На правах рукописи

Лаврова Дарья Сергеевна

МЕТОДОЛОГИЯ ПРЕДОТВРАЩЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ПРОМЫШЛЕННЫЕ СИСТЕМЫ НА ОСНОВЕ АДАПТИВНОГО ПРОГНОЗИРОВАНИЯ И САМОРЕГУЛЯЦИИ

Специальность
05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора технических наук

Санкт-Петербург – 2019

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

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

Официальные оппоненты:
Бирюков Денис Николаевич,
доктор технических наук, доцент, начальник кафедры систем сбора и обработки информации ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского» Министерства обороны Российской Федерации.

Марков Алексей Сергеевич,
доктор технических наук, старший научный сотрудник, президент АО «НПО «Эшелон».

Петренко Сергей Анатольевич,
доктор технических наук, профессор, эксперт секции по проблемам информационной безопасности научного совета при Совете Безопасности Российской Федерации, руководитель Центра Информационной Безопасности АНО ВО «Университет Иннополис».

Ведущая организация:
ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О. Макарова».

Защита состоится «___» декабря 2019 года в _ ч. на заседании диссертационного совета Д 212.229.31 на базе ФГАОУ ВО СПбПУ по адресу: 195251, г. Санкт-Петербург, ул. Политехническая, д. 29, ауд. 175.

С диссертацией, авторефератом можно ознакомиться в библиотеке и на сайте ФГАОУ ВО СПбПУ (www.spbstu.ru). Автореферат размещен на сайте Минобрнауки России (www.vak.gov.ru).
Автореферат разослан «___» _____ 2019 года.

Отзыв на автореферат в двух экземплярах, заверенный печатью организации, просим направлять по адресу ученого совета университета.

Ученый секретарь
диссертационного совета Д 212.229.31,
кандидат технических наук,
доцент Супрун Александр Федорович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Цифровая трансформация технологического уклада привела к развитию современных производственных технологий, интегрирующих физические и информационные процессы, а также обеспечивающих автономное от человека функционирование промышленных систем. Цифровизация промышленной инфраструктуры открыла широкие возможности для реализации компьютерных атак, вектор которых сместился в сторону несанкционированного получения возможности управления системой и нарушения корректности ее функционирования.

Предотвращение компьютерных атак на промышленные системы (ПС), позволяющее не допустить выхода необратимых физических процессов из-под контроля, затруднено ввиду роста числа новых типов компьютерных атак, ограниченного времени на противодействие атакам и отсутствия единой методологии, сочетающей раннее обнаружение атак и противодействие им.

Перечисленные особенности определяют научную проблему создания методологии предотвращения компьютерных атак на ПС. В настоящей работе предпринята попытка создать единую методологию предотвращения компьютерных атак на промышленные системы, направленную на упреждающую саморегуляцию системы при прогнозировании нежелательных тенденций в данных, поступающих от компонентов ПС, что определяет актуальность настоящего исследования. Основу подхода составляют методы, позволяющие на ранней стадии обнаруживать любые типы компьютерных атак и противодействовать им путем автоматической реконфигурации структуры ПС.

Степень разработанности темы исследования. Известно значительное число работ, посвященных созданию подходов к прогнозированию и раннему обнаружению компьютерных атак, в том числе на сложные промышленные и киберфизические системы. Среди них – работы таких российских и зарубежных ученых, как С.А. Петренко, Д.Н. Бирюков, И.Б. Саенко, И.В. Котенко, О.И. Шелухин, Ф. Харроу, А. Окутан. Ряд работ посвящен разработке подходов к противодействию компьютерным атакам. К ним относятся работы А.С. Маркова, Н. Воропая, Н. Геростатопулоса, Р.Сейгера, А. Тиррела, К. Джина.

Объектом исследования являются ПС с развитой сетевой инфраструктурой, в отношении которых реализуются компьютерные атаки.

Предметом исследования являются методы обнаружения и прогнозирования компьютерных атак, методы противодействия компьютерным

атакам как основа технологии автоматического поддержания корректного функционирования ПС.

Цель исследования состоит в обеспечении и поддержании защищенности ПС путем предотвращения компьютерных атак на основе создания методологии раннего обнаружения атак с использованием экстраполяции характеристик системы и реконфигурации системы, позволяющей сохранить ее функциональность в условиях компьютерных атак.

Под предотвращением компьютерной атаки в данной работе понимается комплекс мер, направленных на создание условий, которые исключают проведение атаки или нейтрализуют ее последствия.

Для достижения вышеуказанной цели представляется необходимым решить следующие **задачи**:

1. Провести анализ специфики современных ПС с точки зрения обеспечения информационной безопасности.
2. Создать методологию предотвращения компьютерных атак, в которой объединены методы прогнозирования и саморегуляции, исключающие проведение атаки, а также оценка сохранения защищенности ПС путем формализации условий киберустойчивости.
3. Разработать модель функционирования ПС, инвариантную к типу компьютерной атаки и позволяющую описать последствия реализации атак на ПС.
4. Разработать метод раннего обнаружения компьютерных атак на основе экстраполяции характеристик ПС.
5. Разработать метод саморегуляции на основе реконфигурации структуры ПС.
6. Разработать подход к оценке киберустойчивости ПС, позволяющий определить пределы сохранения системой способности к корректному функционированию.
7. Реализовать прототип системы предотвращения компьютерных атак для применения в ПС с развитой сетевой инфраструктурой на примере интеллектуальных сетей энергоснабжения (Smart Grid).

Научная новизна результатов:

1. Впервые предложена методология предотвращения компьютерных атак на современные ПС, основу которой составляют: графовая модель функционирования ПС; адаптивное прогнозирование путем экстраполяции

временных рядов, сформированных из значений характеристик ПС; автоматическая реконфигурация ПС, обеспечивающая киберустойчивость.

2. Разработана графовая модель функционирования ПС, отражающая последствия всех типов компьютерных атак на ПС, что подтверждается сформулированной и доказанной теоремой о полноте графовой модели.

3. Предложен метод раннего обнаружения компьютерных атак, заключающийся в анализе и экстраполяции временных рядов, сформированных из значений характеристик ПС, с использованием фильтра Калмана и алгоритма машинного обучения Random Forest.

4. Разработан метод саморегуляции, состоящий в реконфигурации структуры ПС, исключающей возможность реализации атаки на ПС или осуществляющей нейтрализацию ее последствий на основе графов де Брёйна и графов перекрытий.

5. Сформулирован принцип киберустойчивости, состоящий в возможности сюръективного отображения из множества способов реконфигурации ПС в множество компьютерных атак, на основе которого предложен подход к определению киберустойчивости ПС на основе эволюционной генетики, позволяющий определить условия, при которых возможно сохранение функционирования системы в условиях деструктивных воздействий.

Теоретическая значимость работы заключается в создании оригинальной единой методологии предотвращения компьютерных атак на ПС, основу которой составляют: универсальная графовая модель, отражающая функционирование ПС и последствия реализации компьютерных атак; методы адаптивного прогнозирования изменения характеристик ПС на основе экстраполяции временных рядов и саморегуляции ПС на основе автоматической реконфигурации ее структуры; в формализации условий сохранения киберустойчивости с использованием моделей эволюционной генетики, определяющих границы области корректного функционирования ПС в условиях компьютерных атак.

Практическая значимость работы определяется возможностью использования разработанных модели, методов, подхода и архитектуры для предотвращения компьютерных атак на ПС с развитой сетевой инфраструктурой. Результаты работы позволяют:

– описывать состояние ПС путем моделирования сетевого взаимодействия их компонентов;

– выявлять и прогнозировать аномалии в характеристиках ПС;

– автоматически реконфигурировать структуру ПС для противодействия компьютерным атакам и сохранения корректного функционирования ПС;

– оценивать граничные условия, при которых рассматриваемая ПС сможет корректно функционировать в условиях компьютерных атак.

Методы исследования. Для решения поставленных задач в диссертационной работе использовались методы математического моделирования, дискретной и вычислительной математики, теории графов, теории вероятностей и математической статистики, теории защиты информации, теории эволюции.

Положения, выносимые на защиту:

1. Графовая модель функционирования ПС, обладающая полнотой моделирования последствий всех типов компьютерных атак на ПС.
2. Метод раннего обнаружения компьютерных атак на основе адаптивного прогнозирования, инвариантный к типу компьютерных атак.
3. Метод саморегуляции на основе автоматической реконфигурации структуры ПС, направленный на исключение условий реализации компьютерных атак.
4. Эволюционный подход к оценке киберустойчивости как условий сохранения защищенности ПС.
5. Архитектура системы предотвращения компьютерных атак для интеллектуальных сетей энергоснабжения (Smart Grid).

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); методы и модели выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса (п. 3); 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).

Степень достоверности результатов исследования подтверждается их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе.

Внедрение результатов работы. Полученные основные научные результаты диссертационной работы используются при выполнении гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (соглашение 075-15-2019-1066), в проектной деятельности АО «НИИ «Рубин», в проектной деятельности ФГУП «Крыловский государственный научный центр», в проектной деятельности АО «РАМЭК-ВС», в проектной деятельности Санкт-Петербургского отделения Российской инженерной академии и АО «ЛОМО», а также в учебном процессе Высшей школы кибербезопасности и защиты информации Института прикладной математики и механики ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» при организации дисциплин «Теория обнаружения вторжений», «Безопасность Интернета вещей» и «Теория и системы управления информационной безопасностью» 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-практическая конференция «РусКрипто» (Москва, 2015-2016, 2018), научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2015-2016, 2018-2019), Межвузовская неделя науки (Санкт-Петербург, 2015), межрегиональная конференция «Информационная безопасность регионов России (Санкт-Петербург, 2013, 2015)» международная конференция «International Conference on. Security of Information and Networks» (Сочи, 2015; Ньюарк (США), 2016), международная научная конференция «Конвергенция цифровых и физических миров: технологические, экономические и социальные вызовы» (Санкт-Петербург, 2018), международная конференция «International Conference on

Industrial Cyber-Physical Systems» (Санкт-Петербург, 2018; Тайбэй (Тайвань), 2019), международная конференция «International Black Sea Conference on Communications and Networking» (Сочи, 2019), международная конференция «World Conference on Smart Trends in Systems, Security and Sustainability» (Лондон (Великобритания), 2019), международный семинар «Nonlinear phenomena in complex systems» (Минск (Беларусь), 2019). Результаты работы победили в конкурсном отборе на предоставление в 2017 году субсидий молодым ученым, молодым кандидатам наук вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, а также в конкурсе 2019-2021 года на получение стипендии Президента РФ молодым ученым и аспирантам.

Публикации по теме диссертации. Результаты диссертационной работы отражены в 66 публикациях, в том числе в 28 публикациях в рецензируемых журналах из перечня ВАК, 3 монографиях и разделах в монографиях, 6 свидетельствах о регистрации программы для ЭВМ, 5 патентах РФ на изобретения.

Структура и объем диссертации. Диссертация состоит из введения, шести глав, заключения, списка использованных источников из 208 наименований. Общий объем работы составляет 303 страницы, в том числе 82 рисунка и 19 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.

В первой главе рассмотрены примеры современных ПС и определена специфика обеспечения их безопасности, заключающаяся, в первую очередь, в наличии развитой и гибкой коммуникационной среды, которая позволяет компонентам ПС реализовывать взаимное управление друг другом. Учитывая высокую вариативность протоколов обмена данными и большое число уязвимостей в компонентах современных ПС, нельзя исключать потерю контроля за потоками данных, которая может привести к скрытому нелегитимному влиянию злоумышленников на работу ПС. Решение задачи обеспечения информационной безопасности осложняется также

необходимостью оперативной обработки больших объемов разнородных данных от компонентов ПС.

Представлен анализ современных научных и практических исследований, направленных на решение задач обнаружения и прогнозирования компьютерных атак, а также противодействия им. Особенное внимание уделено исследованиям, связанным с определением и обеспечением киберустойчивости сложных систем. Результаты исследований продемонстрировали, что, несмотря на наличие перспективных подходов к решению каждой из выделенных задач, на данный момент отсутствует единая методология предотвращения компьютерных атак, учитывающая специфику современных ПС. Также отмечается, что современные методы противодействия компьютерным атакам не являются универсальными, поскольку они тесно связаны с архитектурой защищаемой ПС и особенностями ее сетевой инфраструктуры.

Во второй главе выполнена постановка задачи предотвращения компьютерных атак на ПС, заключающаяся в анализе и адаптивном прогнозе состояния компонентов ПС; саморегуляции структуры ПС и оценке киберустойчивости как интегрального показателя качества выполненного процесса саморегуляции.

Описана предложенная методология предотвращения компьютерных атак, объединяющая методы прогнозирования и саморегуляции, исключающие проведение атаки, а также оценку сохранения защищенности ПС путем формализации условий киберустойчивости.

Сформулирован принцип инвариантности, состоящий в универсальном представлении совокупности функций информационной инфраструктуры ПС, необходимых для формирования среды корректного протекания физических процессов и в раннем обнаружении любых типов компьютерных атак, которое обеспечит запас времени реакции на атаку. Отмечено, что саморегуляция структуры ПС должна выполняться так, чтобы исключить возможность реализации компьютерной атаки или нейтрализовать ее последствия. Сформулированный принцип киберустойчивости состоит в согласовании процессов раннего обнаружения компьютерных атак и саморегуляции структуры ПС, а также в определении условий, при которых возможно сохранение корректного функционирования ПС в условиях компьютерных атак. Отмечено, что предложенная методология направлена на ПС с гибкой, динамической

сетевой инфраструктурой и избыточным составом компонентов и связей между ними.

Разработана графовая модель функционирования ПС, реализующая представление сетевой инфраструктуры ПС в виде ориентированного графа G, множество вершин $V = \{v_1, \dots, v_N\}$ которого характеризует все компоненты ПС, способные к сетевому взаимодействию. Множество дуг $E = \{e_1, \dots, e_M\}$ графа отражает все возможные межкомпонентные связи, проявляющиеся как обмен данными между устройствами. Каждый компонент ПС, моделируемый вершиной v_i, характеризуется набором функций, которые он способен реализовывать: $f_{v_i} = \{f_{v_i}^{(1)}, f_{v_i}^{(2)}, \dots, f_{v_i}^{(k)}\}$. Модель отражает взаимодействие компонентов ПС друг с другом, процессы, необходимые для реализации целевой функции ПС, и саму целевую функцию. Целевая функция F ПС представляется в модели двумя способами одновременно: в виде множества маршрутов на графе (рисунок 1) и в виде набора функциональных последовательностей с заданными типами отношений между функциями: $F = \{F_1, F_2, \dots, F_n\}$.

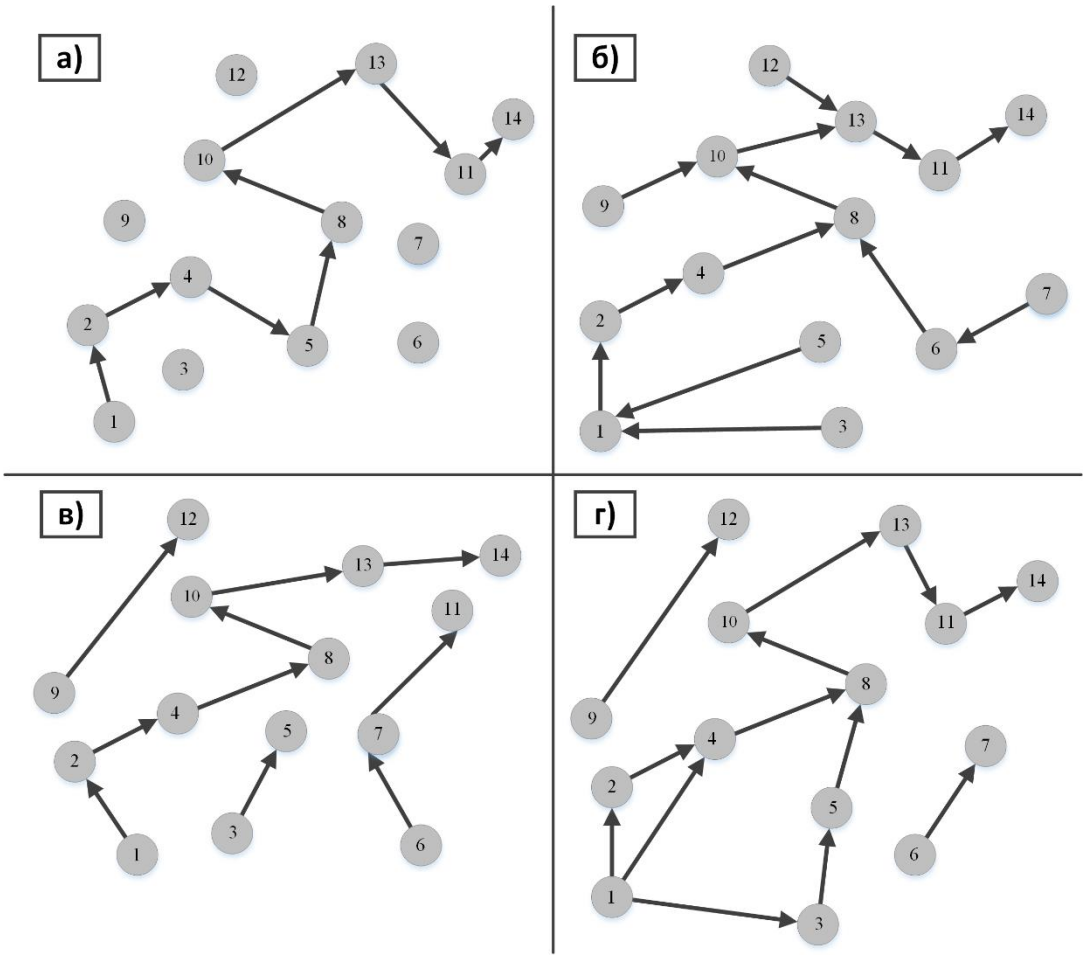

Рисунок 1 – Графовое представление целевой функции ПС

Каждая F_i отражает выполнение одного из процессов и может быть представлена как совокупность упорядоченных взаимосвязанных функций f_j, для которых введены типы отношений $<*, +, (), [] >$. Примеры целевой функции, выраженной с использованием введенных отношений: $F = f_k(f_{k-1}(\dots(f_1)))$, $F = f_n(f_i + f_j * f_k + f_m)$, $F = f_n[f_i + f_j + f_k + f_m]$. В соответствии с рисунком 1, целевая функция может быть представлена на графе в виде:

а) маршрута с последовательным посещением вершин;

б) множества маршрутов, в том числе, имеющих общие вершины;

в) множества независимых маршрутов;

г) гибридного варианта, включающего вышеописанные.

В терминах графовой модели компьютерные атаки описаны в виде преобразований графа G. Они разделяются на структурные, представляющие собой унарные операции над G, и функциональные, заключающиеся в изменении параметров вершин и дуг.

Полноту модели подтверждает следующая

Теорема. Представленная графовая модель отражает все типы компьютерных атак на систему.

Доказательство теоремы основано на рассмотрении объектов компьютерных атак – вершин, дуг и их параметров и отражении изменений в функционировании ПС с использованием матриц смежности $S: s_{ij} = 1\ if\ \exists e_k = (v_i, v_j), e_k \in E, s_{ij} = 0\ otherwise$, матрицы функций вершин $VF: vf_{ij} = 1\ if\ f_j \in \varphi(v_i), vf_{ij} = 0\ otherwise$, матрицы характеристик для дуг $E\Omega: e\omega_{ij} = 1\ if\ \omega_j \in \gamma(e_i), e\omega_{ij} = 0\ otherwise$. Здесь if представляет собой условный оператор, а $otherwise$ означает «в противном случае».

В третьей главе описан подход к предварительной обработке данных, поступающих от компонентов ПС. Обработка данных от сетевых и от конечных устройств ПС различается: сетевой трафик классифицируется с использованием эвристических правил и проходит этап фильтрации; данные от конечных устройств проходят два этапа агрегации, разделенных этапом нормализации. Необходимость классификации сетевого трафика заключается в отделении трафика одноранговых peer-to-peer сетей (P2P) от трафика клиент-серверных сетей для повышения точности при распознавании компьютерных атак. На

данный способ классификации получен патент РФ на изобретение № 2690758 «Способ автоматической классификации сетевого трафика на основе эвристического анализа». В результате предварительной обработки из данных от компонентов ПС формируется множество временных рядов, характеризующих поведение ПС в динамике.

Предложены три метода обнаружения компьютерных атак: на основе мультифрактального анализа, дискретного вейвлет-преобразования и адаптивного прогнозирования. Новизна методов подтверждается патентом РФ на изобретение № 2696296 «Способ обнаружения аномалий в трафике магистральных сетей Интернет на основе мультифрактального эвристического анализа» и свидетельствами о государственной регистрации программ для ЭВМ (№ 2018660237 «Программа для обнаружения аномалий во временных рядах, образованных трафиком магистральных сетей, на основе вычисления мультифрактальных характеристик временных рядов», № 2018660599 «Программа для обнаружения аномалий в трафике магистральных сетей Интернет на основе анализа временных рядов, сформированных коэффициентами детализации дискретного вейвлет-преобразования»).

Методы направлены на анализ временных рядов с целью выявления аномалий, которые потенциально характеризуют влияние компьютерной атаки на функционирование ПС. Описаны принципы работы методов, проведена экспериментальная оценка их точности.

Лучшие результаты продемонстрировал метод обнаружения компьютерных атак на основе адаптивного прогнозирования, который сочетает в себе рекурсивный алгоритм фильтра Калмана и алгоритм машинного обучения Random Forest, в совокупности обеспечивающие раннее обнаружение атаки за счет адаптивной экстраполяции характеристик ПС и автоматическую классификацию полученных значений.

Трудность применения фильтра Калмана для ПС заключается в том, что для построения необходимых матриц и векторов требуется информация о физической модели ПС, которая не всегда доступна. Для решения этой проблемы показания каждого компонента ПС представлены как хаотичная траектория движения некоторого тела в одномерном пространстве. Тело характеризуется координатой Y, переменной скоростью движения V и ускорением a.

Схема работы метода представлена на рисунке 2.

Рисунок 2 – Схема работы метода

В соответствии с предложенной физической моделью, этапы разработанного метода выглядят следующим образом:

1. За начальные оценочные значения берутся самые первые показания компонента ПС: Y_0 и P_0 , где Y_0 – вектор оценки начального значения прогнозируемого параметра, P_0 – ковариационная матрица ошибок оценки на начальном шаге.

2. Начальные значения принимаются за показания компонента в предыдущий момент времени Y_{k-1} и P_{k-1}. Вектор состояния объекта в момент $k-1$ состоит из координаты y_{k-1} объекта на оси Y и скорости V_{k-1} объекта: $Y_{k-1} = \begin{bmatrix} y_{k-1} \\ V_{k-1} \end{bmatrix}$.

3. Обозначим прогнозируемое значение компонента в текущем периоде как Y_{kp} , оно вычисляется на основе предыдущего значения Y_{k-1}: $Y_{kp} = A * Y_{k-1} + B * U_k + W_k$, где A – матрица эволюции системы, $A = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix}$, Δt –

интервал получения значений от компонента ПС, Y_{k-1} – вектор состояния объекта в момент $k-1$, U_k – вектор управляющего воздействия, B – матрица управления, которая прикладывается к вектору управляющих воздействий U_k: $B = \begin{bmatrix} \frac{\Delta t^2}{2} \\ \Delta t \end{bmatrix}$, $U_k = [a_k]$, шумовая матрица W_k – нулевая. Тогда уравнение для вычисления окончательного значения Y_k, полученного после корректировки Y_{kp}, выглядит следующим образом: $Y_k = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} y_{k-1} \\ V_{k-1} \end{bmatrix} + \begin{bmatrix} \frac{\Delta t^2}{2} \\ \Delta t \end{bmatrix} * [a_k] + 0 = \begin{bmatrix} y_{k-1} + V_{k-1} * \Delta t + \frac{\Delta t^2}{2} * a_k \\ V_{k-1} + a_k * \Delta t \end{bmatrix}$. Элементы ковариационной матрицы вычисляются следующим образом: $P_{kp} = A * P_{k-1} * A^{\mathrm{T}} + Q_k$, где Q_k – ковариационная матрица, описывающая случайный характер эволюции системы, ее элементы подбираются экспериментальным путем. На данном шаге заканчивается тап прогнозирования, на последующих шагах выполняется корректировка полученной оценки.

4. Рассчитывается усиление Калмана K , представляющее собой соотношение между ошибками оценок, построенных с использованием физической модели системы, и ошибками измерений. $K = \frac{HP_{kp}}{HP_{kp}H^{\mathrm{T}}+R}$, где H – вспомогательная матрица для приведения усиления Калмана к матрице нужной размерности, в данном случае, $H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, R – ошибки измерений. В упрощенном виде $K = \frac{E_{est}}{E_{est}+E_{meas}}$, где E_{est} – ошибка оценок, E_{meas} – ошибка измерений; $K \in [0,\ 1]$.

5. Для получения от системы показания компонента с вычисленными по ним характеристиками выполняется экстраполяция: $X_k = C * X_{km} + Z_k$, где C – матрица измерений, связывающая истинные значения состояния системы и вектор произведенных измерений, Z_k – нормально распределенная случайная величина с нулевым математическим ожиданием и ковариационной матрицей R_k.

6. Вычисляется матрица ковариации для -го шага: $P_k = (I - KH) * P_{kp}$, где I – единичная матрица, на основе полученного усиления Калмана K, ранее полученной оценки Y_{kp} и имеющегося измерения от компонента X_k , рассчитывается окончательный ответ фильтра Y_k, $Y_k = Y_{kp} + K[X - HY_{kp}]$.

7. Полученное ранее состояние компонента в момент времени k становится его состоянием в момент времени $k-1$, и шаги алгоритма 2–7 повторяются необходимое количество раз. Спрогнозированные значения накапливаются в базе данных.

8. Полученные с помощью фильтра Калмана предсказания разделяются на обучающую и тестовую выборку в соотношении 70% к 30%. Выполняется обучение модели.

9. Выполняется тестирование, вычисляется матрица ошибок классификации и метрики оценки качества классификации.

Экспериментальные исследования метода продемонстрировали высокую точность верного распознавания компьютерных атак на ранней стадии: значения метрик оценки качества классификации находились в пределах 0,93–0,98, время обучения занимало 1–6 секунд, время расчета прогноза на одно наблюдение вперед составило около 0,0001 секунды. К преимуществам метода также относятся низкие требования к объему предоставляемых данных и вычислительных ресурсов.

В четвертой главе описан метод саморегуляции ПС на основе автоматической реконфигурации структуры ПС. Преобразование структуры ПС возможно за счет ее избыточности и динамической сетевой инфраструктуры ПС и позволяет исключить условия реализации атаки или минимизировать ее последствия.

Последствия компьютерной атаки в терминах графовой модели представлены в виде «разрывов» в функциональной последовательности целевой функции ПС. Например, пусть для ПС, реализующей целевую функцию $F = f_6(f_5(f_4(f_3 + f_2[f_1])))$, в результате компьютерной атаки из строя выведен компонент, реализующий функцию f_4. Тогда в результате «разрыва» F остались две последовательности: $f_6(f_5)$ и $f_3 + f_2[f_1]$, для соединения которых необходимо найти нескомпрометированный компонент ПС, способный выполнять функцию f_4 и взаимодействовать с компонентами, реализующими две оставшиеся последовательности.

Такое представление F позволило провести аналогию между восстановлением F и биоинформатической задачей сборки генома. Разработанный метод саморегуляции реализует перенос и адаптацию принципов сборки генома на ПС с использованием математического аппарата графов де

Брёйна и графов перекрытий, обеспечивая повышение скорости реконфигурации.

В зависимости от типа компьютерной атаки и ее влияния на целевую функцию F, предложены различные способы саморегуляции (таблица 1). Функции-риды представляют собой вычислительно простые недекомпозируемые функции, а функции (квази)контиги – вычислительно более сложные функции, которые могут быть представлены как последовательность взаимосвязанных функций-ридов.

Таблица 1 – Способы саморегуляции

Тип нарушения безопасности	Противодействие
1. Нарушение одной функции-рида или одной функции (квази)контига.	Восстановление F с использованием унарных преобразований графа G и графа целевых функций G_F.
2. Нарушение: − нескольких функций-ридов, не связанных между собой; − нескольких функций (квази)контигов, не связанных между собой; − нескольких функций (среди которых есть как функции-риды, так и функции (квази)контиги), не связанных между собой.	Восстановление F с использованием унарных преобразований графа G и графа целевых функций G_F. Также возможно использование графов де Брёйна и/или графов перекрытий.
3. Нарушение нескольких функций (как ридов, так и (квази)контигов), связанных между собой.	Восстановление F с использованием унарных преобразований графа G и графа целевых функций G_F, кластеров функций, графов де Брёйна и/или графов перекрытий.

При нарушении одной функции или нескольких невзаимосвязанных функций предлагается использовать заранее сформированные сценарии саморегуляции, представляемые в терминах графовой модели как унарные преобразования графа (таблица 2).

Таблица 2 – Пример сценариев саморегуляции

Унарная операция, отражающая атаку	Сценарий саморегуляции	Сценарий саморегуляции в терминах графовой модели
1. Удаление вершины v_i из графа G, получение нового графа G'	1. Активация резервной вершины v_i', обладающей не меньшим функционалом f_i в рамках F и соответствующими дугами. Если вершина участвовала в маршруте S, новый маршрут S' повторяет старый, но идет через вершину v'_i вместо вершины v_i. 2. Поиск уже работающей вершины v_j, способной выполнять функцию f_i.	$G =< V, E >$, $G' =< V', E' >$, $G'' =< V'', E'' >$, $V' = V \backslash \{v_i\}, E' \subseteq E$ 1. $V'' = V' \cup \{v_i'\}$, $E' \subseteq E'' \subseteq E$, $\varphi(v_i') \subseteq \varphi(v_i), \theta(v_i) = \theta(v_i')$ $R = \{v_j, \dots, v_i, \dots, v_k\}$, $R' = \{v_j, \dots, v'_i, \dots, v_k\}$; 2. $R' = \pi(F)$
2. Удаление дуги e_{ij} из графа G, получение нового графа G'	1. Создание новой дуги e'_{ij} между вершинами v_i, v_j. Если маршрут проходил через удаленную дугу, то вместо нее используется новая дуга. 2. Поиск альтернативного маршрута с возможностью использовать вершины v_i, v_j; 3. Поиск альтернативного маршрута с запретом на использование вершин v_i, v_j.	$E' = E \backslash \{e_{ij}\}$ 1. $E'' = E \cup \{e'_{ij}\}$, $S = \{v_l, \dots, e_{ij}, \dots, v_k\}$ $S' = \{v_l, \dots, e'_{ij}, \dots, v_k\}$ 2. $S' = \pi(F), v_i, v_j \notin S'$ 3. $S' = \pi(F)$
3. Добавление дуги e_{ij}, получение нового графа G'	1. Удаление дуги без смены маршрута. 2. Удаление дуги, запрет на использование вершин, между которыми возникла	$V'' = V' = V$, $E' = E \cup \{e_{ij}\}$ $E'' = E \backslash \{e_{ij}\}$ 1. $S' = S$

Унарная операция, отражающая атаку	Сценарий саморегуляции	Сценарий саморегуляции в терминах графовой модели
	связь, отражаемая этой дугой. Если маршрут проходил через указанные вершины, производится поиск альтернативного маршрута.	2. $S' = \pi(F), v_i, v_j \notin S'$
4. Замыкание (слияние или отождествление), получение нового графа G'	1. Удаление дуг, инцидентных новой вершине, восстановление удаленных вершин и их дуг, запрет на использование новой вершины для реализации F. 2. Удаление дуг, инцидентных новой вершине, восстановление удаленных вершин и их дуг в том случае, если они необходимы для реализации F, запрет на использование новой вершины для реализации F. 3. Удаление дуг, инцидентных новой вершине, поиск альтернативного маршрута, не включающего новую вершину.	$V' = (V \backslash \{v_i, v_j\}) \cup \{v_k\}$, $E' = (E \backslash \{e_{ab}, \mid a = i \ or \ b = j\}) \cup \{e_{ak} \mid e_{ai} \in E \ or \ e_{aj} \in E\} \cup \{e_{kb} \mid e_{ib} \in E \ or \ e_{jb} \in E\}$ 1. $V'' = V' \cup \{v_i, v_j\}$ $E'' = E$ $S' = S$ 2. $V' \subseteq V'' \subseteq V \cup \{v_k\}$ $E' \backslash \{e_{ak}, e_{kb}\} \subseteq E'' \subseteq E$ $\forall a, b \in V'$ $S' = S$ 3. $E'' = E' \backslash \{e_{ak}, e_{kb}\}$ $\forall a, b \in V'$ $S' = \pi(F)$ $v_k \notin S'$

Описана общая схема работы метода, отмечено, что его реализация может различаться для централизованной и децентрализованной сетевой инфраструктуры ПС. Для децентрализованного случая проведена аналогия с саморегуляцией живой ткани, выделены принципы кооперативного принятия решений и регулярного получения каждым компонентом ПС информации о состоянии ПС. Представлен пример саморегуляции с использованием графов де

Брёйна в случае компьютерной атаки, выражаемой в терминах графовой модели как удаление двух вершин.

Предложенный метод отличается направленностью на преобразование структуры ПС при обнаружении нежелательных тенденций в характеристиках системы, а не на восстановление исходной структуры системы.

В пятой главе выполнена адаптация к ПС принципов эволюционной генетики для формализации условий киберустойчивости системы. Основой для проведенной аналогии стала разработанная графовая модель, обеспечивающая единовременной представление целевой функции F ПС в виде множества маршрутов на графе и в виде набора функциональных последовательностей $F = \{F_1, F_2, \dots, F_n\}$. Предложен способ получения численной оценки текущего значения киберустойчивости, в основе которого лежит оценка видового разнообразия ПС как интегрального показателя качества саморегуляции ПС. Виды в терминах графовой модели представляют собой наборы маршрутов реализации целевой функции F, локализованные в непересекающихся подграфах графа G.

Основу предложенной численной оценки составляет индекс видового разнообразия Симпсона $J = \sum_i \frac{n_i(n_i-1)}{S(S-1)}$, где $n_i -$ число особей в -м виде, а $S -$ число видов. Большое значение J говорит о том, что популяция состоит из малого числа видов, и каждый вид содержит много особей. При малом значении J число видов сопоставимо с численностью популяции. ПС будет киберустойчивой в случае одновременно большого числа видов и особей каждого вида, для этого введен показатель J_{ideal}:

$$J_{ideal} = \sum_i \frac{n_i(n_i-1)}{S_{ideal}(S_{ideal}-1)} \approx \sum_i \left(\frac{n_i}{S_{ideal}}\right)^2 = \sum_i \left(\frac{\frac{N}{S_{ideal}}}{S_{ideal}}\right)^2 = \sum_i \left(\frac{N}{S_{ideal}^2}\right)^2,$$

где S_{ideal} – «идеальное» значение числа видов, $S_{ideal} = \frac{N_{nodes}}{length_{Route} * k}$, N – объем популяции (число маршрутов реализации целевой функции ПС), $length_{Route}$ – длина маршрута, N_{nodes} – число вершин в графе, $k -$ коэффициент, характеризующий достаточное число маршрутов одного вида для рассматриваемой ПС, $k = log_{length_{Route}} N_{nodes}$.

Сложность применения показателей видового разнообразия к ПС заключается в необходимости учитывать локализацию маршрутов,

реализующих F. Введен модифицированный индекс Симпсона: $J' = \sum_i \left(\frac{\sum_j w_j}{S}\right)^2$, где w_j – коэффициент, показывающий степень «занятости» вершин маршрута маршрутами другого вида. Поскольку J' – относительная величина, для оценки киберустойчивости ПС введен показатель $C = \frac{J'}{J_{ideal}} \in [0; +\infty)$, учитывающий значение J_{ideal}. Высокая киберустойчивость ПС характеризуется диапазоном значений $[0,\ 1]$.

Анализ динамики эволюционного процесса позволил формализовать условия киберустойчивости ПС. Динамика числа маршрутов реализации F и вероятность сохранения одних и тех же вершин G (компонентов ПС) определяются прямым (1) и обратным (2) уравнениями Колмогорова, соответственно:

$$\frac{\partial \varphi}{\partial t} = -\frac{\partial (M_{\delta X} \varphi)}{\partial X} + \left(\frac{1}{2}\right) \frac{\partial^2 (D_{\delta X} \varphi)}{\partial X^2}, \quad (1)$$

$$\frac{\partial \varphi}{\partial t} = M_{\delta P} \frac{\partial (\varphi)}{\partial P} + \left(\frac{1}{2}\right) D_{\delta P} \frac{\partial^2 (\varphi)}{\partial P^2}, \quad (2)$$

где $\varphi(X, t|P, 0)$ – плотность вероятности, характеризующая значение частоты X гена в момент времени t при условии, что при $t = 0$ частота была равна P, $M_{\delta X}$ – среднее значение изменения частоты X, $D_{\delta X}$ – дисперсия изменения частоты X.

В шестой главе представлена архитектура системы предотвращения компьютерных атак для ПС с развитой сетевой инфраструктурой на примере интеллектуальных сетей энергоснабжения (Smart Grid).

Поскольку разработанная методология предотвращения компьютерных атак на ПС носит биоинспирированный характер, разработка архитектуры выполнялась с использованием принципов функционирования живого организма. Для этого к ПС адаптированы положения теории функциональных систем П.К. Анохина. Эта теория сосредоточена на «системах, обладающих способностью экстренной самоорганизации, динамически и адекватно приспосабливающие организм к изменению внешней обстановки».

В предложенной архитектуре учтена специфика современных ПС, а именно:

– наличие механизмов взаимодействия между физическими и информационными составляющими ПС;

– наличие объединений компонентов, реализующих определенные функциональные последовательности целевой функции;

– требование к киберустойчивости и непрерывности функционирования ПС;

– необходимость обеспечения саморегуляции ПС в случае сбоев или компьютерных атак;

– способность системы предотвращения атак к накоплению знаний и самообучению, эволюционная защита.

Архитектура системы предотвращения атак на Smart Grid в контексте теории функциональных систем П.К. Анохина представлена на рисунке 3.

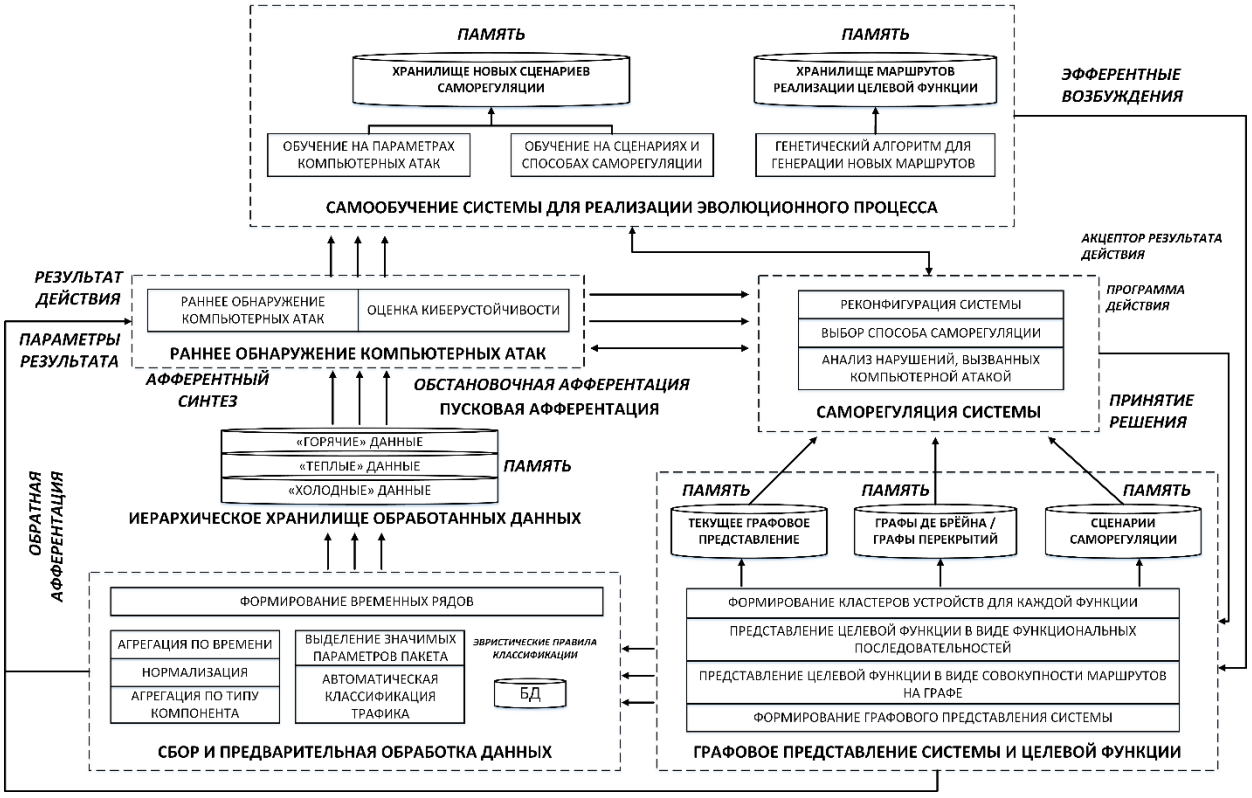

Рисунок 3 — Архитектура системы предотвращения атак на Smart Grid в контексте теории функциональных систем П.К. Анохина

Экспериментальные исследования проведены на данных от промышленных энергетических систем, которые представляют собой первичную стадию развития интеллектуальных сетей энергоснабжения Smart Grid. Сетевая инфраструктура Smart Grid смоделирована в виде графа (рисунок 4) с использованием набора данных «Power System Attack Datasets» от автоматической энергетической системы, собранных университетом штата

Миссисипи и национальной лабораторией Ок-Ридж, США. Данные содержат характеристики системы при нормальном функционировании и при воздействии на систему различных компьютерных атак. На основе этих данных было смоделировано 28 компьютерных атак следующих сценариев: внедрение ложных данных, изменение настроек системы, удаленное отключение компонентов системы.

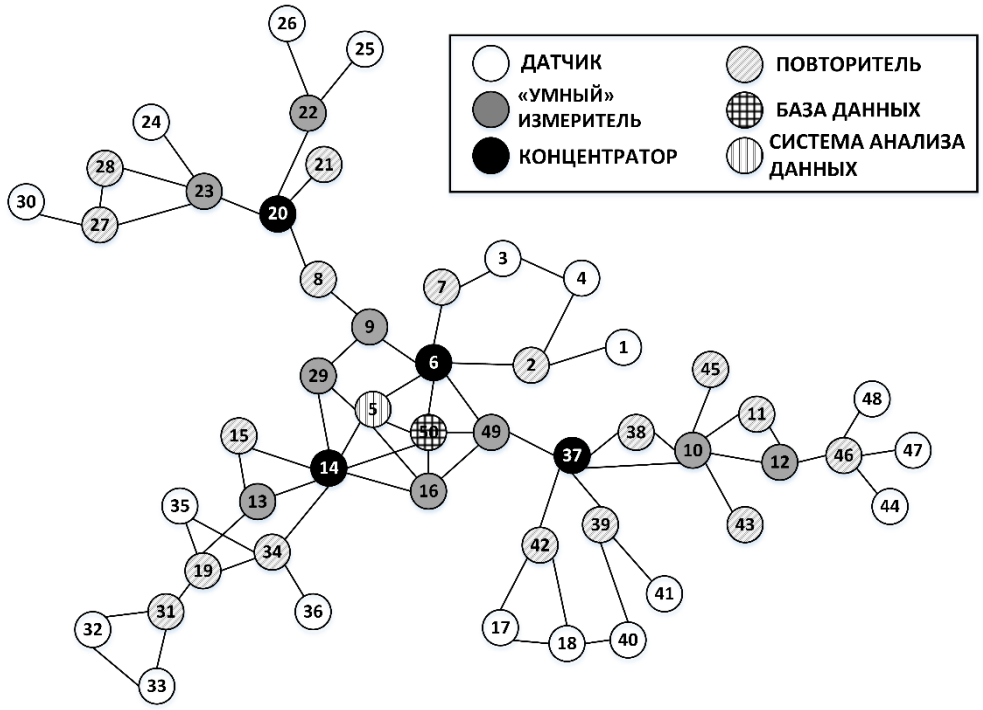

Рисунок 4 – Граф, моделирующий сетевую инфраструктуру Smart Grid

Метод раннего обнаружения компьютерных атак успешно обнаружил все атаки за счет точного предсказания фильтром Калмана поведения временных рядов как в нормальном состоянии, так и при атаках (рисунки 5, 6). Время расчета показаний фильтра Калмана для одного временного ряда длиной 5067 наблюдений составило примерно 0,47 секунд. Время, затраченное на расчет прогноза на одно наблюдение вперед, составило около 0,0001 секунды. Значения показателей качества работы алгоритма на тестовой выборке представлены в таблице 3. Лес содержит 30 деревьев, глубина каждого не превышает пяти уровней. Обучение алгоритма заняло около 0,2 секунд, при этом работа алгоритма на тестовой выборке заняла около 0,02 секунд.

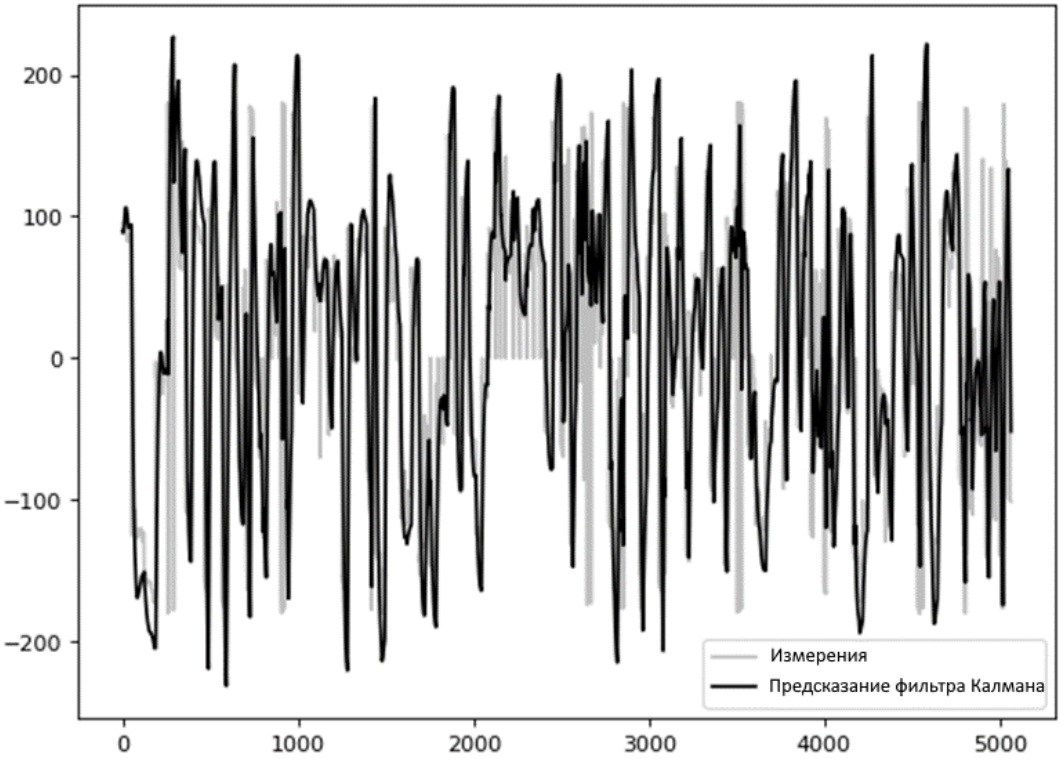

Рисунок 5 – Прогнозирование временного ряда для «умного» измерителя при атаке внедрения ложных данных

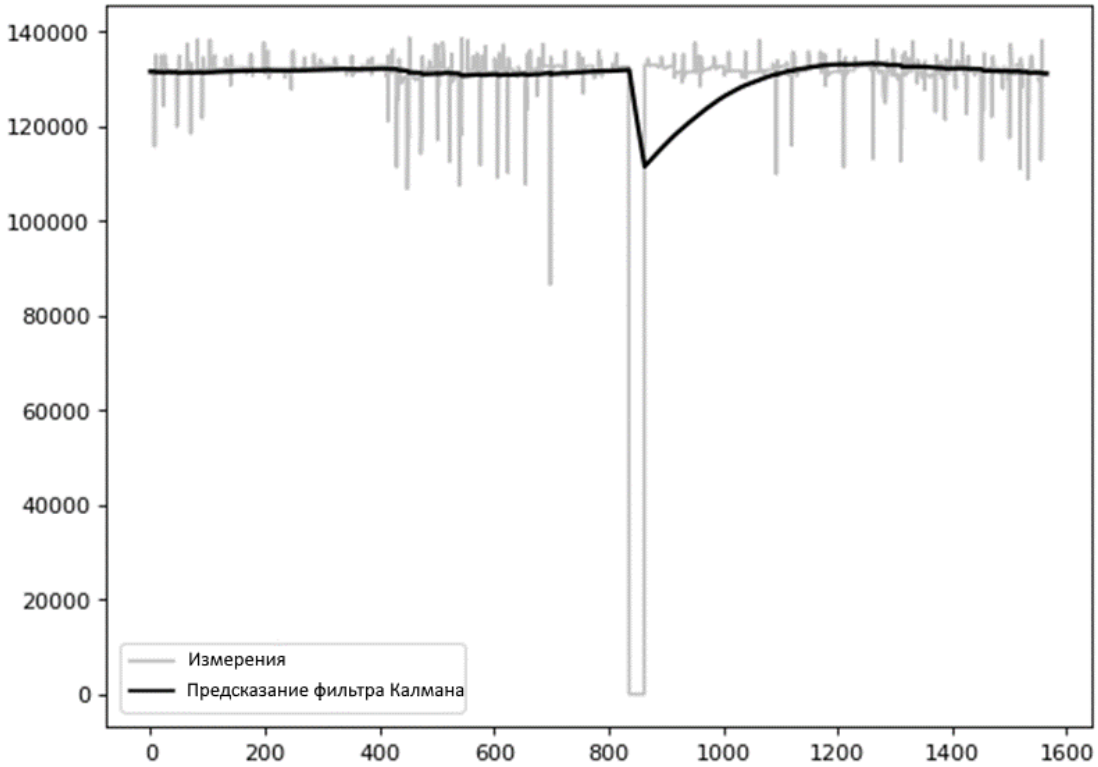

Рисунок 6 – Прогнозирование временного ряда для «умного» измерителя при атаке удаленного отключения устройства

Таблица 3 – Значение метрик качества работы Random Forest

Название метрики качества	Значение метрики качества
Accuracy	0,97
Precision	0,97
Recall	0,95

Таким образом, разработанный метод раннего обнаружения атак на основе адаптивного прогнозирования продемонстрировал хорошую точность обнаружения и высокую скорость работы.

Саморегуляция смоделированной системы в случае различных атак производилась либо с использованием готовых сценариев, либо с использованием графов де Брёйна/графов перекрытий. На рисунке 7 представлен граф, моделирующий подсистему анализа Smart Grid; точечными стрелками представлена целевая функция $F = f_7\left(f_6\left(f_5\left(f_4\left(f_3(f_2(f_1))\right)\right)\right)\right)$.

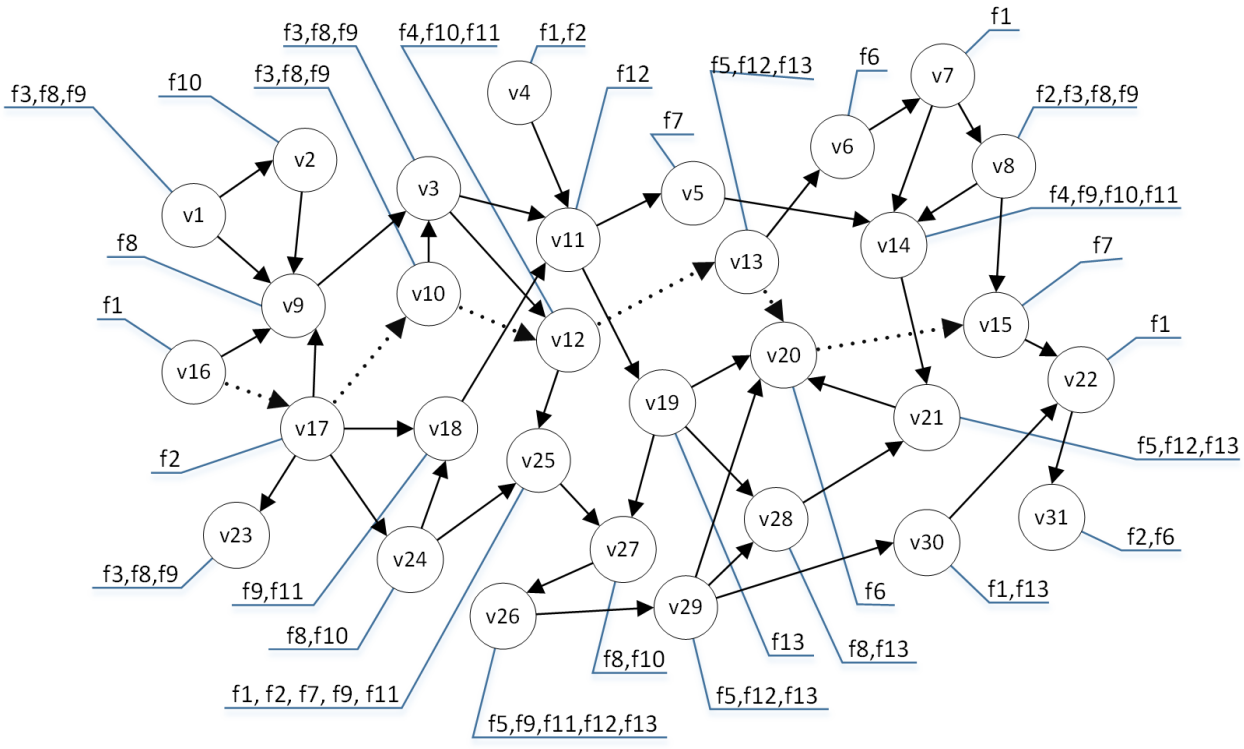

Рисунок 7 – Граф, моделирующий подсистему анализа Smart Grid

В результате смоделированной компьютерной атаки, заключающейся в выведении из строя трех компонентов (v_{10}, v_{12}, v_{13}), была выполнена саморегуляция с использованием графов перекрытий (рисунок 8).

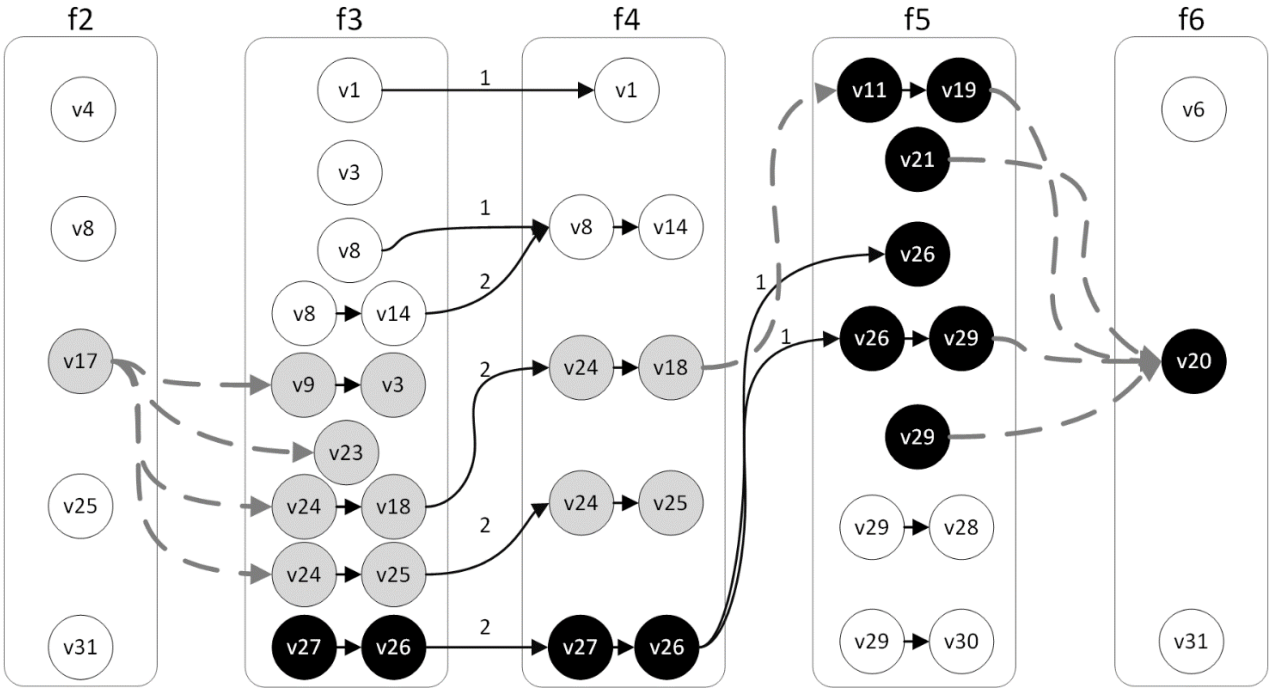

Рисунок 8 – Саморегуляция с использованием графа перекрытий

Новый маршрут реализации целевой функции представлен на рисунке 9.

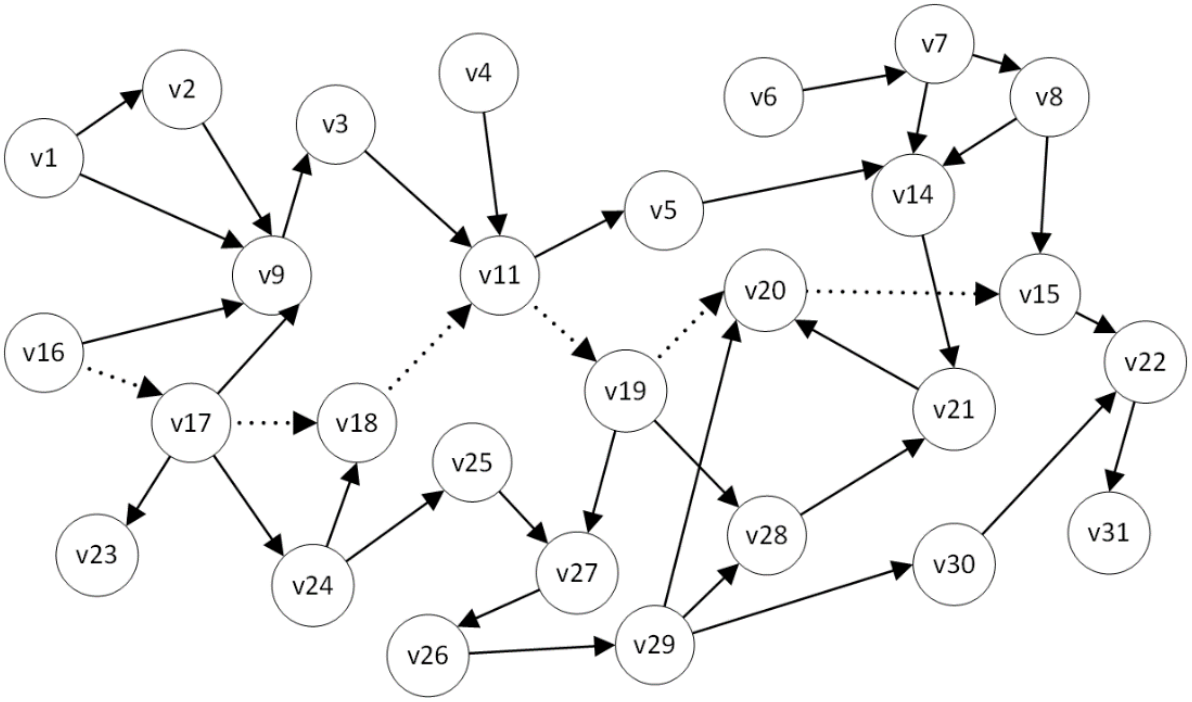

Рисунок 9 – Новый маршрут целевой функции подсистемы анализа Smart Grid

Оценка киберустойчивости подтвердила, что введенный показатель киберустойчивости, основанный на индексе видового разнообразия Симпсона, отражает как прогрессивную эволюцию системы, так и ее деградацию вследствие компьютерной атаки.

Вычисленное для смоделированной системы эталонное значение модифицированного индекса Симпсона J_{ideal} составило 65,93. Результирующее значение модифицированного показателя Симпсона равно $J = 275{,}56$. Значение киберустойчивости C составило 4,179.

В результате смоделированной компьютерной атаки, заключающейся в выведении из строя одного компонента системы, значение показателя киберустойчивости изменилось до 6,46, что говорит об уменьшении видового разнообразия системы.

В результате саморегуляции, заключающейся в замене удаленной вершины графа на другую, значение киберустойчивости C стало равным 4,42. Динамика значений показателя киберустойчивости представлена на рисунке 10. Следует отметить, что несмотря на то, что значение показателя снизилось, оно не достигло изначального уровня.

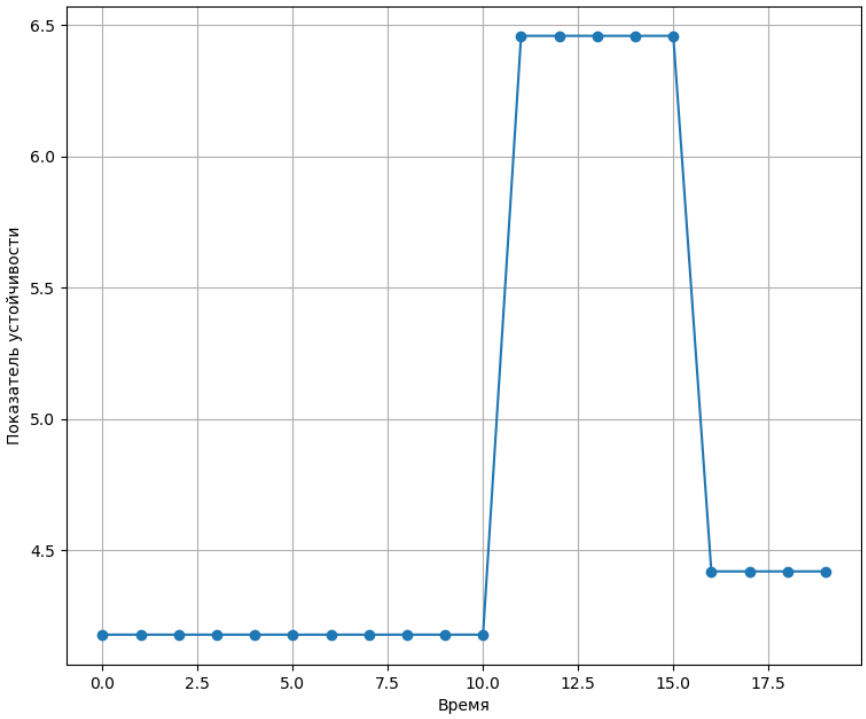

Рисунок 10 – Динамика показателя киберустойчивости до атаки, во время атаки и после саморегуляции ПС

Для увеличения значения киберустойчивости использован эволюционный подход, использующий мутацию и скрещивание маршрутов реализации целевой функции. В результате эволюционного процесса появилось пять видов рабочих маршрутов, в то время как изначально число видов было равно 3. Динамика изменения показателя устойчивости в результате эволюционного процесса представлена на рисунке 11.

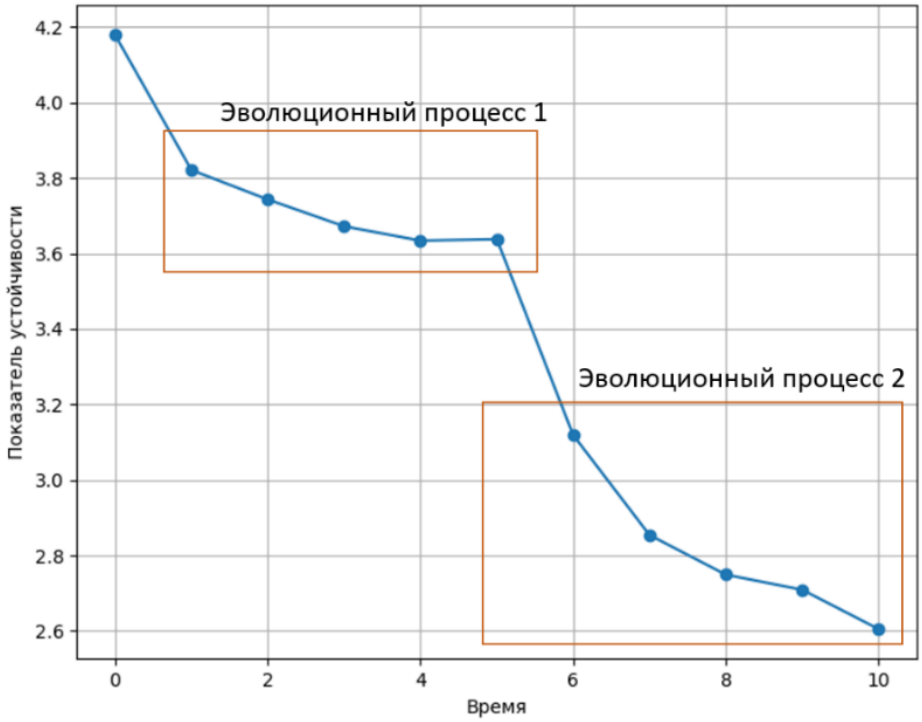

Рисунок 11 – Динамика показателя киберустойчивости в ходе эволюционного процесса

Таким образом, все разработанные методы продемонстрировали свою эффективность в части обнаружения компьютерных атак на основе адаптивного прогнозирования и в части саморегуляции с использованием графов перекрытий.

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

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате диссертационного исследования предложена методология раннего обнаружения атак с использованием экстраполяции характеристик ПС и реконфигурации ПС, позволяющая сохранить ее функциональность в условиях

компьютерных атак, и тем самым обеспечить и поддерживать защищенность ПС. Получены следующие результаты:

1. Проведен анализ специфики современных ПС с точки зрения обеспечения информационной безопасности, сформулированы особенности ПС, порождающие проблемы безопасности, для устранения которых необходимо осуществлять предотвращение компьютерных атак.

2. Предложена методология предотвращения компьютерных атак на современные ПС, основу которой составляют: графовая модель функционирования ПС; адаптивное прогнозирование путем экстраполяции временных рядов, сформированных из значений характеристик ПС; автоматическая реконфигурация ПС, обеспечивающая киберустойчивость.

3. Разработана графовая модель функционирования системы, обладающая полнотой моделирования последствий всех типов компьютерных атак на ПС.

4. Разработан метод раннего обнаружения компьютерных атак на основе анализа временных рядов и адаптивного прогнозирования, инвариантный к типу компьютерных атак.

5. Разработан метод саморегуляции на основе автоматической реконфигурации структуры ПС, направленный на исключение условий реализации компьютерных атак.

6. Предложен эволюционный подход к оценке киберустойчивости как условий сохранения защищенности ПС.

7. Разработана архитектура и реализован прототип системы предотвращения компьютерных атак для интеллектуальных сетей энергоснабжения (Smart Grid).

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ:

В рецензируемых журналах из перечня ВАК:

1. Печенкин, А.И. Моделирование высокоскоростной параллельной обработки сетевого трафика на многопроцессорном кластере / А.И. Печенкин, **Д.С. Лаврова** // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2012. – № 4. – С. 33–39.

2. Печенкин, А.И. Параллельный анализ безопасности сетевого трафика на многопроцессорном кластере / А.И. Печенкин, **Д.С. Лаврова** // Проблемы

информационной безопасности. Компьютерные системы. – СПб., 2013. – № 1. – С. 55–62.

3. Печенкин, А.И. Обнаружение инцидентов безопасности в интернете вещей / А.И. Печенкин, **Д.С. Лаврова** // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2015. – № 2. – С. 69–79.

4. Полтавцева, М.А. Планирование задач агрегации и нормализации данных интернета вещей для обработки на многопроцессорном кластере / М.А. Полтавцева, А.И. Печенкин, **Д.С. Лаврова** // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2016. – № 1. – С. 37–46.

5. **Лаврова, Д.С.** Подход к разработке SIEM-системы для Интернета вещей / Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2016. – № 2. – С. 51–59.

6. **Лаврова, Д.С.** Онтологическая модель предметной области Интернета вещей для анализа безопасности / Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2016. – № 3. – С. 68–75.

7. Зегжда, П.Д. Систематизация киберфизических систем и оценка из безопасности / П.Д. Зегжда, М.А. Полтавцева, **Д.С. Лаврова** // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2017. – № 2. – С. 127–138.

8. Зегжда, П.Д. Прецедентный анализ гетерогенных слабоструктурированных 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. – СПб., 2018. – № 1. – С. 17–31.

9. Калинин, М.О. Обнаружение угроз в киберфизических системах на основе методов глубокого обучения с использованием многомерных временных рядов / М.О. Калинин, **Д.С. Лаврова**, А.В. Ярмак // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2018. – № 2. – С. 111–117.

10. Зегжда, П.Д. Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании / П.Д. Зегжда, **Д.С. Лаврова**, А.А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2018. – № 2. – С. 48–58.

11. **Лаврова, Д.С.** Анализ безопасности на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / Д.С. Лаврова, И.В. Алексеев, А.А. Штыркина, //

Проблемы информационной безопасности. Компьютерные системы. – СПб., 2018. – № 2. – С. 9–15.

12. **Лаврова, Д.С.** Предупреждение DOS-атак путем прогнозирования значений корреляционных параметров сетевого трафика / Д.С. Лаврова, Е.А. Попова, А.А. Штыркина, С.И. Штеренберг // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2018. – № 3. – С. 70–77.

13. Зегжда, П.Д. Обнаружение аномалий в сетевом трафике с использованием дискретного вейвлет-преобразования и метода разладки / П.Д. Зегжда, Е.Б. Александрова, **Д.С. Лаврова**, А.А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2018. – № 4. – С. 14–21.

14. **Лаврова, Д.С.** Обнаружение нарушений информационной безопасности в АСУ ТП на основе прогнозирования многомерных временных рядов, сформированных из значений параметров работы конечных устройств системы / Д.С. Лаврова, А.А. Хушкеев // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2019. – № 1. – С. 18–30.

15. Александрова, Е.Б. Применение закона Бенфорда для обнаружения DOS-атак на промышленные системы / Е.Б. Александрова, **Д.С. Лаврова**, А.В, Ярмак // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2019. – № 1. – С. 79–88.

16. Зегжда, Д.П. Подход к созданию критерия устойчивого функционирования киберфизических систем / Д.П. Зегжда, Е.Ю. Павленко, **Д.С. Лаврова**, А.А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2019. – № 2. – С. 156–163.

17. Зегжда, Д.П. Прогнозирование кибератак на промышленные системы с использованием фильтра Калмана / Д.П. Зегжда, **Д.С. Лаврова**, А.В. Ярмак // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2019. – № 2. – С. 164–171.

18. Полтавцева, М.А. An approach to data normalization in the Internet of Things for security analysis / М.А. Полтавцева, А.И. Печенкин, **Д.С. Лаврова** // Программные продукты и системы. – СПб., 2016. – № 2. – С. 83–88.

19. **Лаврова, Д.С.** Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам / Д.С. Лаврова, Д.П. Зегжда, Е.А. Зайцева // Вопросы кибербезопасности. – М., 2019. – № 2 (30). – С. 13–20.

20. **Lavrova, D.** Applying correlation analysis methods to control flow violation detection in the Internet of Things / D. Lavrova, A. Pechenkin, V. Gluhov // Automatic Control and Computer Sciences. - 2015. - Vol. 49. - Issue №8. - P. 735–740.

21. **Lavrova, D.S.** An approach to developing the SIEM system for the Internet of Things / D.S. Lavrova // Automatic Control and Computer Sciences. - 2016. - Vol. 50. - Issue №8. - P. 673–681.

22. 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.

23. **Lavrova, D.S.** An ontological model of the domain of applications for the Internet of Things in analyzing information security / D.S. Lavrova, Y.S. Vasil'ev // Automatic Control and Computer Sciences. - 2017. - Vol. 51. - Issue №8. - P. 817–823.

24. 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.

25. Kalinin, M.O. Detection of threats in cyberphysical systems based on deep learning methods using multidimensional time series / M.O. Kalinin, **D.S. Lavrova**, A.V. Yarmak // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 912–917.

26. Zegzhda, P.D. Multifractal analysis of Internet backbone traffic for detecting denial of service attacks / P.D. Zegzhda, **D.S. Lavrova**, A.A. Shtyrkina // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 936–944.

27. **Lavrova, D.S.** Security analysis based on controlling dependences of network traffic parameters by wavelet transformation / D.S. Lavrova, I.V. Alekseev, A.A. Shtyrkina // Automatic Control and Computer Sciences. - 2018. - Vol. 52. - Issue №8. - P. 931–935.

28. 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.

В монографиях и разделах в монографиях:

29. **Лаврова, Д. С.** От информационной безопасности к кибербезопасности. Опыт научно-исследовательских работ и подготовки кадров в Санкт-Петербургском политехническом университете Петра Великого / Зегжда П.Д., Зегжда Д.П., Александрова Е.Б., Калинин М.О., Лаврова Д.С. – СПб.: Изд-во Политехн. ун-та, 2017. – 322 с., ISBN 978-5-7422-5604-5.

30. **Лаврова, Д. С.** Математические методы обнаружения и предотвращения компьютерных атак на распределенные системы / Д.С. Лаврова; под ред. профессора РАН, доктора техн. наук Д. П. Зегжды. – М.: Горячая линия – Телеком, 2019. – 92 с. ISBN 978-5-9912-0826-0.

31. **Лаврова, Д.С.** 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 978-5-9912-0827-7.

В свидетельствах о регистрации программы для ЭВМ:

32. Программа для ЭВМ 2019610598 Российская Федерация. Программа для оценки безопасности киберфизической системы на основе вычисления показателя Херста [Текст] / Зегжда Д.П., Павленко Е.Ю., **Лаврова Д.С.**, Ярмак А.В.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018665297 заявл. 27.12.2018 ; опубл. 14.01.2019.

33. Программа для ЭВМ 2018660604 Российская Федерация. Программа для анализа безопасности на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования [Текст] / Зегжда П.Д., **Лаврова Д.С.**, Алексеев И.В.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018617984 заявл. 26.07.2018 ; опубл. 27.08.2018.

34. Программа для ЭВМ 2018660237 Российская Федерация. Программа для обнаружения аномалий во временных рядах, образованных трафиком магистральных сетей, на основе вычисления мультифрактальных характеристик

временных рядов [Текст] / Зегжда П.Д., **Лаврова Д.С.**; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018617982 заявл. 26.07.2018 ; опубл. 21.08.2018.

35. Программа для ЭВМ 2018660599 Российская Федерация. Программа для обнаружения аномалий в трафике магистральных сетей Интернет на основе анализа временных рядов, сформированных коэффициентами детализации дискретного вейвлет-преобразования [Текст] / Зегжда П.Д., **Лаврова Д.С.**; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018618268 заявл. 26.07.2018 ; опубл. 27.08.2018.

36. Программа для ЭВМ 2019661032 Российская Федерация. Программа для формирования стратегий реализаций архитектурного гомеостаза на основе разложения целевой функции и использования принципа суперпозиции [Текст] / Зегжда Д.П., **Лаврова Д.С.**, Павленко Е.Ю., Зайцева Е.А.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2019660010 заявл. 06.08.2019 ; опубл. 16.08.2019.

37. Программа для ЭВМ 2019660900 Российская Федерация. Программа для оценки устойчивости функционирования киберфизической системы на основе вычисления спектральных характеристик моделирующего ее графа [Текст] / Зегжда Д.П., **Лаврова Д.С.**, Павленко Е.Ю., Штыркина А.А.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2019619758 заявл. 06.08.2019 ; опубл. 15.08.2019.

В патентах РФ на изобретения:

38. Пат. 2654167 Российская Федерация. Способ обнаружения скрытых взаимосвязей в Интернете Вещей [Текст] / Зегжда П.Д., **Лаврова Д.С.**, Печенкин А.И.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский

политехнический университет Петра Великого". – № 2015148437; заявл. 10.11.2015 ; опубл. 15.05.2017, Бюл. № 14 – 2 с.

39. 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.

40. Пат. 2642414 Российская Федерация. Способ визуализации взаимосвязей в Интернете Вещей [Текст] / Зегжда П.Д., **Лаврова Д.С.**, Печенкин А.И.; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2016118327 заявл. 11.05.2016 ; опубл. 24.01.2018, Бюл. № 3 – 2 с.

41. Пат. 2696296 Российская Федерация. Способ обнаружения аномалий в трафике магистральных сетей Интернет на основе мультифрактального эвристического анализа [Текст] / Зегжда П.Д., **Лаврова Д.С.**; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018138651 заявл. 01.11.2018 ; опубл. 01.08.2019, Бюл. № 22 – 2 с.

42. Пат. 2690758 Российская Федерация. Способ автоматической классификации сетевого трафика на основе эвристического анализа [Текст] / Зегжда П.Д., **Лаврова Д.С.**; заявитель и патентообладатель федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого". – № 2018132592 заявл. 12.09.2018 ; опубл. 05.06.2019, Бюл. № 16 – 2 с.

В изданиях, индексируемых РИНЦ:

43. **Лаврова, Д.С.** Корреляционно-регрессионный анализ событий безопасности в Интернете Вещей / Д.С. Лаврова, А.И. Печенкин // Методы и технические средства обеспечения безопасности информации. – 2015. – № 24. – С. 24–26.

44. **Лаврова, Д.С.** Моделирование событий в Интернете Вещей и построение справочников метаданных устройств / Д.С. Лаврова, М.А. Полтавцева // Методы и технические средства обеспечения безопасности информации. – 2015. – № 24. – С. 26–28.

45. Зегжда, Д.П. Оценка киберустойчивости информационно-технологических систем на основе самоподобия / Д.П. Зегжда, П.Д. Зегжда, **Д.С. Лаврова**, А.А. Штыркина // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 101–104.

46. **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.

47. Штыркина, А.А. Обнаружение аномалий в трафике магистральных сетей Интернет с использованием мультифрактального анализа / А.А. Штыркина, П.Д. Зегжда, **Д.С. Лаврова** // Методы и технические средства обеспечения безопасности информации. – 2018. – № 27. – С. 14–15.

48. Алексеев, И.В. Анализ безопасности магистральных каналов связи на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / И.В. Алексеев, П.Д. Зегжда, **Д.С. Лаврова**, А.А. Штыркина // Методы и технические средства обеспечения безопасности информации. – 2018. – № 27. – С. 16–17.

49. Штыркина, А.А. Подход к оценке структурной устойчивости киберфизических систем на основе спектральной теории графов / А.А. Штыркина, Е.Ю. Павленко, **Д.С. Лаврова** // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 21–23.

50. **Лаврова, Д.С.** Подход к предотвращению кибератак на децентрализованную сетевую инфраструктуру сложных промышленных объектов / Д.С. Лаврова // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 26–28.

51. Зайцева, Е.А. Нейтрализация последствий деструктивных воздействий путём применения теории графов для переконфигурирования структуры системы / Е.А. Зайцева, **Д.С. Лаврова**, Д.П. Зегжда // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 7–8.

52. Zegzhda, D.P. Approach to Internet of Things detection of security incidents using SIEM technology / D.P. Zegzhda, **D.S. Lavrova** // Интеллектуальные технологии на транспорте. – 2017. – № 1 (9). – С. 35–41.

53. **Лаврова, Д.С.** Обнаружение и анализ инцидентов безопасности в интернете вещей / Лаврова Д.С. // Информатика и кибернетика (ComCon-2015) сборник докладов студенческой научной конференции Института информационных технологий и управления. Н. М. Вербова (отв. ред.). – 2015. – С. 247–250.

В изданиях, индексируемых Scopus и Web of Science:

54. Kalinin, M. High performance traffic processing in virtualized framework / M. Kalinin, **D. Lavrova**, A. Pechenkin // Доклади на Българската Академия на Науките. – 2015. – Т. 68. – № 7. – P. 909–916.

55. **Lavrova, D.** Applying correlation and regression analysis to detect security incidents in the internet of things // D. Lavrova, A. Pechenkin // International Journal of Communication Networks and Information Security. – 2015. – Т. 7. – № 3. – P. 131–137.

56. Stepanova, T. Ontology-based Big Data approach to automated penetration testing of large-scale heterogeneous systems / T. Stepanova, A. Pechenkin, **D. Lavrova** // ACM International Conference Proceeding Series 8. Сер. "Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015". – 2015. – P. 519–525.

57. Zegzhda, P. Safe integration of SIEM-systems with Internet of Things: data aggregation, integrity control, and bioinspired safe routing / P. Zegzhda, D. Zegzhda, M. Kalinin, A. Pechenkin, A. Minin, **D. Lavrova** // ACM International Conference Proceeding Series 9. Сер. "Proceedings of the 9th International Conference on Security of Information and Networks, SIN 2016". – 2016. – P. 81–87.

58. **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.

59. **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.

60. **Lavrova, D.** Wavelet-analysis of network traffic time-series for detection of attacks on digital production infrastructure / D. Lavrova, P. Semyanov, A. Shtyrkina, P. Zegzhda // International Scientific Conference “The Convergence of Digital and Physical Worlds: Technological, Economic and Social Challenges” (CC-TESC2018). – 2018. – 00052.

61. Zegzhda, D. Detection of information security breaches in distributed control systems based on values prediction of multidimensional time series / D. Zegzhda, **D. Lavrova**, A. Khushkeev // Proceedings - 2019 IEEE Industrial Cyber-Physical Systems, ICPS 2019. – 2019. – P. 780–784.

62. **Lavrova, D.** Using GRU neural network for cyber-attack detection in automated process control systems / D. Lavrova, D. Zegzhda, A. Yarmak // Proceedings - 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). – 2019. – P. 818-823.

63. **Lavrova, D.** Predicting cyber attacks on industrial systems using the Kalman filter / D. Lavrova, D. Zegzhda, A. Yarmak // Proceedings - 2019 IEEE World Conference on Smart Trends in Systems, Security and Sustainability. – 2019. – P. 818–823.

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

В других изданиях:

65. **Лаврова, Д.С.** Параллельная обработка сетевого трафика для анализа безопасности передаваемых объектов / Д.С. Лаврова // Информационная безопасность регионов России. – 2013. – С. 224–225.

66. **Лаврова, Д.С.** Расследование инцидентов безопасности в Интернете Вещей с использованием корреляционно-регрессионного анализа / Д.С. Лаврова, А.И. Печенкин // Информационная безопасность регионов России. – 2015. – С. 110.