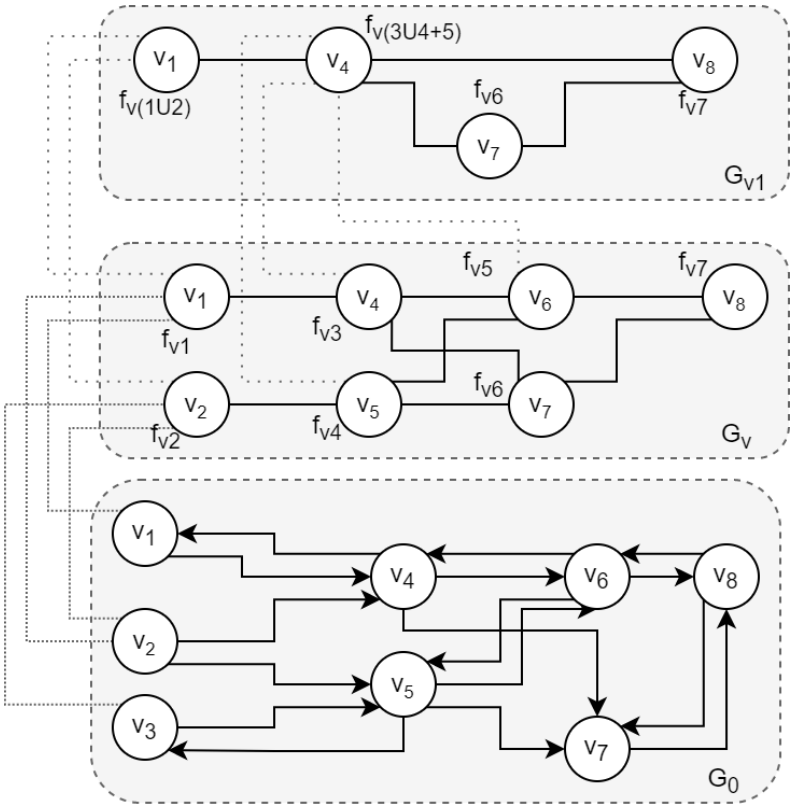

Рисунок 2 – Схема, представляющая модель промышленной КФС на основе связанных графов для решения задачи обеспечения устойчивости

Исходя из адекватности методов моделирования на основе данных и адекватности метамодели, показана полнота и достоверность модели на основе данных. Сформулировано *условие полноты* представления объекта защиты в метамодели: для каждой из гипотез $h_k \in H$, где H – все множество гипотез, используемых методами решения задач безопасности, должна существовать соответствующая порождающая модель $mp_j \in MP$, где MP – множество порождающих моделей АМИБ ПКФС на данный момент. Приведен фрагмент схемы работы АМИБ в части, относящейся к управлению моделью объекта защиты.

В четвертой главе описаны методы и модели обработки данных и управления гетерогенными данными в системе АМИБ ПКФС. Проведена формализация структур данных в системе АМИБ, выделены группы методов решения задач безопасности и по отношению к каждой группе определены требования, модель применения и входные данные.

Сформулирована задача подсистемы предварительной обработки данных как подготовка структурированных данных для методов решения задач безопасности. Формализована задача поиска схемы обработки данных на основе графа обработки $G = (V, E)$. Вершины графа ассоциированы с экземплярами методов обработки данных $V = \{m_l | m_l \in M_i\}$ и задаются отображением $V \to M_i$, ребра представляют собой пути передачи фрагментов данных, формирующие маршрут преобразований. Каждое ребро ассоциировано с некоторым фрагментом данных $E = \{d_j | d_j \in D^{IN} \cup d_j \in D^{OUT} \cup d_j \in m_l(D_L)\}$, где D^{IN} – входные наборы данных, D^{OUT} – выходные, $m_l \in M_i$ – метод обработки, D_L – фрагменты данных преобразуемые методом m_l. Выбор инструментов реализации происходит на основе отображения $G^{\Sigma} \to Instr$. Для этого общий граф $G^{\Sigma} = (V, E)$ разбивается на набор подграфов, ассоциированных с инструментами: $G^{\Sigma} = \bigcup_{k=1}^{|In_i|} G_k$ где выполняется условие: $\forall(v_h \in G_k | k \in [1, |In_i|]) \; \exists\left[\left(v_g \in G | v_g = v_h\right) \wedge \nexists\left(v_r \in G | (v_r = v_h \wedge r \neq g)\right)\right]$ и установлено соответствие между граничными вершинами $Vout_{k-1} \to Vin_k$. На основе маршрута на графе обработки определяется значение времени подготовки каждого фрагмента данных. *Условия реализуемости* обработки данных с требуемыми параметрами формализуются следующим образом:

1. $\exists(G^{\Sigma} \rightarrow Instr)$ – общий граф обработки может быть реализован на базе существующего множества инструментов.

2. $\forall\left(t_j.d_h \in t_j.D_L | t_j \in Tasks_i\right)$ – для каждого фрагмента входных данных каждой задачи (метода решения задач безопасности) существует соответствующий выходной фрагмент данных в графе обработки $\exists\left(v_{res} \in G^{\Sigma}.V, e_{res} \in G^{\Sigma}.E | e_{res} \rightarrow v_{res} \wedge t_j.d_h = e_{res}.d_j\right)$.

3. $\forall(Vout_k \in Vres_i)\left[Tr_k^{\Sigma} < Tr_k^{MAX}\right]$ – общее время обработки данных на k-м маршруте не превышает заданного граничного значения, определяемого на уровне схемы мониторинга при решении задач безопасности.

Сформулированы особенности предварительной обработки данных в системах АМИБ ПКФС: гетерогенность данных и их источников; ограничения на ресурсы; потери данных при передаче. Выделены факторы, позволяющие сократить время предварительной обработки данных: исключение длительных операций над данными; сокращение числа операций над данными; сокращение объема данных в памяти.

Представлены методы агрегации потоковых данных в системе АМИБ, ориентированные потоковую обработку информации и использующие свойство самоподобия данных, выраженное в требовании со стороны методов решения задач как запрос входных временных рядов одних и тех же параметров с различным периодом агрегации. Агрегация одиночных параметров проводится с введением над временными рядами отношения порядка и формирование связи родитель – потомок по данным (рисунок 3).

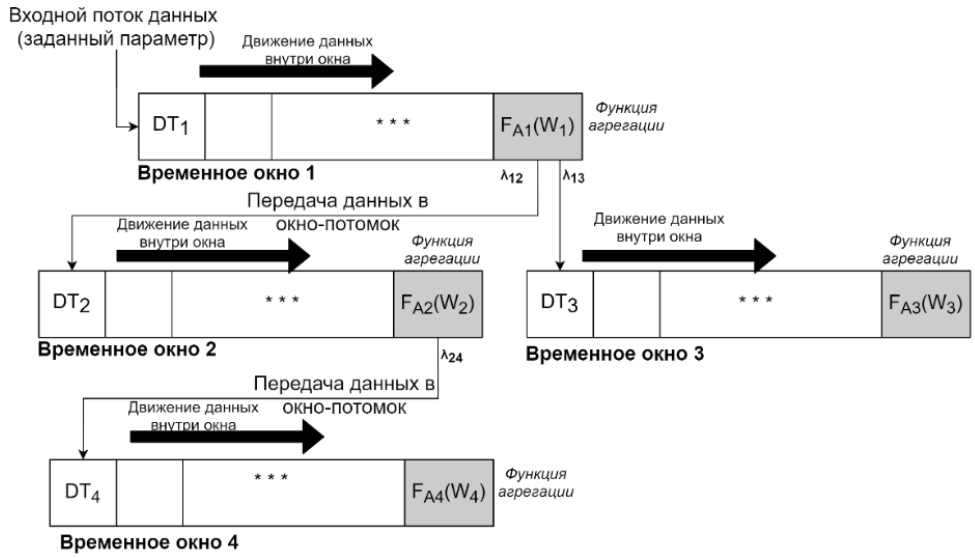

Рисунок 3 – Иерархия временных окон анализа на основе временных рядов

Многомерная совместная агрегация нескольких параметров основывается на построении графа связей одиночных иерархий временных рядов, задающего ассоциации между параметрами и позволяющего реализовать быстрый поиск и выбор групп данных для совместного анализа. Приведены основные этапы работы каждого метода агрегации и детали операций переноса данных в рамках иерархий временных окон (временных рядов). Предложенные методы позволяют сократить объем данных в памяти и ускорить агрегацию данных в МИБ за счет потоковых технологий обработки данных.

Рассмотрен вопрос хранения данных мониторинга: выделены четыре вида данных разной степени структуризации с разными требованиями к системе хранения. Аргументировано применение соответствующих типов хранилищ данных и определен порядок миграции данных между хранилищами.

Приведен метод интеллектуального анализа гетерогенных данных, обусловленный расширением задач безопасности МИБ. Рассматривается задача сравнительного анализа объектов и систем в условиях семантической и синтаксической неоднородности (гетерогенности) описывающих их данных, слабой степени структуризации, неполноты данных и описаний. Представление информации формализуется на основе подхода «bag of objects», где каждый элемент определяется как некоторый объект $o_i \in O$, характеризующийся множеством заранее неопределенных свойств. Каждый объект определяется его свойствами $\forall(o_i \in O)|(o_i = \{c|c_i = Val \vee c_i = RefO \vee c_i = Unknown\})$. Каждое свойство может иметь установленное значение (Val), являться ссылкой на другой объект ($RefO$) или его значение может быть неизвестно ($Unknown$). Аналогично система представляется как множество объектов. Для сравнения объектов o_i, o_j, представленных множествами свойств C_i и C_j, используется обобщенный вектор их свойств $\overline{C_{i,j}}$ полученный объединением свойств и заданием отношения порядка:

$$\left.\begin{matrix} o_i \to C_i = \{c_i^1, \dots, c_i^k\} \\ o_j \to C_j = \{c_j^1, \dots, c_j^n\} \end{matrix}\right\} \to C_{i,j} = C_i \cup C_j \to \overline{C_{i,j}} \quad (3)$$

Предлагается метрика схожести объектов как среднее между схожестью всех свойств с известными для обоих объектов значениями с учетом схожести наборов свойств:

$$S = \frac{\alpha * s^1 + \beta * s^2}{2} \in [0,1], \quad (4)$$

где $s^1 = dist(\overline{C_{i,j}}, \overline{C_{j,i}}) \in [0,1]$ – схожесть наборов свойств как расстояние между векторами (3), $s^2 = \frac{\sum_{k=1}^{N} s_k^2}{N} \in [0,1]$ – схожесть объектов по значениям

свойств, $s_k^2 = dist(c_{i,k}.Value, c_{j,k}.Value) \in [0,1]$ – расстояние между значениями свойства c_k объектов o_i , o_j , а N – общее число свойств с определенными значениями. Коэффициенты $\alpha > 0$ и $\beta > 0$ связаны ограничением $\alpha + \beta = 1$ и являются настраиваемыми параметрами весов между наличием и значением свойств.

Рассмотрена оценка схожести систем, представленных объектами, на основе прецедентного анализа, с точки зрения поиска максимально уязвимого элемента (объекта) и поиска схожих сценариев в базе знаний прецедентов. В первом случае мера схожести между прецедентами P_i и P_j задается на основе формулы (4) как максимальная схожесть их объектов:

$$Sim_{P_i,P_j}^{one} = \max_{k,l}(s(o_k, o_l)),$$

(5)

где $o_k \in P_i, o_l \in P_j, k \in [1, |P_i|], l \in \left[1, \left|P_j\right|\right]$. Во втором предлагается использовать среднюю меру схожести объектов в этих системах:

$$Sim_{P_i,P_j}^{all} = \frac{\sum_{k=1}^{K} s_k}{K}, \quad (6)$$

где -число оцениваемых объектов во входном наборе.

Представлена оценка значимости свойств для поддержания актуальности базы знаний и их фильтрации при снижении размерности расчетов.

Представлен метод управления Большими данными в системе мониторинга информационной безопасности на основе двухэтапной предварительной обработки данных и трех типов хранилищ информации отличающийся интеграцией гетерогенных Больших и Быстрых данных при обработке и хранении для обеспечения оперативности АМИБ (рисунок 4).

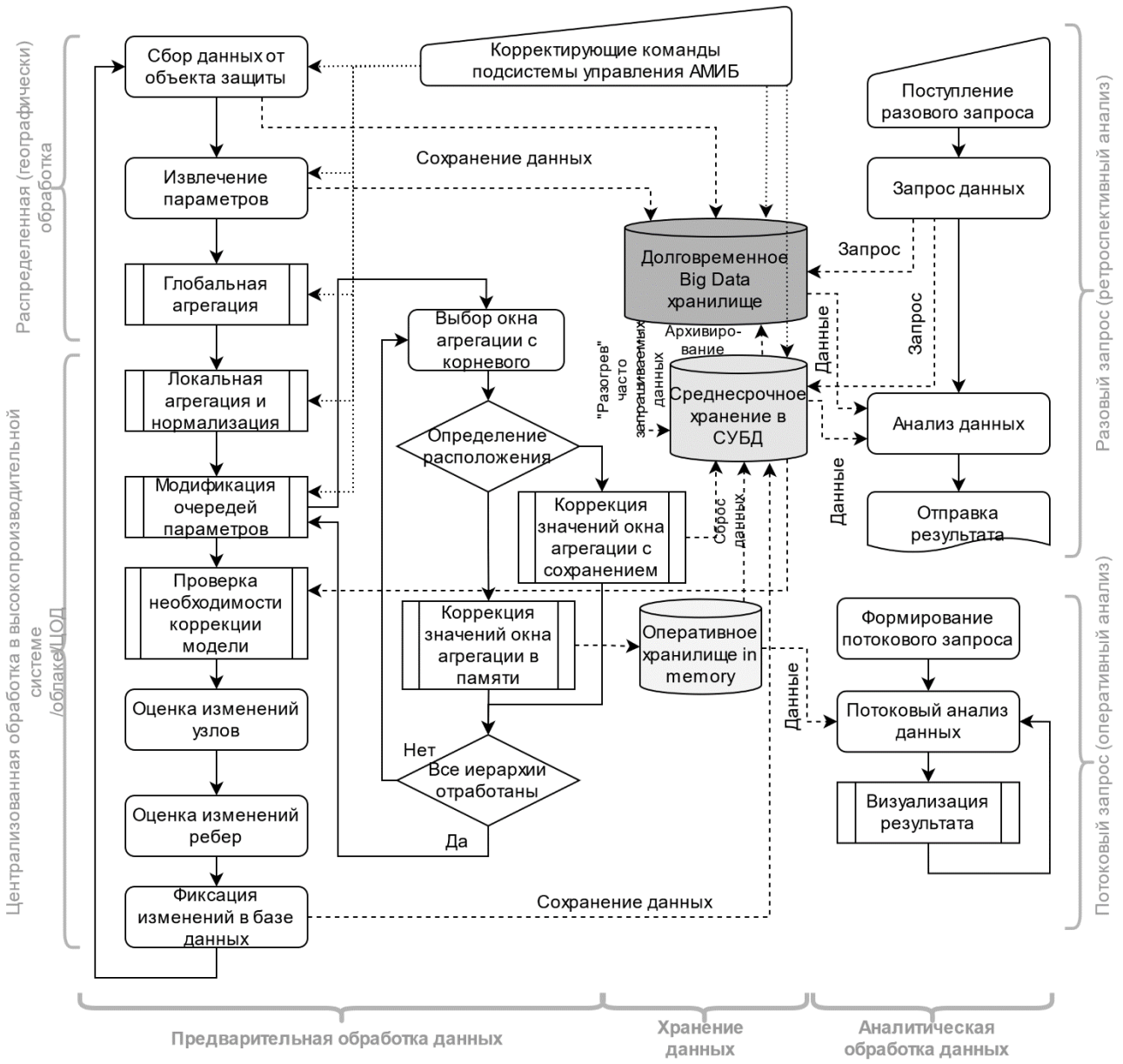

Рисунок 4 – Схема метода управления Большими данными в АМИБ

В пятой главе представлен макет системы АМИБ ПКФС, включающий структуру системы мониторинга, спроектированную с учетом реализации принципов целостности, конвергентности и иерархической связности системологического подхода. Определены основные архитектурные уровни АМИБ: уровень управления данными; уровень анализа и принятия решений; уровень адаптивного управления. Представлена структурная схема системы АМИБ (рисунок 5).

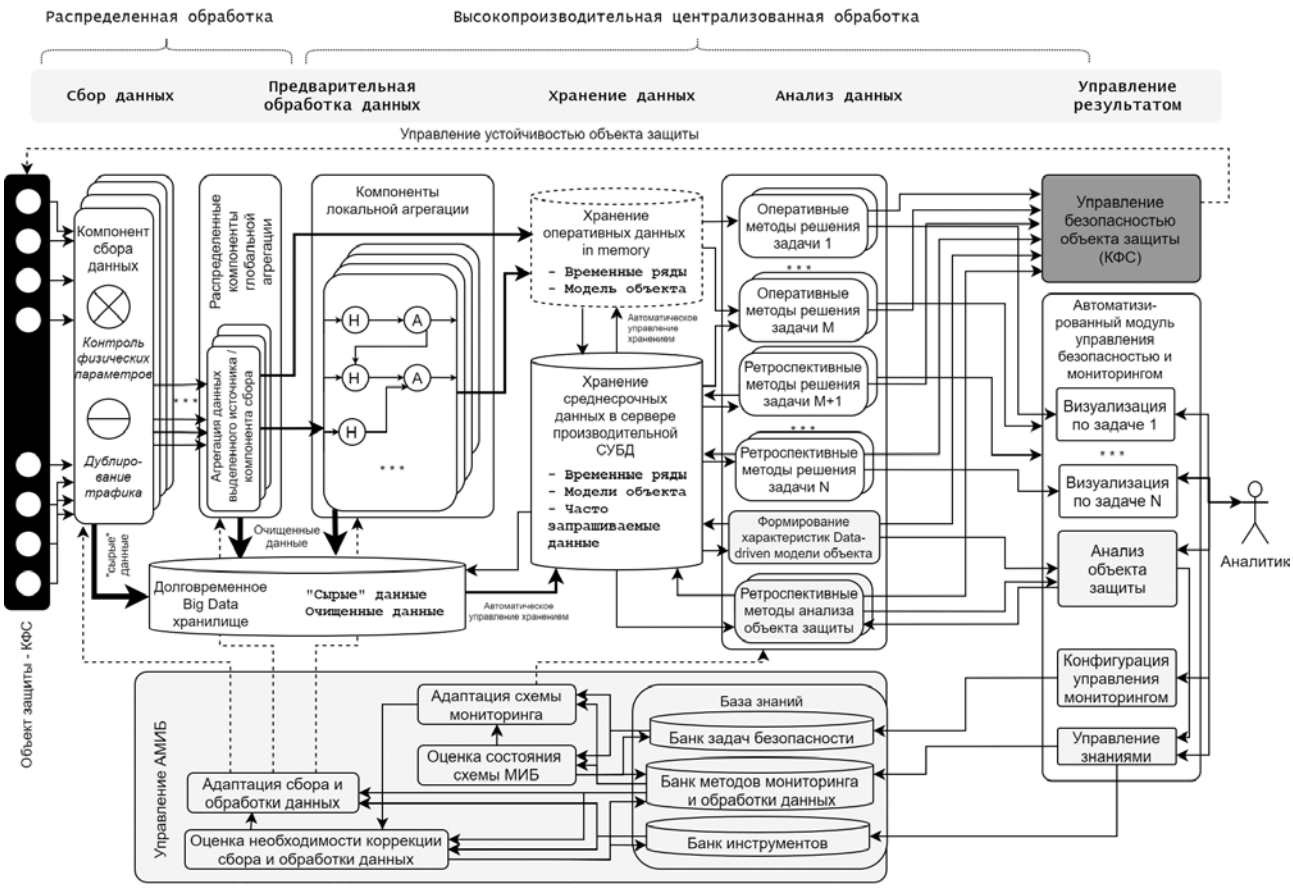

Рисунок 5 – Структурная схема системы адаптивного мониторинга информационной безопасности промышленных КФС

Предлагаемый подход к практической реализации системы ориентирован на высоко производительные, масштабируемые, отказоустойчивые технологические платформы, примером которых (для более узкого круга задач) служит платформа Crossbeam.

Представлены результаты экспериментального применения метода интеллектуального управления АМИБ в рамках задачи поиска аномалий в сетевом трафике КФС, на основе сформированного банка методов. Применялись граничные условия скорости работы, точности, требуемого числа вычислительных узлов и многопоточных вычислений. Приведен пример фильтрации методов по граничным условиям скорости (рисунок 6) и точности по метрике $Accuracy$ (рисунок 7). Показан пример поиска единственного решения в условиях Парето-оптимальности вариантов схем.

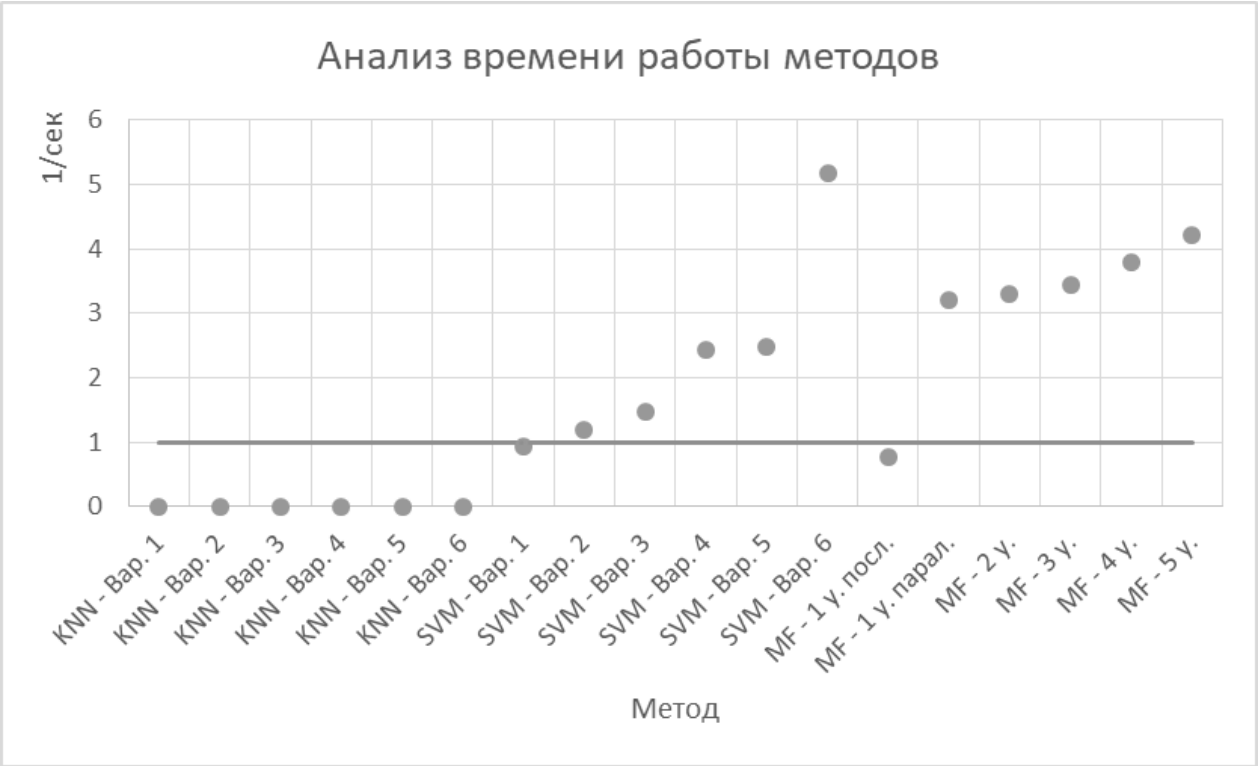

Рисунок 6 – Оценка граничного условия по времени работы методов

Рисунок 7 – Оценка граничного условия по точности работы ($Accuracy$)

Приведен пример оценки характеристик мониторинга в терминах наблюдаемости и идентифицируемости для мониторинга на базе графовой модели атаки.

Представлены результаты экспериментальной оценки методов агрегации потоковых данных на основе двух различных наборов данных ПКФС. Проведено сравнение метода иерархической агрегации с методом агрегации по наименьшему периоду, использующим формирование более высоко-агрегированных данных «по требованию». Разница в объеме подготовленных данных в памяти возникает при более чем двух связанных окнах, для трех окон составляет 25%, а для 10 – уже 98%. Сравнение объема подготовленных данных с отдельной агрегацией рядов без иерархической связи также показывает преимущество разработанного метода, возрастающее по мере роста числа временных рядов (окон) в одной иерархии (рисунок 8).

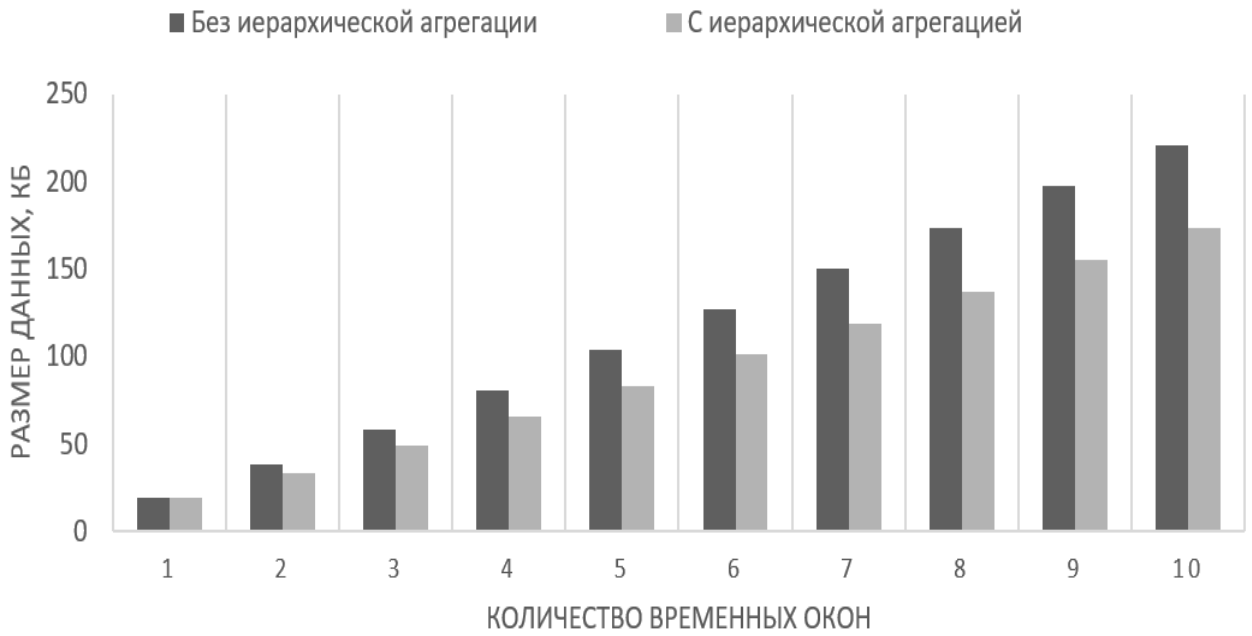

Рисунок 8 – Сравнение иерархической агрегации и аналога с отдельным ведением временных окон (рядов)

Представлены результаты экспериментальных исследований, показывающие ограничения метода многомерной агрегации. Показано, что при числе пар агрегируемых параметров больше пяти или глубине вложенности агрегации больше шести узлы графа объединяются в связанную компоненту, и эффективность извлечения пар параметров ухудшается. Отмечается, что методы анализа данных МИБ КФС оперируют, как правило, двумя-тремя значениями агрегируемых параметров и для данного типа систем указанное ограничение не является критическим. Показано, что размер временного окна существенно не влияет на производительность операций.

Проведено сравнение работы предложенного метода многомерной агрегации с обычной многомерной агрегацией, как по времени работы (рисунок

9), так и по объему данных в памяти. Показано, что предлагаемый метод дает преимущество в скорости работы, значимое при совместном анализе более чем двух параметров и составляющее от 50% (при 20 уникальных значениях) до 60% при максимально оцененном разнообразии в 50 индивидуальных параметров. Также показано, что в данном случае применение специализированного метода приводит к росту объёма данных в памяти на 30-40%, что ограничивает его применение на мало-ресурсных узлах, но не существенно для более производительных узлов анализа, так как абсолютные значения объемов данных для 12 совместно анализируемых параметров составляют порядка 27 мегабайт.

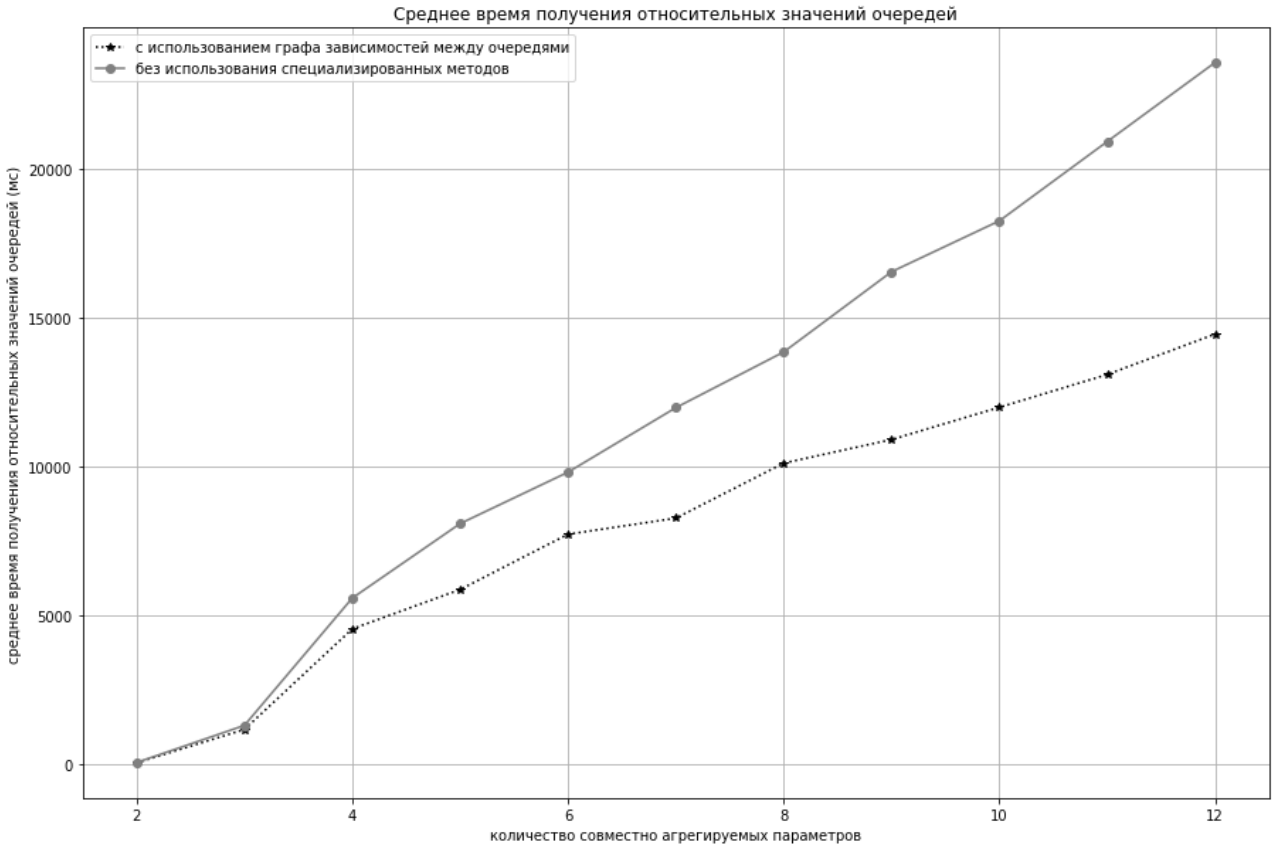

Рисунок 9 – Среднее время извлечения данных (20 параметров)

Приведены схемы хранения данных для всех типов данных и хранилищ АМИБ ПКФС, рассмотрена задача оптимального хранения графовых структур применяемых в современных методах МИБ и заложенных в модели на основе данных. Представлена модификация схемы хранения графов для повышения эффективности решения задач мониторинга. В схему хранения вводится дополнительный признак конечных (только входных или выходных) узлов, позволяющий существенно повысить скорость ряда операций над графом.

Представлена экспериментальная оценка метода интеллектуального анализа гетерогенных данных на примере поддержки принятия решений при тестировании на проникновение. Показано, что предложенные метрики позволяют эффективно определять значимые свойства объектов, находить схожие объекты и прецеденты. Приведены результаты экспериментального тестирования поиска подобных прецедентов (систем). Представлен верх ранжированного списка объектов прецедентов из базы знаний наиболее сходных с входным тестовым набором (с явным указанием типа для читаемости таблицы) и оценки их схожести с объектами входного набора (таблица 1).

Таблица 1. Ранжированные результаты оценки схожести прецедентов с входным набором

Номер прецедента	Тип объекта в базе знаний	Тип объекта в прецеденте	S (4)	$Sim^{one}_{P_i,P_j}$ (5)	$Sim^{all}_{P_i,P_j}$ (6)
P5	IP	IP	1,00	1,00	0,33
P0	PC	PC	0,85	0,93	0,86
	PC	PC	0,85		
	Application	Application	0,93		
	***	***	***		
P2	PC	PC	0,75	0,93	0,57
	PC	PC	0,75		
	Application	Application	0,93		
	***	***	***		
P1	PC	PC	0,75	0,85	0,78
	PC	PC	0,75		
	Network	Network	0,85		

Показано, что изменение значимости свойств на основе небольшого (до 10) числа прецедентов в сторону как уменьшения, так и увеличения значимости позволяет обеспечить актуальность базы знаний прецедентов в изменяющихся внешних условиях.

В заключении приведены основные результаты, полученные автором в ходе выполнения работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате диссертационного исследования предложен системологический подход и методология адаптивного управления мониторингом информационной безопасности промышленных КФС, позволяющие выбрать оптимальную схему мониторинга на основе множеств задач безопасности, методов их решения и групп данных объекта защиты, за счет чего - обеспечить полноту, достоверность и оперативность информирования об инцидентах безопасности КФС в условиях эволюционных изменений объекта защиты и среды его функционирования.

Получены следующие результаты:

1. Проведен анализ систем мониторинга информационной безопасности, сформулирована роль МИБ как непрерывного процесса, обеспечивающего необходимый набор данных для работы системы управления безопасностью. Выделена специфика современных КФС как объекта защиты и проведена систематизация задач МИБ и методов их решения. Выполнена постановка задачи АМИБ ПКФС и сформулированы требования адаптивности, полноты, достоверности и оперативности.

2. Разработаны принципы целостности, конвергенции и иерархической связности системологического подхода к АМИБ ПКФС. На основе принципа целостности разработана высокоуровневая модель адаптивного мониторинга, отражающая взаимосвязь функций МИБ и этапов управления информационной безопасностью КФС.

3. Разработана методология управления АМИБ на основе отображения множеств задач безопасности, методов их решения и данных объекта защиты, в том числе:

- построен набор отображений множеств задач безопасности, методов их решения и данных объекта защиты, реализующий принцип конвергенции, определены условия достаточности и не избыточности отображения;

- разработан метод интеллектуального управления АМИБ на основе теории оптимального выбора, реализующий принципы целостности и конвергенции и позволяющий найти оптимальную схему мониторинга;

- разработан подход к оценке параметров мониторинга ПКФС, выражающий характеристики полноты, достоверности и оперативности мониторинга через характеристики наблюдаемости и идентифицируемости технических систем.

4. Разработана модель объекта защиты, адаптивная к различным способам структурной и функциональной организации объекта за счет

использования концепции УРСЗ и подхода на основе данных (Data-driven), включая:

- метамодель промышленной КФС на основе концепции УРСЗ, соответствующую принципам целостности и иерархической связности и отражающую связь задач безопасности, методов их решения и элементов модели объекта защиты на основе данных;

- модель КФС на основе данных (Data-driven) с использованием связанных графов, реализующую принципы целостности, конвергенции и иерархической связности.

5. Разработан набор методов обработки и управления Большими данными в системе мониторинга безопасности КФС, в том числе:

- проведена формализация структур данных в задачах АМИБ ПКФС, выявлены основные структуры входных данных, востребованные для анализа;

- разработана схема двухэтапной предварительной обработки Больших данных мониторинга информационной безопасности, методы одномерной и многомерной агрегации потоковых данных, позволяющие снизить время обработки информации в КФС, и метод интеллектуального анализа гетерогенных данных на основе паттернов, с актуализацией базы знаний по мере накопления прецедентов;

- разработан метод управления Большими данными при АМИБ ПКФС, включающий: поддержку анализа Больших данных путем реализации двух моделей запроса; схему предварительной обработки Больших данных; схему хранения данных с автоматической миграцией и взаимным отображением структур данных между хранилищами.

6. Разработан макет системы АМИБ, включающий структуру системы мониторинга на основе принципов целостности, конвергенции и иерархической связности. Проведено практическое исследование, в котором показана применимость метода интеллектуального управления АМИБ и подхода к оценке характеристик КФС, а также приведены оценки эффективности предложенных методов агрегации и анализа данных.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ:

В рецензируемых журналах из перечня ВАК:

1. Зегжда П.Д. Моделирование информационных систем для решения задачи управления безопасностью / П.Д. Зегжда, Д.П. Зегжда, А.И. Печенкин, **М.А. Полтавцева** // Проблемы информационной безопасности. Компьютерные системы. - 2016. - № 3. - С. 7-16.

2. **Полтавцева, М.А.** Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение / М.А. Полтавцева, А.И. Печенкин // Проблемы информационной безопасности. Компьютерные системы. - 2017. - № 3. - С. 62-69.

3. Зегжда, Д.П. Систематизация киберфизических систем и оценка их безопасности / Д.П. Зегжда, **М.А. Полтавцева,** Д.С. Лаврова// Проблемы инфор-мационной безопасности. Компьютерные системы. - 2017. - № 2. - С.127-138.

4. Зегжда, Д.П. Подходы к моделированию безопасности киберфизических систем/ Д.П. Зегжда, Ю.С. Васильев, **М.А. Полтавцева** // Проблемы информационной безопасности. Компьютерные системы. - 2017. - № 3. - С.30-43.

5. Васильев, Ю.С. Проблемы безопасности цифрового производства и его устойчивость к киберугрозам / Ю.С. Васильев, Д.П. Зегжда, **М.А. Полтавцева** // Проблемы информационной безопасности. Компьютерные системы. - 2017. - № 4. - С. 47-63.

6. **Полтавцева, М.А.** Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя/ М.А. Полтавцева, С.И. Штеренберг // Проблемы информационной безопасности. Компьютерные системы. - 2018. - № 2. - С. 59-68.

7. Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю.С. Васильев, **М.А. Полтавцева**, И.Ф. Кефели, А.И. Боровков // Вопросы кибербезопасности. - 2018. - № 2. - С. 2-15.

8. **Полтавцева, М.А.** Метод автоматизированного обучения системы поддержки принятия решений для анализа защищенности автоматизированных систем / М.А. Полтавцева, Е.А. Зайцева // Проблемы информационной безопасности. Компьютерные системы. - 2018. - № 4. - С. 22-32.

9. Зегжда, П. Д. Прецедентный анализ гетерогенных слабо структурированных объектов в задачах информационной безопасности/ П. Д. Зегжда, **М.А. Полтавцева,** А.И. Печенкин, Д.С. Лаврова, Е.А. Зайцева //

Проблемы информационной безопасности. Компьютерные системы. - 2018. - № 1. - С. 17-31.

10. Зайцева, Е.А. Использование графового представления и прецедентного анализа для оценки защищенности компьютерных систем / Е.А. Зайцева, Д.П. Зегжда, **М.А. Полтавцева** // Проблемы информационной безопасности. Компьютерные системы. - 2019. - № 2. - С. 136-148.

11. **Полтавцева, М.А.** Построение адаптивной системы сбора и подготовки данных при мониторинге безопасности / М.А. Полтавцева, Д.П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 2. - С. 92-101.

12. **Полтавцева, М.А.** Характеристики мониторинга безопасности киберфизических систем / М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 1. - С. 73 -88.

13. **Полтавцева, М.А.** Моделирование промышленных киберфизических систем на основе данных / М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 4. - С. 95-106.

14. **Полтавцева, М.А.** Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем / М.А. Полтавцева // Вопросы кибербезопасности. - 2021. - № 2. - С. 51-60.

15. **Полтавцева, М.А.** Системологический подход к адаптивному мониторингу информационной безопасности КФС / М.А. Полтавцева // Защита информации. Инсайд. - 2021. - № 2. - С. 77-83.

16. **Полтавцева, М.А.** Формирование структур данных в задачах активного мониторинга безопасности / М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. - 2021. - № 1. - С. 9-19.

17. **Poltavtseva, M.A.** Heterogeneous Data Aggregation and Normalization in Information Security Monitoring and Intrusion Detection Systems of Large-scale Industrial CPS / M.A. Poltavtseva // Proceedings of the Institute for System Programming of the RAS. - 2020. - Т. 32. - № 5. - С. 131-142.

18. **Полтавцева, М.А.** Управление адаптивным мониторингом информационной безопасности КФС / М.А. Полтавцева // Защита информации. Инсайд. - 2021. - № 3. - С. 2-8.

В изданиях, индексируемых Scopus и/или Web of Science:

19. **Poltavtseva, M.A.** Planning of aggregation and normalization of data from the Internet of Things for processing on a multiprocessor cluster / M.A. Poltavtseva, D.S. Lavrova, A.I. Pechenkin // Automatic Control and Computer Sciences. - 2016. - Vol. 50. - Issue №8. - P. 703–711.

20. **Poltavtseva, M.A.** Intelligent data analysis in decision support systems for penetration tests / **M.A. Poltavtseva**, A.I. Pechenkin // Automatic Control and Computer Sciences. - 2017. - Vol. 51. - Issue №8. - P. 985–991.

21. Zegzhda, D.P. Systematization and security assessment of cyber-physical systems / D.P. Zegzhda, **M.A. Poltavtseva**, D.S. Lavrova // Automatic Control and Computer Sciences. - 2017. - Vol. 51. - Issue №8. - P. 835–843.

22. Zegzhda, D.P. Modeling of information systems to their security evaluation / D.P. Zegzhda, P.D. Zegzhda, A.I. Pechenkin, **M.A. Poltavtseva** // Proceedings of the 10th International Conference on Security of Information and Networks (SIN '17). - New York. - Association for Computing Machinery. - 2017. - P. 295-298.

23. Zegzhda, P.D. A use case analysis of heterogeneous semistructured objects in information security problems / P.D. Zegzhda, **M.A. Poltavtseva**, A.I. Pechenkin, D.S. Lavrova, E.A. Zaitseva // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 918–930.

24. Lavrova, D. Detection of cyber threats to network infrastructure of digital production based on the methods of Big Data and multifractal analysis of traffic / D. Lavrova, **M. Poltavtseva**, A. Shtyrkina, P. Zegzhda // International Scientific Conference “The Convergence of Digital and Physical Worlds: Technological, Economic and Social Challenges” (CC-TESC2018). – 2018. – 00051.

25. Zegzhda, D.P. Approaches to Modeling the Security of Cyberphysical Systems / Yu. S. Vasil’ev, D.P. Zegzhda, **M.A. Poltavtseva** // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 1000–1009.

26. Lavrova, D. Security analysis of cyber-physical systems network infrastructure / D. Lavrova, **M. Poltavtseva**, A. Shtyrkina // Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS 2018. – 2018. – P. 818–823.

27. Vasil’ev, E Yu. S. Problems of Security in Digital Production and Its Resistance to Cyber Threats /Yu.S. Vasil’ev, D.P. Zegzhda, **M.A. Poltavtseva** // Auto-matic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. – P. 1090–1100.

28. **Poltavtseva, M.A.** The Hierarchial Data Aggregation Method in Backbone Traffic Streaming Analyzing to Ensure Digital Systems Information Security / M.A. Poltavtseva, P.D. Zegzhda, I.D. Pankov // 2018 Eleventh

International Conference "Management of large-scale system development". – 2018. - P. 1-5.

29. **Poltavtseva, M.A.** A Distributed Intrusion Detection System with Protection from an Internal Intruder / M.A. Poltavtseva, S. I. Shterenberg // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 945–953.

30. **Poltavtseva, M.A.** High-performance NIDS Architecture for Enterprise Networking / M.A. Poltavtseva, D.P. Zegzhda, E. Y. Pavlenko // 2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom. - 2019. – Vol. 7. - P. 808-812.

31. Zaitseva E.A., Use of Graph Representation and Case Analysis to Assess the Security of Computer Systems / E.A. Zaitseva, D.P. Zegzhda, **M.A. Poltavtseva** // Automatic Control and Computer Sciences. - 2019. - Vol. 53. - Issue №8. - P. 937–947.

32. **Poltavtseva, M.A** Heterogeneous Semi-structured Objects Analysis. / M.A Poltavtseva, P. Zegzhda // Eds.: Arai K., Kapoor S., Bhatia R. - Advances in Intel-ligent Systems and Computing. - Springer, Cham. – 2019. - Vol. 868. - P.1259-1270.

33. Zegzhda, D. Multifractal security analysis of cyberphysical systems / D. Zegzhda, D. Lavrova, **M. A. Poltavtseva** // Nonlinear Phenomena in Complex Systems. – 2019. – Vol. 22. – Issue №8. – P. 196–204.

34. **Poltavtseva, M.A** Automation of open sources data processing for the security assessment / M.A Poltavtseva, D.A. Bazarnova // Proceedings - 2019 Ivannikov Memorial Workshop, IVMEM 2019. - 2019. - P. 64-67.

35. Pavlenko, E. Y. Ensuring the sustainability of cyberphysical systems based on dynamic reconfiguration / E. Y. Pavlenko., D.P. Zegzhda, **M. A. Poltavtseva** // Proceedings - 2019 IEEE International Conference on Industrial Cyber Physical Systems, ICPS 2019. – 2019. - P. 785-789.

36. **Poltavtseva, M.A** Conceptual Data Modeling Using Aggregates to Ensure Large-Scale Distributed Data Management Systems Security / M.A Poltavtseva, M.O. Kalinin // Studies in Computational Intelligence. - 2020. - Vol. 868. - P. 41-47.

37. Fatin, A. D. A Survey of Mathematical Methods for Security Analysis of Cyberphysical Systems / A. D. Fatin, E. Yu. Pavlenko, **M. A. Poltavtseva** // Automatic Control and Computer Sciences. - 2020. - Vol. 54. - P. 983–987.

38. **Poltavtseva, M.A** Building an Adaptive System for Collecting and Preparing Data for Security Monitoring / M.A Poltavtseva, D.P. Zegzhda // Automatic Control and Computer Sciences. - 2020. - Vol. 54. - P. 968–976.

39. **Poltavtseva, M.A** Multi-Dimensional Data Aggregation in the Analysis of Self-Similar Processes / M. A. Poltavtseva, T. A. Andreeva.// Nonlinear Phenomena in Complex Systems. – 2020. – Vol. 23. – Issue №3. – P. 262–269.

40. **Poltavtseva M. A.** Heterogeneous Semi-Structured Data Analysis in Information Security / M. A. Poltavtseva, P. V. Semyanov, E. A. Zaitzeva // 2020 International Conference Engineering and Telecommunication (En&T). – 2020. - P. 1-5, doi: 10.1109/EnT50437.2020.9431309.

41. Pavlenko, E.Yu. Mathematical methods for implementing homeostatic control in digital production systems / E.Yu. Pavlenko, **M. A. Poltavtseva** // Lecture Notes in Networks and Systems. - 2021. – Vol. 157. - P. 1-9.

В монографиях и разделах в монографиях:

42. **Полтавцева М.А.,** Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин и др.; Под ред. доктора технических наук, профессора Д. П. Зегжды. – М.: Горячая линия – Телеком, 2019. – 640 с.: ил. ISBN 978-5-9912-0826-0.

43. **Полтавцева, М.А.** Адаптивный мониторинг промышленных киберфизических систем / М.А. Полтавцева.; Под ред. доктора технических наук, профессора Д. П. Зегжды. – СПб.: ПОЛИТЕХ-ПРЕСС, 2021. – 166 с. ISBN 978-5-7422-7345-5

В свидетельствах о регистрации программы для ЭВМ:

44. Программа для ЭВМ 2020663668 Российская Федерация. Программа для иерархической агрегации данных в системе мониторинга безопасности [Текст] / М. А. Полтавцева, Т. М. Андреева. // свидетельство о государственной регистрации программы для ЭВМ: - № 2020663668 : заявл. 05.11.2020 : опубл. 16.11.2020.

45. Программа для ЭВМ 2020664631 Российская Федерация. Программа для многомерной агрегации данных в системе мониторинга безопасности [Текст] / М. А. Полтавцева, Т. М. Андреева. // свидетельство о государственной регистрации программы для ЭВМ: - № 2020664631 : заявл. 09.11.2020 : опубл. 16.11.2020.

В патентах РФ на изобретения:

46. Пат. 2643620 Российская Федерация. Способ планирования задач предобработки данных Интернета Вещей для систем анализа [Текст] / Зегжда П.Д., Лаврова Д.С., Печенкин А.И., **Полтавцева М.А.**; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2016118326 заявл. 11.05.2016 ; опубл. 16.11.2017, Бюл. № 4 – 2 с.

В изданиях, индексируемых РИНЦ:

47. Лаврова, Д.С. Siem-система для обнаружения и анализа инцидентов безопасности в интернете вещей/ Д.С. Лаврова, **М.А. Полтавцева**, А.И. Печенкин, Д.П. Зегжда // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 35-36.

48. Печенкин А.И. An approach to data normalization in the internet of things for security analysis / А.И. Печенкин, **М.А. Полтавцева**, Д.С. Лаврова // Программные продукты и системы. - 2016. - № 2. - С. 83-88.

49. Печенкин А.И. Функционально-семантическое моделирование информационных систем для решения задач безопасности/ А.И. Печенкин, **М.А. Полтавцева**, П.Д. Зегжда, Д.П. Зегжда // Методы и технические средства обеспечения безопасности информации. - 2016. - № 25. - С. 108.

50. **Полтавцева, М.А.** Поддержка механизма вывода систем разграничения доступа на базе онтологий в реляционном сервере / М.А. Полтавцева // Методы и технические средства обеспечения безопасности информации. - 2016. - № 25. - С. 109-111.

51. **Полтавцева, М.А.** Классификация методов представления иерархий в РСУБД / М.А. Полтавцева, А.А. Полтавцев // Программные продукты, системы и алгоритмы. - 2016. - № 1. - С. 1-6.

52. **Полтавцева, М.А.** Построение защищенных систем управления большими данными крупномасштабных объектов / М.А. Полтавцева //Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 19-21.

53. **Полтавцева, М.А.** Параллельное выполнение нормализации и агрегации первичных данных интернета вещей / М.А. Полтавцева // 21 век: фундаментальная наука и технологии. Материалы VIII международной научно-практической конференции. н.-и. ц. «Академический». - 2016. - С. 106-109.

54. **Полтавцева, М.А.** Формирование экземпляров онтологических классов при обработке неструктурированных данных в решении задач

информационной безопасности / М.А. Полтавцева, А.И. Печенкин // В сборнике: Региональная информатика и информационная безопасность. сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. - 2017. - С. 60-64.

55. **Полтавцева, М.А.** Сокращение размерности данных и поиск уязвимых объектов методами интеллектуального анализа при тестировании на проникновение / М.А. Полтавцева, А.И. Печенкин // Методы и технические средства обеспечения безопасности информации. - 2017. - № 26. - С. 54-56.

56. **Полтавцева, М.А.** Хранение графов в информационных системах / М.А. Полтавцева, А.А. Полтавцев / В сборнике: Информационные ресурсы и системы в экономике, науке и образовании. Сборник статей VII Международной научно-практической конференции. - 2017. - С. 104-109.

57. **Полтавцева, М.А.** Иерархический метод агрегирование данных при потоковом анализе магистрального трафика сети INTERNET / М.А. Полтавцева, П.Д. Зегжда, И.Д Панков // Управление развитием крупномасштабных систем (MLSD2018). Материалы одиннадцатой международной конференции. В 2-х томах. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. - 2018. - С. 367-370.

58. **Полтавцева, М.А.** Особенности применения технологий обработки больших данных в задачах обеспечения кибербезопасности / М.А. Полтавцева // Методы и технические средства обеспечения безопасности информации. - 2018. - № 27. - С. 4-7.

59. **Полтавцева, М.А.** Анализ слабо структурированных данных смешанной семантики / М.А. Полтавцева // Перспективные направления развития отечественных информационных технологий. материалы IV межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. - 2018. - С. 151-152.

60. **Полтавцева, М.А.** Защита данных в системах мониторинга безопасности крупномасштабных объектов / М.А. Полтавцева, М. О. Калинин // Материалы двенадцатой международной конференции. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. - 2019. - С. 1019-1029.

61. **Полтавцева, М.А.** Адаптивный мониторинг информационной безопасности КФС как системная задача / М.А. Полтавцева // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 88–89.

62. **Полтавцева, М.А.** Подготовка и обработка Больших данных в системах адаптивного мониторинга безопасности КФС / М.А. Полтавцева //

Управление развитием крупномасштабных систем MLSD'2020. Труды тринадцатой международной конференции. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. - 2020. – С. 1659-1666.

63. **Полтавцева, М.А.** Обработка онтологий при атрибутивном контроле доступа в киберфизических системах / М.А. Полтавцева // Программные продукты и системы. - 2021. - № 1. - С. 36-41.