Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук
(СПб ФИЦ РАН)

На правах рукописи

Семенов Виктор Викторович

Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, профессор
Лебедев Илья Сергеевич

Санкт-Петербург – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы диссертации. Цифровая трансформация промышленности и повседневных сфер деятельности человека, развитие «Индустрии 4.0», сенсорных и беспилотных технологий привели к широкому распространению киберфизических систем (КФС), реализующих физические процессы при помощи обмена информацией друг с другом. В виду тесной интеграции КФС в производственно-технологические системы, системы критической информационной инфраструктуры, а также значительного количества возможных точек вхождения, задача мониторинга информационной безопасности (ИБ) для КФС является более сложной, по сравнению с классическими информационными системами.

В случае реализации угроз ИБ основной целью злоумышленника, как правило, является получение возможности управления КФС при помощи информационных воздействий, при этом деструктивные информационные воздействия могут влиять как на процессы хранения, обработки и передачи информации внутри системы, так и на физические процессы исполнительных механизмов КФС, приводя при этом к финансовым потерям, а также нанося организациям серьёзный имиджевый ущерб.

Реализация угроз ИБ киберфизических систем, тесно интегрированных в критическую информационную инфраструктуру, способна привести к серьёзным техногенным, экологическим катастрофам и человеческим жертвам. Ежегодно растёт число атак на КФС, в том числе являющиеся объектами критической инфраструктуры, что в совокупности с недостаточной точностью и оперативностью обнаружения нарушений ИБ КФС определяет **важность** и **значимость** решаемой научной задачи.

Таким образом, сложность проектирования и эксплуатации систем обеспечения информационной безопасности КФС, недостаточный уровень точности и быстроты выявления нарушений ИБ КФС существующими методами с одной стороны и необходимость снижения рисков нарушений функционирования

КФС при осуществлении атак с другой стороны приводят к противоречию, выходом из которого является объективная необходимость разработки и усовершенствования методов оценивания защищённости киберфизических систем от информационных угроз.

Степень разработанности темы. Проблемные вопросы обеспечения информационной безопасности КФС и оценивания защищённости КФС от информационных угроз освещались в публикациях большого числа исследователей, таких как Р.М. Юсупов, В.Ю. Осипов, И.В. Котенко, И.Б. Саенко, П.Д. Зегжда, Д.П. Зегжда, И.С. Лебедев, А.А. Молдовян, Н.А. Молдовян, A. Gomez, M. Kravchik, M. Elnour, P. Narang и других.

Представленные подходы можно разделить по наиболее часто применяемым исследователями методам. Графовые методы анализа в задачах мониторинга ИБ КФС представлены в работах П.Д. Зегжды, Д.П. Зегжды, Е.Ю. Павленко, Д.С. Лавровой. Анализ самоподобия процессов КФС – в работах И.В. Котенко, И.Б. Саенко, Д.П. Зегжды. Методы машинного обучения, используемые в качестве инструмента классификации, широко представлены в работах И.В. Котенко, В.А. Десницкого, А.В. Мелешко, A. Gomez, M. Kravchik, M. Elnour и ряде других.

Анализ отечественных и зарубежных работ показал, что, как правило, оценивание защищённости КФС является многоэтапным процессом, которому предшествует построение модели угроз исследуемой КФС и этап выделения информативных признаков, производимый на основе данных обучения. Базовой составляющей процесса мониторинга является классификация, опционально включающая процессы постобработки результатов. Стоит отметить, что при всей высокой значимости полученных научных результатов имеется ряд вопросов, которые остаются недостаточно исследованными.

Целью диссертационной работы является повышение полноты и точности обнаружения нарушений информационной безопасности киберфизических систем за счёт выделения наиболее информативных анализируемых признаков и использования в системе мониторинга информационной безопасности значений

временных рядов за предшествующие моменты времени с применением весовых коэффициентов значимости.

Цель работы достигается совокупным решением следующих **частных задач**:

- определение угроз информационной безопасности, характерных для различных типов КФС, и разработка модели угроз ИБ объектов исследования;
- разработка алгоритма, способного из доступного числа параметров КФС выделить наиболее информативные для данной КФС и использовать их для формирования признакового описания состояния ИБ КФС;
- разработка метода оценивания состояния ИБ элементов КФС, основанного на применении ансамбля параллельно работающих классификаторов и весовых коэффициентов Фишберна в качестве постобработки результатов классификации;
- разработка методики идентификации состояния ИБ КФС на основе предложенных метода и модели с использованием машинного обучения при анализе значений временных рядов от наиболее информативных источников;
- разработка прототипа программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз на основе анализа временных рядов;
- количественное сравнение полученных в диссертационной работе результатов с результатами других исследователей.

Объектом исследования являются КФС, в отношении которых осуществляются деструктивные информационные воздействия.

Предметом исследования являются модели оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов.

Научную новизну диссертационной работы составляют:

1. Модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем,

отличающаяся от известных применением анализа главных компонент для вычисления информативности признаков и выделения списка параметров, характеризующих состояние ИБ отдельных элементов КФС.

2. Метод оценивания состояния ИБ элементов КФС, отличающийся от существующих комбинированным подходом, сочетающим применение в системе управления событиями информационной безопасности ансамбля параллельно работающих классификаторов и весовых коэффициентов Фишберна при анализе совокупности информативных признаков, полученных из временных рядов, характеризующих функционирование КФС.

3. Методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС, отличается от существующих применением разработанных модели и метода и позволяет повысить скорость идентификации состояния ИБ элементов КФС без существенной потери точности за счёт уменьшения размерности обрабатываемых данных и идентификации состояния ИБ на основе решающего правила, учитывающего значения временных рядов, полученные за предшествующие моменты времени.

Теоретическая и практическая значимость работы. Разработанные модель, метод и методика представляют собой научно-методическую основу, практическая реализация которой позволяет осуществлять мониторинг состояния КФС, находящихся под воздействием информационных угроз. Разработанная методика может применяться в качестве апостериорного анализа, который помогает восстановить ход распространения инцидента ИБ и в дальнейшем вырабатывать защитные меры, минимизирующие риски подобных инцидентов в процессе дальнейшей эксплуатации. При этом повышается оперативность, точность и полнота оценивания защищённости ИБ КФС, что позволяет на практике эффективно применять разработанный подход в системах мониторинга событий информационной безопасности.

Методология представленного исследования заключается в постановке и формализации частных задач, связанных с разработкой модели формирования информативных признаков, метода анализа временных рядов, составленных из значений, получаемых из сетевого трафика КФС и методики оценивания защищённости на основе разработанных алгоритмов.

Методы исследования. При решении поставленных задач использовались положения теории информационной безопасности информационных систем, методы математической статистики, включая метод анализа главных компонент для вычисления информативности признаков, описывающих состояние информационной безопасности КФС, теория предпочтений для формирования соответствий элементов анализируемых временных рядов с весовыми коэффициентами значимости, методы машинного обучения для решения задач классификации состояний ИБ, методы математического моделирования для построения формализованных моделей исследуемых объектов и протекающих в них информационных процессов.

На защиту выносятся следующие положения:

1. Модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем.
2. Метод оценивания состояния ИБ элементов КФС, основанный на комбинированном подходе применения параллельно работающего ансамбля классификаторов и весовых коэффициентов Фишберна при анализе совокупности наиболее информативных признаков.
3. Методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС.

Соответствие диссертации паспорту научной специальности. Представленные результаты соответствуют паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Обоснованность и достоверность результатов диссертационной работы подтверждается результатами вычислительных экспериментов, их сравнением с результатами других исследователей, практической апробацией разработанной методики и одобрением основных положений диссертации на научно-технических конференциях, публикациями в ведущих рецензируемых журналах, внедрением результатов работы.

Апробация результатов исследования. Основные результаты диссертации публично представлялись на следующих всероссийских и международных конференциях:

- The 11th conference on Internet of Things and Smart Spaces ruSMART, 2018 г.;
- 27-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», 2018 г.;
- XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)», 2018 г.;
- 28-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», 2019 г.;
- The 4th International Conference on Interactive Collaborative Robotics, 2019 г.;
- The 12th conference on Internet of Things and Smart Spaces ruSMART, 2019 г.;
- XI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2019)», 2019 г.;
- The 13th conference on Internet of Things and Smart Spaces ruSMART, 2020 г.;
- The 5th International Conference on Interactive Collaborative Robotics, 2020 г;
- 29-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», 2020 г.

Внедрение результатов работы.

Результаты, полученные в диссертации, были внедрены в рамках выполнения следующих НИР: Проект по программе Президиума РАН № 0073-2018-0007 «Разработка масштабируемых устойчивых алгоритмов построения семантических моделей больших данных и их использование для решения прикладных задач кластеризации и машинного обучения», 2018, 2019 гг.; Проект по программе Президиума РАН № 0073-2018-0008 «Теория и распределенные алгоритмы самоорганизации группового поведения агентов в автономной миссии», 2018, 2019 гг., НИОКТР № 0073-2019-0001 «Теоретические основы и алгоритмические модели когнитивного управления, взаимодействия и анализа состояния групп гетерогенных робототехнических комплексов», 2019, 2020 гг. Результаты исследования использовались при разработке информационных систем в компании АО «НПК «ТРИСТАН».

Публикации по теме диссертации. По научным результатам диссертационного исследования автором опубликовано 29 работ, в том числе 11 публикаций в журналах из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук», одна из статей в указанном перечне опубликована без соавторов, 9 публикаций в изданиях, индексируемых в Scopus и Web of Science, одно свидетельство о государственной регистрации программы для ЭВМ (РОСПАТЕНТ), зарегистрировано без соавторов.

Опубликованы статьи в следующих журналах из перечня ВАК при Министерстве науки и высшего образования РФ:

- «Научно-технический вестник информационных технологий, механики и оптики»;
- «Проблемы информационной безопасности. Компьютерные системы»;
- «Информационные технологии»;
- «Прикладная информатика»;

- «Информация и космос»;
- «Наукоемкие технологии в космических исследованиях Земли».

Полный перечень публикаций и приравненных к ним работ представлен в приложении 4 диссертации.

Личный вклад соискателя. Результаты по положениям, выносимым на защиту в диссертационной работе получены автором самостоятельно, в частности разработаны модель формирования признакового описания состояния ИБ, метод оценивания защищённости элементов киберфизических систем от информационных угроз, а также методика идентификации состояния информационной безопасности киберфизических систем на основе анализа временных рядов. Самостоятельно разработан и зарегистрирован в установленном порядке прототип программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз на основе анализа временных рядов. Прочие результаты опубликованы самостоятельно и в соавторстве, при этом вклад соискателя в совместных публикациях был решающим.

Структура и объём диссертации. Текст работы состоит из следующих структурных элементов: титульный лист; оглавление; введение; основная часть, включающая четыре главы; заключение; список используемых сокращений; список литературы, содержащий 147 наименований; три приложения, содержащие модель угроз информационной безопасности для различных типов КФС, копии зарегистрированных свидетельств на результаты интеллектуальной деятельности, копии актов внедрения, список публикаций автора по теме диссертации. Общий объем диссертационной работы – 133 страницы. Работа включает в себя 36 рисунков, 16 таблиц.

Краткое содержание работы.

В первой главе дана общая характеристика КФС, приведена модель угроз ИБ при функционировании КФС различного назначения. Дан обзор современных методов оценивания состояния ИБ КФС, проанализированы исследования,

посвященные выявлению нарушений информационной и функциональной безопасности КФС.

Во второй главе описана постановка задачи исследования и разработана модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем, отличающаяся от существующих применением метода главных компонент для вычисления информативности признаков и создания уникального признакового описания состояния ИБ для разных типов КФС или отдельных элементов КФС.

В третьей главе разработан метод оценивания состояния информационной безопасности элементов киберфизических систем и методика, использующая предложенный метод. Приведены схемы и алгоритмы реализации предложенных подходов. Предложенный метод позволяет существенно повысить точность идентификации состояния ИБ элементов КФС как за счёт применения ансамбля параллельно работающих классификаторов, так и с помощью обобщения и взвешенного усреднения результатов идентификации на временном отрезке, сокращая при этом ошибки из-за случайных отклонений параметров функционирования КФС.

Разработанная методика характеризуется большей полнотой идентификации атак и деструктивных воздействий, меньшим временем принятия решения за счёт лишь однократной предобработки исходных данных обучающей и тестовой выборок на этапе формирования информативных признаков и дальнейшем применении классификаторов, работающих параллельно.

В четвёртой главе показана экспериментальная реализация методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов, использующая методы их обработки. Полнота и точность идентификации при применении методики оценена на основе серии экспериментов. Произведено сравнение показателей качества идентификации с результатами других исследователей, применивших различные методы предобработки и последующей классификации

временных рядов, характеризующих функционирование КФС. Выделены ограничения и разработаны практические рекомендации по применению методики для повышения защищённости КФС от внешних воздействий.

Проведенные эксперименты показали выполнимость целей мониторинга инцидентов ИБ, что позволяет применять разработанные модель, метод и методику в качестве дополнительных программных систем мониторинга ИБ КФС.

В заключении приведены основные результаты диссертационной работы и выводы, описаны возможные сценарии применения методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов, а также сформулированы перспективы области исследования.

ГЛАВА 1. Обеспечение информационной безопасности киберфизических систем (КФС)

1.1 Общая характеристика исследуемых объектов

Киберфизические системы (КФС), являясь основой для реализаций множества современных инновационных решений, существенно уязвимы с точки зрения успешных информационных атак, приводящих к критическим сбоям или аномальному функционированию [1, 2]. Реализация Национальной технологической инициативы в Российской Федерации [3], развитие технологий «Индустрии 4.0» привели к включению киберфизических систем в приоритетный список инноваций, являющихся критически важными для защиты национальных интересов [4]. Согласно определению [5] КФС – система, «подразумевающая интеграцию вычислительных ресурсов в физические сущности любого вида» [6].

Основу производственных предприятий «Индустрии 4.0» составляют технологии промышленного Интернета вещей, обеспечивающие работу устройств технологического оборудования – киберфизических систем [7]. В свою очередь, устройства, которые в силу выполняемых и решаемых задач непосредственно взаимодействуют с физическими объектами и процессами называются встраиваемыми устройствами [8].

Встраиваемые устройства используются во многих областях, от промышленной инфраструктуры до применения в быту. Например, программируемые логические контроллеры (ПЛК) используются в промышленных системах управления для контроля электроэнергетических сетей, объектах здравоохранения, химических производственных объектах, нефте- и газоперерабатывающих заводах, в частности [9, 10]. ПЛК соединяются и транслируют данные между системой управления и физическим миром [11]. IoT - встраиваемые устройства находят применение в том числе для управления освещением, контроля доступа в помещения и наблюдения [12]. Как правило, основными требованиями для встраиваемых устройств выступают низкое

энергопотребление, небольшие габариты, и низкая себестоимость, что ограничивает вычислительные мощности подобных устройств.

ГОСТ Р ИСО/МЭК 27000-2012 [13] определяет атаку как попытку уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. Из-за своего широкого распространения КФС становятся перспективной мишенью для проведения различного рода вредоносных атак [14, 15], ведущих к утечке приватной информации или даже катастрофическим сбоям систем [16, 17]. Широко известным примером злонамеренной атаки на ПЛК является «Stuxnet» вредоносное ПО, которое в 2010 году воздействуя на код ПЛК повредило 20% иранских центрифуг, которые управлялись при помощи ПЛК [18].

За последние несколько лет, заражённые вредоносными программами IoT-устройства использовались для проведения распределенных атак типа «отказ в обслуживании» (DDoS). Злоумышленники используют сети, состоящие из зараженных вредоносными программами устройств, таких как подключенные к Интернету бытовая техника и домашние роутеры. Зачастую сами владельцы устройств не знают, что их устройства были скомпрометированы. Подобные устройства являются привлекательными мишенями для вредоносных программ из-за отсутствия криптографического шифрования по умолчанию и слабой аутентификации. В этих атаках в основном задействованы домашние устройства, такие как маршрутизаторы, веб-камеры и принтеры [19]. Расширенное описание угроз ИБ для IoT-устройств можно найти в [20]. Потенциально серьезные последствия атак обуславливают значительный интерес исследователей к информационной и функциональной безопасности КФС.

Рассмотрим более подробно устройство КФС. На рис. 1 показана общая модель КФС, которая включает в себя три базовые категорий компонентов: (1) связь, (2) вычисления и управление и (3) мониторинг и управляющие воздействия. Связь может быть беспроводной [21] или проводной, и она как правило соединяет КФС с системами более высокого уровня, такими как центры управления, или с

компонентами более низкого уровня в физическом мире [22]. Вычислительная и управляющая часть - это то место, откуда отправляются команды управления и принимаются показатели работы с датчиков КФС. Датчик (sensor) - это электронное устройство, которое измеряет физические свойства КФС, такие как скорость, ускорение, температуру [23], вес, звук [24], освещенность [25], контакт, геопозицию, наличие, идентичность, химический состав и т.д. [26].

Компоненты мониторинга [27] и управляющих воздействий соединяют КФС с физическим миром через датчики для мониторинга физических компонентов и исполнительные механизмы для управления ими [28].

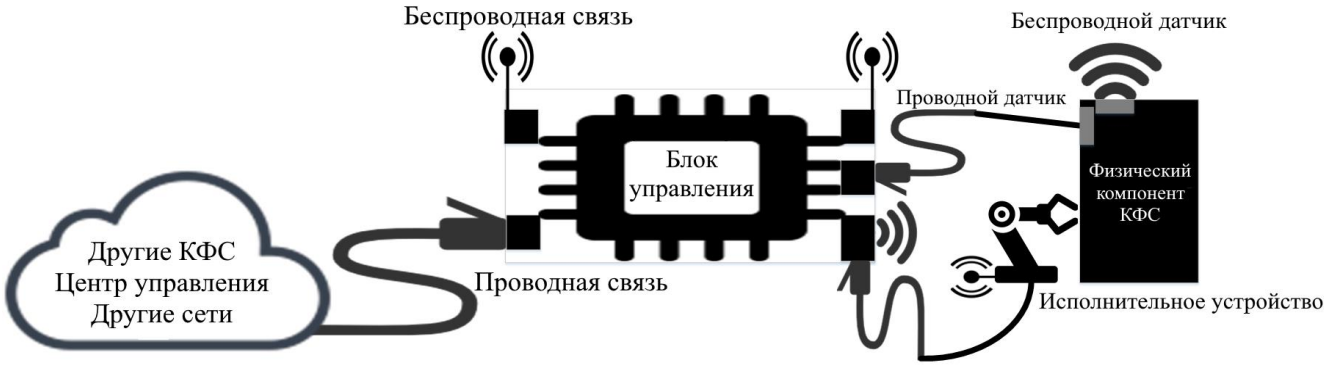

Рисунок 1 – Общая модель КФС

Компонент КФС может связываться с центром управления или другими узлами КФС, а также содержать датчик или механизм для взаимодействия с физическим миром. Каждое из этих взаимодействий имеет различные последствия для ИБ. Например, деструктивные информационные воздействия широко используются злоумышленниками для неожиданных атак с серьёзными физическими последствиями [22, 29]. Имеют место и обратные ситуации, в которых физические взаимодействия с компонентами КФС приводят к подмене информации с датчиков и их передаче в информационную управляющую систему [30].

1.2 Модель угроз информационной безопасности при функционировании КФС

В виду тесной интеграции КФС в производственно-технологические системы, системы критической информационной инфраструктуры, а также значительного количества возможных точек вхождения, задача мониторинга ИБ для КФС является более сложной, по сравнению с классическими информационными системами [31, 32]. В случае реализации угроз ИБ основной целью злоумышленника как правило является получение возможности управления КФС при помощи информационных воздействий [31], при этом деструктивные информационные воздействия могут влиять как на процессы хранения, обработки и передачи информации внутри системы, так и на физические процессы исполнительных механизмов КФС.

Согласно ГОСТ [33] модель угроз ИБ – это описательное представление свойств или характеристик угроз безопасности информации. Понимание потенциальных угроз является одним из ключевых этапов в задаче выявления нарушений ИБ КФС [34]. В свою очередь, модель угроз информационной безопасности содержит совокупность сведений, характеризующих состояние ИБ объекта КФС при возникновении определённых опасных событий, процессов или явлений с учётом их актуальности, возможности реализации и последствий [35]. Внедрение программных и аппаратных закладок возможно на различных этапах жизненного цикла КФС и даже при наличии средств защиты нельзя исключать возможность перехвата и подмены управляющего сигнала [36].

Возможные пути проникновения вредоносного программного обеспечения (ПО) в систему управления КФС приведены на рисунке 2.

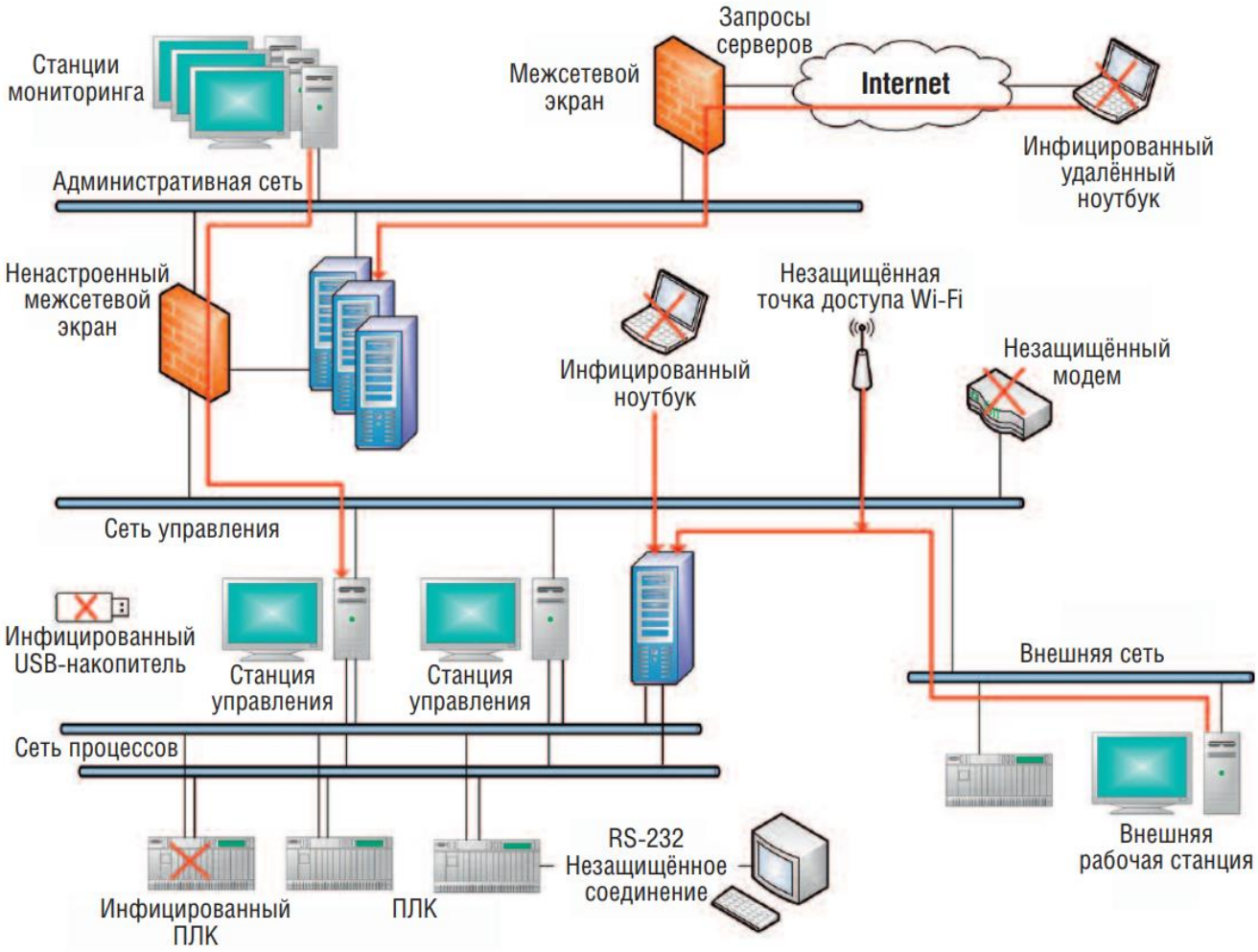

Рисунок 2 – Возможные пути проникновения вредоносного ПО в систему управления КФС

Типовыми угрозами для КФС являются [37]:

- перехват и внедрение данных на уровне взаимодействия между ПЛК КФС;
- модификация данных, поступающих от компонентов КФС;
- перехват управления отдельными устройствами КФС;
- атаки отказа в обслуживании на компоненты КФС;
- подмена таблицы маршрутизации;
- переполнение таблицы маршрутизации;
- ослабление сетевого периметра с помощью бекдоров;
- эксплуатация уязвимостей в используемых протоколах;
- перехват и модификация сетевых сообщений;
- модификация аппаратного и программного обеспечения;

- удаленное выполнение вредоносного кода;
- активация программных и аппаратных закладок;
- подмена и уничтожение данных в каналах связи;
- модификация системного времени;
- нелегитимное внесение изменений в структуру КФС.

На рисунке 3 показаны деструктивные воздействия на элементы КФС на различных уровнях: физическом, сетевом и уровне приложений.

Рисунок 3 – Угрозы на различных уровнях КФС

Из вышеперечисленного перечня основными угрозами для КФС можно считать несанкционированные изменения информации, атаки на её целостность. Как правило, злоумышленник хочет получить доступ к удалённому управлению КФС или прервать работу физической составляющей системы.

Мониторинг состояния информационной безопасности элементов КФС осуществляется на основе совокупности методов оценивания различных факторов:

$$M = <P_i, P_f, P_c>, \quad (1)$$

где:

- P_i – методы оценивания ИБ на основе конфиденциальности целостности и доступности для информационной составляющей КФС;
- P_f – методы оценивания согласованности информационной и физической составляющих с учетом их взаимного влияния друг на друга;
- P_c – методы оценивания влияния информационных атак на систему управления КФС.

При этом, преодоление нарушителем средств защиты информации (СЗИ) приводит к реализации угроз, а, следовательно, нарушению целевых функций КФС.

Данные для осуществления мониторинга (1) формируются из значений характеристик $H = <f_1, f_2, \ldots, f_n>$, составленных из параметров функционирования КФС. Параметры функционирования, поступающие от КФС и формируемые от множества источников, синхронизируются по времени и объединяются во временные ряды. Потоки данных, создаваемые измерительными компонентами, такими как удаленные терминальные блоки диспетчерского управления и сбора данных (SCADA), передают телеметрические данные от элементов КФС в систему обеспечения ИБ. В свою очередь, команды от главной контролирующей системы передаются обратно к подключенным компонентам, реализуя тем самым закрытие процесса контура управления.

Условно можно выделить две большие группы нарушителей [38]:

1) имеющие доступ к КФС;

2) не допущенные к работе с КФС.

Знание источника (субъекта) атаки и существующих уязвимостей значительно сужает круг потенциально возможных нелегитимных точек вхождения в систему и является отправной точкой в определении механизмов атак.

В обзоре [22] для каждой угрозы определены пять факторов: мотив, источник (субъект), цель, вектор атаки и потенциальные последствия.

Рассмотреть всё множество угроз ИБ КФС не представляется возможным из-за огромнейшего разнообразия и значительных отличий архитектур КФС. По приведённому в [22] плану, в рамках диссертации была составлена модель угроз ИБ при функционировании КФС различного назначения для четырёх характеристичных классов: автоматизированных систем управления (АСУ) (приложение 1, таблица 1), «умных» сетей электроснабжения (приложение 1, таблица 2), медицинских устройств (приложение 1, таблица 3), «умных» транспортных средств (приложение 1, таблица 4).

1.3 Аудит информационной безопасности КФС

Для киберфизических систем понятие информационной безопасности расширяется, дополняя традиционную концепцию обеспечения целостности, конфиденциальности и доступности циркулирующей в них информации [39, 40], необходимостью поддержания корректного функционирования КФС в условиях деструктивных информационных воздействий [41]. На рисунке 4 представлена модель информационно-функциональной безопасности КФС.

Рисунок 4 – Модель информационно-функциональной безопасности КФС

Управление рисками является важной задачей аудита информационной безопасности КФС. В КФС на ранних этапах проектирования не уделялось

должного внимания рискам нарушений ИБ [42]. С распространением применения КФС интенсивность передачи данных и обмена трафиком серьёзно увеличивалась [43]. Получение доступа к управлению КФС неавторизованными пользователями и другие злонамеренные атаки могут привести к раскрытию конфиденциальных данных и вызвать ряд других серьезных проблем ИБ.

Стандарты оценивания рисков ИБ КФС. Стандарт NIST (SP) 800–82 [44] описывает комплексный подход для защиты АСУ, одновременно рассматривая требования к производительности, надежности и информационной безопасности. Система CSF (Cybersecurity Framework) [45], которая направлена на повышение безопасности критической инфраструктуры страны от атак, устанавливает основанный на оценке риска подход к управлению рисками и снижению рисков ИБ для критической инфраструктуры. IEC 62351 [46] является отраслевым стандартом, направленным на повышение ИБ операций управления энергосистемами. В настоящее время стандарт содержит 11 частей, в которых описаны меры безопасности для аутентификации, целостности, конфиденциальности и контроля доступа.

Согласно [33] угроза информационной безопасности определяется как совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Риск нарушения информационной безопасности – возможность реализации угрозы [47]. Нахождение КФС под угрозой можно выявлять при помощи мониторинга функционирования системы [48].

Инцидент информационной безопасности – это появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности [49].

Риски ИБ вызваны взаимодействиями внутри КФС, между КФС и окружением, а также между КФС и авторизованными пользователями. Как было сказано выше, конфиденциальность, целостность и доступность, представляют

собой фундаментальные цели безопасности в информационных системах (ИС) и КФС. В отличие от традиционных информационных систем, обеспечение доступности является наиболее важной задачей в КФС. Таблица 1 показывает, что приоритеты фундаментальных целей в КФС и ИС не совпадают [50, 51].

Таблица 1 – Приоритет между основными целями ИБ в КФС и ИС

Приоритет	**КФС**	**ИС**
высокий	доступность	конфиденциальность
средний	целостность	целостность
низкий	конфиденциальность	доступность

Оценка рисков и управление ими направлены на выявление активов, анализ уязвимостей, а также измерение возможных убытков [52]. В целом, можно разделить оценку рисков на качественную и количественную. Качественная оценка в значительной степени опирается на опыт экспертов, в то время как количественная оценка определяет точное значение величины риска КФС.

Традиционные технологии ИБ информационных систем также адаптируемы для защиты КФС, например, брандмауэр и технология обнаружения вторжений. КФС должна иметь индивидуальный межсетевой экран, который поддерживает идентификацию и анализ состояния информационной безопасности в реальном времени. Когда наблюдается аномальный трафик или неавторизованный доступ срабатывают правила фильтрации с целью обеспечения ИБ. Угрозы КФС, происходящие из киберпространства в основном непредсказуемы [53]. Традиционная теория надежности и технологии отказоустойчивости полностью не могут предотвратить сбой или даже отказ работы КФС. Технология обнаружения вторжений признает наличие системных уязвимостей и предполагает, что некоторые уязвимости могут быть использованы злоумышленниками, стремящимися получить доступ к управлению КФС. Исследования технологии обнаружения вторжений должны уделять больше внимания уменьшению потерь от атакованной КФС и восстановлению целевой функции системы.

С углублением интеграции между информационными технологиями и индустриализацией количество объектов и масштаб сети значительно увеличиваются, а защита ИБ во всем жизненном цикле КФС становится гораздо более сложной задачей. Стратегия совместного управления, основанная на технологии блокчейн, стала новой перспективной областью ИБ. Технология блокчейн обеспечивает отказоустойчивость и поддерживает целостность, согласованность, аутентичность и невозможность отказа от хранимых и передаваемых данных, что представляет собой технологию распределённого однорангового общего интеллектуального регистра, основанную на криптографии. Блокчейн-технология может применяться для идентификации, аутентификации, децентрализованных сетей промышленных площадок, ИБ больших промышленных данных «интеллектуальных производств». В настоящее время существует много проблемных вопросов в стандартах блокчейн. Исследования, основанные на блокчейн, выявление новых вычислительных структур и структур хранения данных, а также облегченных методов защиты формируют новое отдельное направление исследований для обеспечения безопасности в интеллектуальных производственных КФС.

В то же время, многие методологии оценки рисков ИБ хорошо разработаны для КФС, среди которых:

- анализ дерева отказов;
- анализ причин и последствий отказов;
- анализ угроз технологических процессов;
- инженерное моделирование;
- системно-теоретический анализ процессов;
- подходы на основе байесовских сетей.

Анализ дерева отказов: анализ дерева отказов [54] является самой ранней технологией в оценке рисков безопасности, а также графическим методом, широко используемым для оценки угроз и рисков в КФС. Сущность метода заключается в представлении возможных нормальных и аномальных событий, которые могут

вызвать нежелательное событие верхнего уровня. Дерево отказов состоит из следующих компонентов: узлы (нежелательные события в системе), элементы (отношения между узлами; могут быть «И» или «ИЛИ») и ребра (путь нежелательных событий через систему). Анализ дерева отказов эффективно используется в КФС критической инфраструктуры, связанных с высокой степенью риска. На рис. 5 показана схема построения простого дерева отказов.

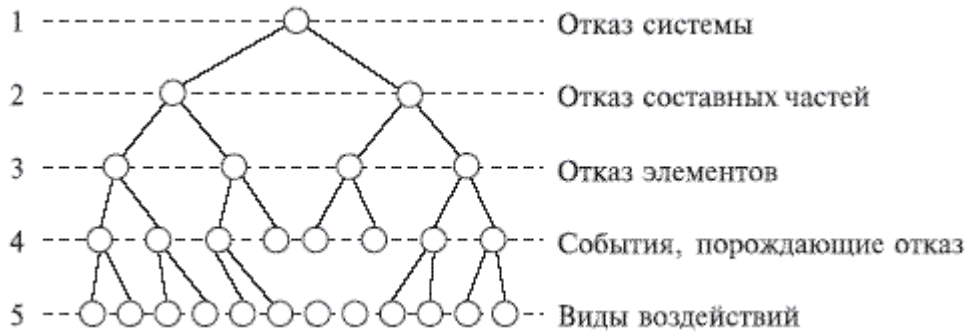

Рисунок 5 – Условная схема построения дерева отказов КФС

Анализ причин и последствий отказов - это структурированный метод анализа безопасности КФС, позволяющий распознавать и оценивать потенциальные отказы системы и их последствия. В количественном анализе вычисляется значение приоритета риска, которое является произведением вероятности возникновения и вероятности обнаружения риска [55]. В работе [56] предложена модификация метода на основе вероятностного подхода, при помощи которой можно определить, происходит ли сбойный режим с вероятностью, превышающей допустимый порог. Анализ причин и последствий отказов выполняется на ранней стадии жизненного цикла КФС [57].

В промышленности широко применяется метод анализа угроз технологических процессов (HAZOP) [58] для изучения не только нарушений ИБ КФС, но и проблем работоспособности КФС путем изучения последствий любых отклонений от запланированных состояний ИБ. Метод позволяет идентифицировать, как процесс отклоняется от проектных состояний ИБ и переходит в небезопасные состояния ИБ, путём определения возможных рисков и потенциальных уязвимостей на объектах КФС [59].

Инженерное моделирование [60]: - это метод разработки поведенческих моделей систем, работающих в реальном времени и анализа моделей с целью обеспечения безопасности КФС. Метод анализирует архитектуру системы для определения набора наиболее информативных признаков, после чего извлекает признаки через различные каналы физической среды при помощи внутренних или внешних датчиков через узлы системы и киберфизические взаимодействия и, наконец, анализирует абстрактную модель для оценивания ожидаемых признаков состояния ИБ и выявления небезопасного функционирования системы.

Системно-теоретический анализ процессов. Упомянутые выше традиционные методы анализа рисков было трудно адаптировать во многих киберфизических системах со сложным программным обеспечением, поэтому был предложен системно-теоретический анализ процессов (СТАП) [61]. КФС представляется при помощи иерархической структуры управления. Взаимодействия между каждым уровнем структуры управления обеспечивают необходимые ограничения на поведение компонентов на следующем нижнем уровне, эти ограничения влияют на поведение всей системы. Работа на каждом уровне этой структуры управления основана на контуре управления с обратной связью. Цель СТАП достигается путем выявления сценариев аномальных ситуаций. Метод индифферентен к виду воздействий на систему.

Подходы на основе байесовских сетей. Унифицированная структура оценивания рисков [62] была предложена в сетях диспетчерского управления и сбора данных (SCADA), подход объединяет дерево атак, дерево ошибок и дерево событий для построения модели байесовской сети (БС). Часть методов количественного оценивания состояния ИБ КФС основана на опыте и знаниях экспертов. Подходы такого типа могут корректировать параметры модели из ограниченных данных путем самообучения и динамически оценивать риски при известных или неизвестных атаках. В связи с отсутствием большого количества данных был представлен подход нечётко-вероятностной БС для динамической оценки рисков ИБ в АСУ [63]. Сложность структуры КФС создает некоторые

проблемы для оценки рисков ИБ, но БС может легко описать взаимозависимости между сетевыми компонентами. В работе [29] модель нечётко-вероятностной БС используется для анализа и прогнозирования рисков ИБ, алгоритм нечеткого приближенного динамического вывода нацелен на динамическую оценку рисков ИБ. В работе [64] показан новый мультимодельный подход к прогнозированию инцидентов и оценке рисков динамической ИБ промышленных систем управления. Их метод также основан на многоуровневой байесовской сети. Основанный на активах динамический подход оценки воздействия был представлен в [65] для анализа риска в АСУ. Этот подход состоит из двух частей: динамическая и объектно-ориентированная модель активов и модель распространения воздействия кибератаки [66-68]. Модель активов строится на основе сетей Петри, которые являются инструментом графического и математического моделирования [69-71].

1.4 Исследования, посвященные выявлению нарушений информационной безопасности (ИБ) и идентификации состояния ИБ КФС

На сегодняшний день имеется множество работ отечественных и зарубежных исследователей, посвященных разработке методов, методик и систем обнаружения нарушений ИБ КФС [72-74]. Существенная часть исследователей рассматривает вопросы выявления аномалий ИБ КФС [75], которые могут быть вызваны атаками злоумышленников [76], например, внедрением программных закладок в КФС [77]. В литературе описано достаточно математических методов, при помощи которых можно классифицировать аномалии, среди которых метод опорных векторов [78], скрытые марковские модели (СММ) [79], искусственные нейронные сети (ИНС) [80] и другие [81, 82].

В работе [83] предлагается метод выявления аномалий ИБ в КФС водоснабжения, основанный на машинном обучении. Исходные данные для машинного обучения были получены на разработанном программно-аппаратном прототипе системы водоснабжения с использованием ряда микроконтроллеров, датчиков и исполнительных механизмов. Было протестировано несколько методов машинного обучения из библиотеки scikit-learn языка программирования Python. В

результате экспериментов исследователи определили метод обучения и его параметры, обеспечивающие лучшую точность распознавания аномальных состояний ИБ. Точность на построенном наборе данных при использовании алгоритма *k*-NN составила 0,83-0,87 и зависела от параметра модели *k*.

Авторы подхода, описанного в работе [84], разработали программу [85], анализирующую временные ряды, описывающие функциональное состояние КФС. Программа получает на вход временной ряд и значение погрешности, в рамках которой допускается отклонение показателя Херста от значений, характерных для самоподобных процессов. После расчета показателя выполняется проверка на предмет вхождения полученного результата в разрешённый диапазон и на основе этого делается вывод о возможной аномалии в КФС.

Обнаружению деструктивных воздействий на физическую составляющую КФС посвящена работа [86]. Эксперимент заключался в использовании системы, анализирующей изменения значений напряжения от переключателей, оборудованных «умными» датчиками. Недостатком предложенного авторами подхода является игнорирование существования информационной составляющей КФС. При такой постановке задачи не будут обнаружены атаки на целостность и конфиденциальность данных, если они не вызывают скачков напряжения.

В свою очередь, статистический анализ позволяет эффективно обнаруживать аномалии, так как контролируемые КФС имеют суточные шаблоны поведения [87], что отражается не только в физических, но и в информационных процессах КФС. Вышеуказанный подход также является широко распространенным методом обнаружения небезопасного функционирования программной части КФС [88]. В работе [89] вычисляется расстояние Махаланобиса между статистическими распределениями обучающей и тестовой выборки, после этого становится возможным отличить разрешённый (известный) код от запрещённого (неизвестного). Для этих же целей можно применить критерий Колмогорова-Смирнова [90]. Методы статистического обнаружения хорошо работают без заранее известной информации об устройствах. Стоит отметить, что эффективное

обнаружение аномалий функционирования КФС требует не только корректной идентификации самих состояний ИБ, но и разрешённой последовательности их проявлений.

Применение коэффициента Хёрста для отслеживания состояния информационной безопасности отдельных компонентов КФС, описано в работах [91-93]. При уменьшении вышеуказанного коэффициента появляется возможность судить о потенциальных вмешательствах в работу системы и её нахождении в небезопасном состоянии. При этом, используется критерий самоподобия информационных или физических процессов КФС.

Авторами работы [94] предложен метод выявления атак на КФС во время их функционирования, основанный на киберфизическом контроле доступа. Недостатком предложенного метода является высокая нагрузка на вычислительную систему КФС, что может быть крайне нежелательно в устройствах с ограниченными ресурсами. Похожий метод используется в работе [95], он основан на контроле пакетов трафика, передаваемых между различными модулями КФС и не вызывает большой дополнительной нагрузки, но его способность обнаруживать аномалии функционирования сильно ограничена.

В основном, работы современных исследователей сосредоточены на анализе либо функциональной [96-98] либо информационной [99-103] компоненты КФС, при этом отсутствуют сложившиеся комплексные подходы обеспечения ИБ с учётом всех особенностей КФС, как объекта защиты от информационных угроз.

В работах [104, 105] классификация состояния ИБ осуществляется на основе сравнения текущих временных рядов сигналов с профилем нормального поведения. Для создания подобного профиля даже для отдельного компонента КФС необходим учёт значительного числа показателей, поэтому к недостаткам предложенного подхода можно отнести низкую эффективность для крупномасштабных КФС [106].

В источнике [107] авторы предлагают метод одновременного мониторинга информационной и функциональной безопасности КФС. К недостаткам данного подхода следует отнести его применимость только к КФС с небольшим количеством элементов и выполняемых функций.

В значительном количестве работ авторы используют методы на основе искусственных нейронных сетей, к таким исследованиям можно отнести работы [108-110].

Готовым программным решением, направленным на обеспечение защищённости КФС критической инфраструктуры, является ПО, созданное «Лабораторией Касперского» для автоматизированных систем управления технологическим процессом (АСУ ТП) [111] – Kaspersky Industrial CyberSecurity (KICS) [112]. Работа ПО основана на оценке целостности контролирующей системы и сигнатурном анализе. К зарубежным аналогам Kaspersky Industrial CyberSecurity (KICS) отечественных программных продуктов можно отнести разработки Microsoft и Symantec [113, 114].

1.5 Выводы по главе 1

В первой главе дана общая характеристика КФС, приведена модель угроз ИБ при функционировании КФС различного назначения. Дан обзор современных методов оценивания состояния ИБ КФС, проанализированы исследования, посвященные выявлению нарушений информационной и функциональной безопасности КФС.

Исходя из анализа современных исследований и коммерческих решений, можно сделать вывод о том, что в настоящее время в мире отсутствуют сложившиеся комплексные подходы, направленные на выявление нарушений ИБ систем, реализующих информационные и физические процессы одновременно.

Появление отказов, сбоев отдельных объектов КФС из-за информационных угроз может быть вызвано не только наличием ошибок, но и внедрёнными на различных этапах жизненного цикла программными и аппаратными закладками,

которые могут влиять на работу встроенной внутренней системы защиты. В связи с этим, возникает необходимость разработки дополнительных независимых средств идентификации состояния ИБ, анализирующих состояние ИБ системы по внешним и внутренним каналам на основе временных рядов, объективно отражающих вышеуказанное состояние системы.

Возможность обнаружения изменений является гибким подходом для выявления нарушений ИБ, поскольку не требуется знать природу вредоносного кода или несанкционированного физического воздействия, а необходимо идентифицировать состояние ИБ и передать информацию об изменении в работе системы.

Существующие методы и подходы имеют следующие недостатки:

- Большинство исследовательских методов не в состоянии различить природу происхождения выявленных нарушений ИБ. Нельзя с достаточной долей вероятности сделать вывод о том, вызваны ли выявленные аномалии случайными инцидентами или злонамеренными атаками. Стоит отметить, что на данный момент нет единого мнения о том, действительно ли воздействия различных типов на КФС необходимо дифференцировать по природе происхождения или их следует объединять с точки зрения системного теоретического анализа.
- КФС представляют собой систему, работающую в реальном времени, поэтому должно проводиться динамическое выявление нарушений ИБ.

Таким образом, можно сделать вывод об объективной необходимости разработки соответствующих методов для устранения вышеописанных недостатков.

ГЛАВА 2. Разработка модели формирования признакового описания состояния информационной безопасности элементов киберфизических систем

2.1 Задача системы идентификации состояния ИБ КФС

Атакующие воздействия на элементы КФС требуют, как правило, наличия открытых коммуникационных интерфейсов для осуществления взаимодействия с элементами системы. Потенциальными угрозами являются возможность заражения вредоносным ПО через Интернет и внутренние сети, несанкционированное управление КФС при помощи облачных технологий в рабочем и производственном процессе, и т.д. Формирование инцидента свидетельствует о наличии действий атакующего, направленных на нарушение одного или нескольких требований информационной безопасности.

Деструктивные информационные воздействия на КФС $V = <v_1, v_2, \ldots, v_n>$ оказывают влияние на процессы хранения, обработки и передачи данных. Предполагается, что предлагаемые методы на основе анализа временных рядов должны обеспечивать мониторинг целевых процессов как на физическом, так и на программно-информационном уровне — в части хранения, обработки и передачи информации (рисунок 6).

Рисунок 6 – Место предлагаемых методов идентификации состояния ИБ КФС

Контролирующие воздействия вызывают определенные изменения, фиксируемые на основе различных каналов получения информации от исследуемых объектов [115-118]. При формировании модели безопасного функционирования в условиях воздействия угроз ИБ необходимо учесть, что КФС характеризуется протеканием множества информационных процессов, следствием осуществления которых являются различные внешние и внутренние сигналы.

Выбор каналов для формирования модели оценивания защищённости исследуемых объектов от информационных угроз обосновывается возможностью предсказания по вышеуказанным каналам заранее смоделированных деструктивных воздействий, при этом дисперсия исходных данных является

первичным критерием их отбора. Предлагаемая модель не связана с конкретным типом и архитектурой КФС, поскольку показатели протекания процессов нормируются и приводятся к единому масштабу.

Несмотря на свою разнородность КФС можно рассмотреть по уровням в виде отдельных составных частей [119] (рисунок 7):

- прикладное программное обеспечение;
- операционная система;
- аппаратная часть;
- мехатронная часть.

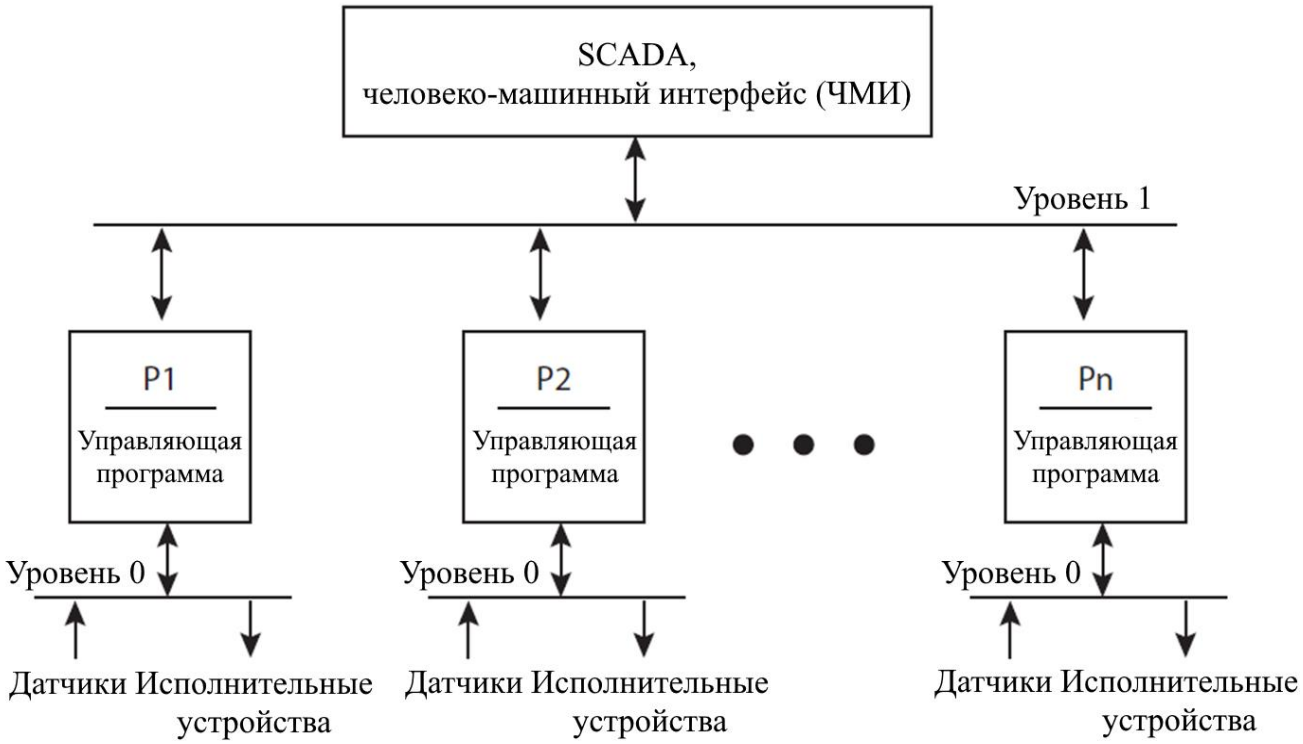

Рисунок 7 – Уровни управления КФС

Такое представление позволяет осуществлять анализ групп данных, получаемых по различным каналам [120]. В зависимости от выполняемых команд, взаимодействия узлов между собой, воздействия внешней среды будет происходить изменение сигналов, которые можно получить, как по внешним, так и по и внутренним каналам.

Сигналы, формируемые от датчиков или получаемые от внутренних программно-аппаратных модулей, объединяются во временные ряды. Для целей

выявления нарушений ИБ КФС удобно использовать временные ряды, составленные из параметров функционирования КФС и отражающие состояние ИБ системы или её отдельных элементов [121]. Процесс выявления аномалий основан на том, что изменения этих сигналов показывают отклонения от разрешённых (безопасных) режимов работы. Система выявления нарушений ИБ разрешает конфликт между легитимным и нелегитимным контурами управления [122] (рисунок 8) и содержит модели различных разрешённых и неразрешённых режимов функционирования КФС, а также вычислительный модуль для принятия решений.

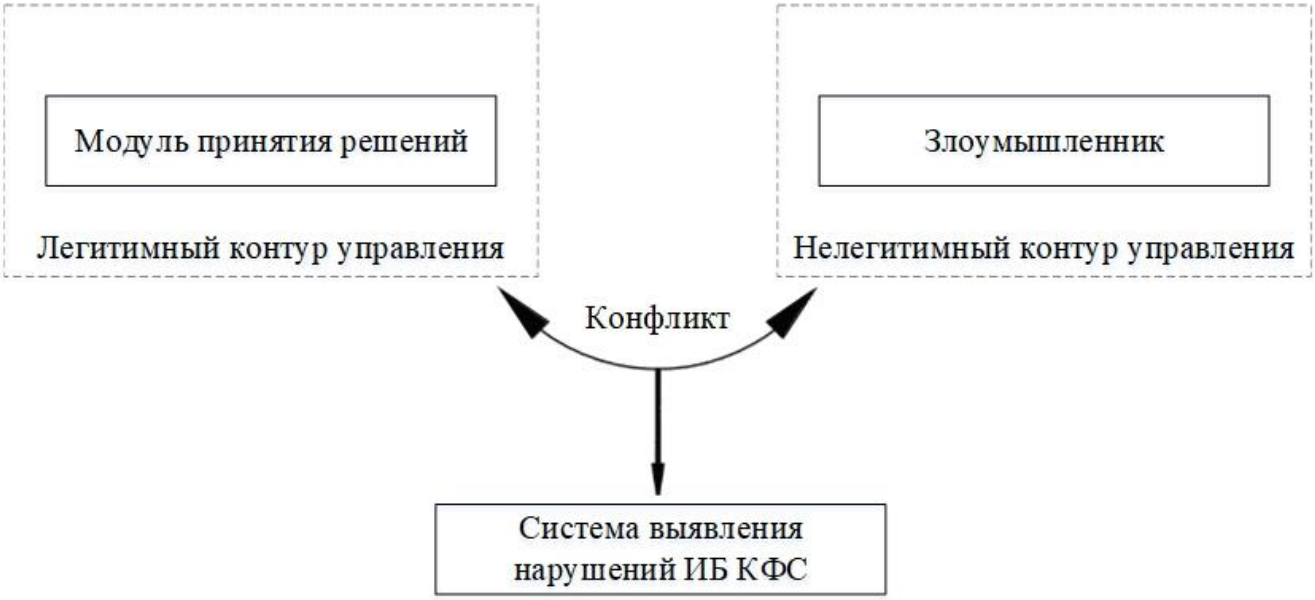

Рисунок 8 – Задача системы выявления нарушений ИБ КФС

2.2 Постановка задачи исследования

Научная задача диссертационной работы состоит в разработке методов повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз.

КФС реализует заранее определённые её структурными и техническими особенностями функции и представляет собой замкнутую систему, в которой протекает конечное множество информационных и физических процессов. Предполагается, что существует множество объектов обучающей выборки $\{o_1, \ldots, o_m\} = \{\{x_1(t_1), x_2(t_1), \ldots, x_n(t_1)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\} \subset X$, составленных из временных рядов, отражающих состояние ИБ КФС или её отдельных элементов, множество меток классов состояний ИБ $\{C_0, C_1\} \subset C$. Требуется построить

алгоритм μ, способный соотнести элементы множества X с одним из известных классов, соотнесённых с состоянием ИБ:

$$\mu: X \rightarrow C, \tag{2}$$

где: C_0 – множество меток классов безопасных состояний ИБ КФС, C_1 – множество меток классов аномальных (опасных) состояний ИБ, $\{c_1, c_2, \ldots, c_k\} \subset C_0$, $\{c_{k+1}, c_{k+2}, \ldots, c_l\} \subset C_1$, l – число идентифицируемых состояний ИБ КФС, m – число объектов в обучающей выборке.

Универсальным способом представления динамически изменяющихся данных являются временные ряды [123, 124]. Временной ряд X – это собранный в разные моменты времени статистический материал о значении каких-либо параметров исследуемого процесса [125] КФС. $X = \{x(t_1), x(t_2), \ldots, x(t_m)\}$, полученные значения являются следствием протекания процессов КФС. Оценивание защищённости киберфизических систем от информационных угроз на основе анализа временных рядов можно свести к задаче классификации их элементов и выявлению значений, относящихся к небезопасному классу C_1. Обилие в КФС циклических (повторяющихся) процессов определяет успешную применимость предлагаемого подхода. В исследуемой задаче формируется m элементов временных рядов $X = \{\{x_1(t_1), x_2(t_1), \ldots, x_n(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_n(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\}$, представляющих собой сгруппированные и синхронизированные по времени множества значений сигналов от n источников.

Таким образом, метка класса состояния ИБ КФС в дискретный момент времени t должна определяться как:

$$c(t) = \mu(x_{1,t}, x_{2,t}, \ldots, x_{s,t}),\ c \in C,\ x_{i,t} \in D_f,\ s << n, \tag{3}$$

где: C – множество меток классов (состояний ИБ КФС), t – метка времени, $t = 1,\ldots, m$, D_f – множество допустимых значений признака, s – количество отобранных наиболее информативных признаков.

2.3 Модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем

Исходное признаковое пространство $H = (f_1, f_2, \ldots, f_n)$ представляет собой набор возможных параметров функционирования КФС, которые могут включать в себя как характеристики информационных процессов (например, параметры сетевого трафика), так и данные о протекающих физических процессах (например, информацию с датчиков). Очевидно, что крайне важным является выявление признаков, позволяющих достичь максимальной полноты и точности идентификации.

Задача формирования признакового описания состояния ИБ элементов КФС требует произвести оценку информативности источников системы мониторинга ИБ КФС. Существуют два основных подхода к оцениванию информативности: энергетический и информационный. В случае энергетического подхода наиболее информативными будут являться признаки, чьё абсолютное значение наибольшее. Очевидно, что из-за различной физической природы величин, формируемых системой мониторинга КФС данный подход в решаемой задаче не принесёт удовлетворительных результатов. В случае же информационного подхода информативность оценивается по величине достоверного различия между классами состояний ИБ в пространстве признаков.

Наилучшим подходом для оценивания информативности признаков в задаче идентификации состояния ИБ КФС, является информационный подход, который позволяет производить отбор признаков, обладающих максимальной дискриминаторной способностью для защищаемого типа КФС.

Метод анализа главных компонент (МГК) широко используется для понижения размерности исходных данных. В большинстве исследований [126] МГК применяется в качестве предобработки, в этом случае исходное многомерное признаковое пространство преобразуется в пространство главных компонент (ГК), в настоящей диссертации в отличие от известных работ МГК предлагается

использовать с целью вычисления информативности каждого признака (источника информации о процессах системы).

На практике различные физические величины, характеризующие функционирование КФС имеют разный диапазон представленных в обучающей выборке значений и разложение в большей степени зависит от параметров с бóльшими диапазонами. Значения различных параметров, характеризующих функционирование и информационные процессы КФС, могут отличаться на несколько порядков, при этом переменные с большим разбросом характеризуется большей дисперсией и, следовательно, имели бы больший вес в МГК, связанный с типом измеряемой переменной [127]. Для того, чтобы вклад переменной, и её информативность оценивалась вне зависимости от типа измеряемого параметра производится выравнивание разброса значений путём центрирования и нормировки (рисунок 9).

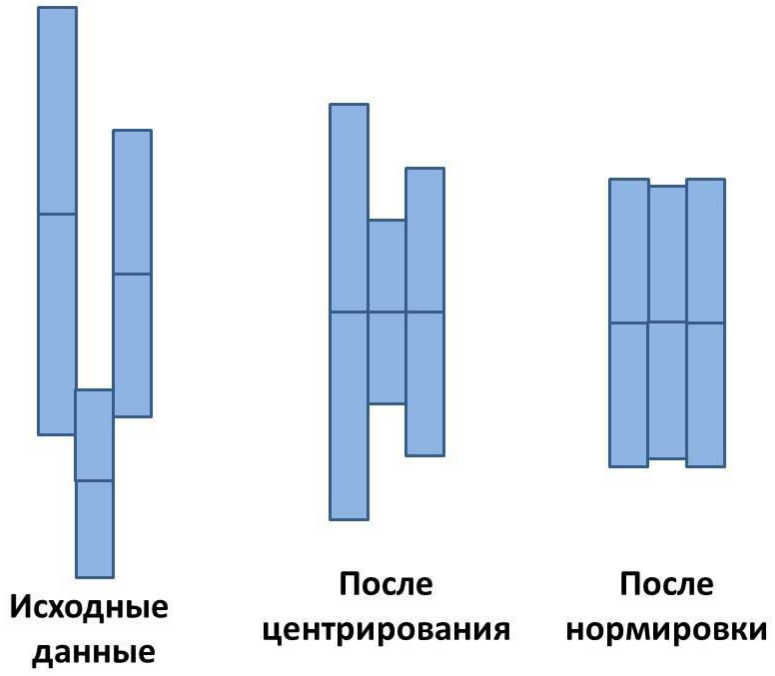

Рисунок 9 – Предобработка исходных данных

Матрица данных **X** представляет собой результаты измерения некоторых параметров объекта КФС во времени:

$$\mathbf{X} = \begin{pmatrix} x_1(t_1) & x_2(t_1) & \dots & x_{\mathrm{n}}(t_1) \\ x_1(t_2) & x_2(t_2) & \dots & x_{\mathrm{n}}(t_2) \\ \dots & \dots & \dots & \dots \\ x_1(t_m) & x_2(t_m) & \dots & x_{\mathrm{n}}(t_m) \end{pmatrix}, \quad (4)$$

где m – количество векторов данных (число строк), n – исходная размерность пространства данных (число столбцов).

Центрированием называют вычитание из каждого столбца x_j среднего (по столбцу) значения m_j [128]:

$$m_j = \frac{x_{1,j} + x_{2,j} + \dots + x_{n,j}}{n} \quad (5)$$

Вторым преобразованием исходных данных является нормировка. Данная процедура выравнивает вклад разных переменных МГК-модель. При этом преобразовании каждый столбец x_j делится на свое стандартное отклонение s_j [129].

$$s_j = \sqrt{\frac{\sum_{i=1}^{n}(x_{i,j} - m_j)^2}{n}} \quad (6)$$

Комбинацию центрирования и нормировки по столбцам называют автошкалированием.

$$\widetilde{x_{i,j}} = \frac{x_{i,j} - m_j}{s_j} \quad (7)$$

Таким образом, перед применением МГК для анализа обучающей выборки КФС, необходимо произвести автошкалирование (центрирование и нормировку) данных. Каждая строка вышеуказанной матрицы **X**, в данном случае, – матрица временных рядов предобработанных данных, составленных из параметров, надёжно описывающих состояние ИБ КФС.

Разложение матрицы **X** в виде матричного уравнения при помощи метода анализа главных компонент можно представить в следующем виде:

$$\mathbf{X} = \mathbf{T}\mathbf{P}^{\mathrm{T}} + \mathbf{E}, \quad (8)$$

где **T** – матрица счетов (*scores*), **P** – матрица нагрузок (*loadings*), **E** – матрица остатков (*errors or residuals*).

$$\mathbf{T} = \begin{pmatrix} t_{1,1} & t_{1,2} & \dots & t_{1,k} \\ t_{2,1} & t_{2,2} & \dots & t_{2,k} \\ \dots & \dots & \dots & \dots \\ t_{m,1} & t_{m,2} & \dots & t_{m,k} \end{pmatrix}. \quad (9)$$

Каждая строка матрицы **T** – это проекция вектора предобработанных данных на *k* главных компонент; число строк – *m* (количество временных рядов), число столбцов – *k* (количество векторов ГК, выбранных для проецирования) [130].

$$\mathbf{P} = \begin{pmatrix} p_{1,1} & p_{1,2} & \dots & p_{1,k} \\ p_{2,1} & p_{2,2} & \dots & p_{2,k} \\ \dots & \dots & \dots & \dots \\ p_{n,1} & p_{n,2} & \dots & p_{n,k} \end{pmatrix}. \quad (10)$$

Каждый столбец **P** — вектор главных компонент, число строк – *n* (размерность исходного пространства данных), число столбцов — *k* (количество векторов ГК, выбранных для проецирования) [130]. Величины нагрузок *p* – принадлежат диапазону [-1; +1] и отражают влияние на данную ГК конкретной исходной переменной.

Матрица ошибок (или остатков): $\mathbf{E} = \mathbf{X} - \mathbf{T}\mathbf{P}^{\mathrm{T}}$.

Для вычисления информативности признаков необходимо решить задачу выбора числа ГК (*k*), для чего последовательно при каждом значении *k*, начиная с единицы, рассчитываются значения объяснённой дисперсии (ERV) по формуле:

$$\mathrm{ERV} = 1 - \sum_{t=1}^{m}\sum_{j=1}^{n} e_{t,j}^2 \Big/ \sum_{t=1}^{m}\sum_{j=1}^{n} x_{t,j}^2, \quad (11)$$

где: $e_{t,j}$ – элементы матрицы $\mathbf{E}_t$; $x_{t,j}$ – элементы матрицы $\mathbf{X}_t$.

Решающее правило для выбора *k*: $\mathrm{ERV}_k \geqslant \varepsilon$, где ε выбирается эмпирически в зависимости от конкретной КФС. Тогда, информативность *i*-го признака при *k* главных компонентах вычисляется при помощи матрицы **P** по формуле:

$$I_{f_i} = \sqrt{\sum_{j=1}^{k} p_{i,j}^2} \quad (12)$$

Идентификаторы источников упорядочиваются по информативности $I_{f1} \geqslant I_{f2} \geqslant \dots \geqslant I_{fs}$ и по правилу Кайзера отбирается *s* источников, информативность которых больше средней информативности:

$$I_{f_i} > \frac{1}{n}\sum_{i=1}^{n} I_{f_i}, \quad (13)$$

где: I_{fi} – информативность i-го источника; $\frac{1}{n}\sum_{i=1}^{n} I_{f_i}$ – средняя информативность всех рассматриваемых источников; $i = 1, \ldots, n$.

Идентификаторы источников заносятся в архив и участвуют в дальнейшем построении модели классификации. Следует отметить, что информативность s наиболее информативных источников не превосходит информативность s старших главных компонент. Блок-схема алгоритма представлена на рисунке 10.

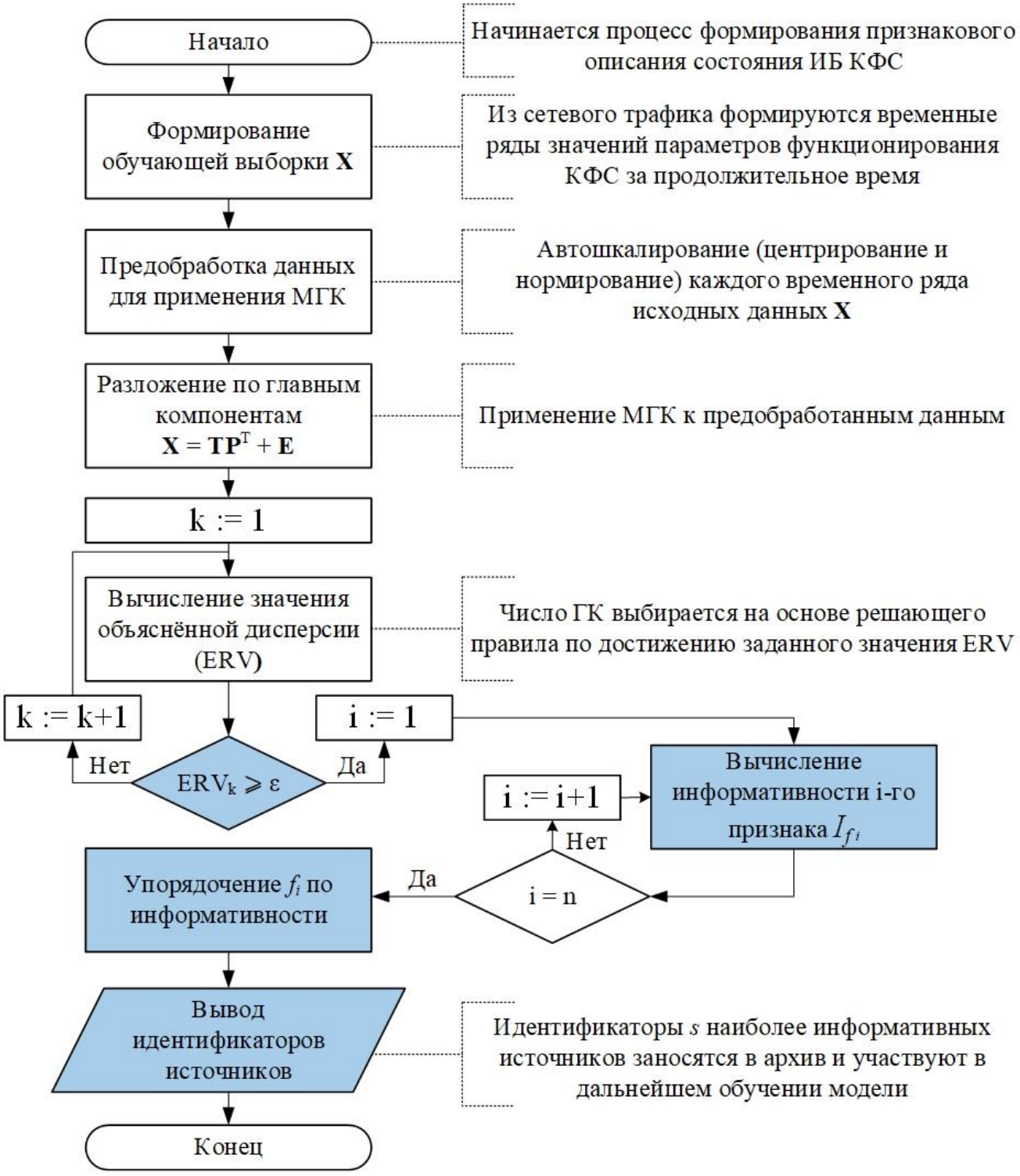

Рисунок 10 – Блок-схема алгоритма формирования признакового описания состояния ИБ элементов КФС

Применимость разработанной модели и её эффективность подтверждена при помощи результатов серии экспериментов, которые будут рассмотрены в главе 4 и подробно представлены в п. 4.3 и 4.4.2.

2.4 Выводы по главе 2

Во второй главе описана постановка задачи исследования и разработана модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем, отличающаяся от известных применением анализа главных компонент для вычисления информативности признаков и формирования списка параметров, характеризующих состояние ИБ отдельных элементов КФС. К преимуществам модели относятся её универсальность, которая достигается за счёт использования временных рядов, получаемых из сетевого трафика или сигналов иной природы происхождения, характеризующих информационные и физические процессы КФС.

Предложенная модель формирования признакового описания состояния ИБ позволяет на последующих этапах реализации алгоритма методики идентификации состояния ИБ элементов КФС повысить полноту, точность и скорость мульти-классификации. Модель инвариантна к размерности и порядкам величин, из которых составлены временные ряды, подаваемые на вход предложенного алгоритма.

Таким образом, с целью дальнейшего повышения скорости и показателей качества идентификации в системах управления информационной безопасностью (*Security Information Management*) и управления событиями безопасности (*Security Event Management*) предложено и обосновано применение новой модели, позволяющей сформировать признаковое описание состояния ИБ элементов КФС из исходного признакового пространства.

ГЛАВА 3. Разработка методики идентификации состояния информационной безопасности элементов киберфизических систем

В третьей главе описываются метод и методика идентификации состояния информационной безопасности элементов киберфизических систем. Данный этап следует непосредственно после определения наиболее информативных признаков.

3.1 Метод оценивания состояния информационной безопасности элементов киберфизических систем

3.1.1 Применение классифицирующего алгоритма на основе деревьев решений

Рассмотрим задачу классификации временных рядов, характеризующих состояние информационной безопасности КФС. Пусть имеется m сгруппированных временных рядов $X = \{\{x_1(t_1), x_2(t_1), \ldots, x_n(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_n(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\}$, каждому из которых соответствуют значения от определённого источника, то есть набор характеристик информационных или физических процессов КФС. Необходимо определить метку класса c (состояние ИБ), к которому относятся подаваемый на вход временной ряд. Для обучения модели проводится серия экспериментов, затем каждый трек полученного сигнала преобразуется в последовательность значений во времени. Каждое изменение при реализации стратегии поведения определяется множеством временных рядов, которые используются в качестве обучающей выборки.

В работе применён и исследован алгоритм на основе деревьев решений, который относится к группе логических классификаторов [131]. Суть алгоритма заключается в построении бинарного дерева, во внутренних узлах которого располагаются предикаты, а в листах – метки классов c_i ($i = 1, \ldots, l$). Выбор предикатов осуществляется с помощью критериев информативности [132].

В бинарном дереве решений:

- каждой внутренней вершине v приписана функция (или предикат) β_v: X → {0, 1};

- каждой листовой вершине v приписан прогноз $c_v \in C$.

Предикаты β_v сравнивают значение одного из признаков с порогом τ:

$$\beta_v(x; j, \tau) = [x_j < \tau] \quad (14).$$

Алгоритм $a(x)$, начиная с корневой вершины v_0 вычисляет значение функции β_{v0}. Если оно равно нулю, то алгоритм переходит в левую дочернюю вершину, иначе в правую, после чего вычисляет значение предиката в новой вершине и делает переход или влево, или вправо. Процесс продолжается, пока не будет достигнута листовая вершина; алгоритм возвращает тот класс, который приписан этой вершине.

Таким образом, подавая на вход исходные значения в момент времени t построенный алгоритм $a(x)$ на основе обучающего набора формирует ответ – метку класса $c_v \in C$, ассоциированную с состоянием ИБ КФС.

3.1.2 Улучшение показателей качества идентификации при помощи параллельно работающих классификаторов

КФС – сложная система, каждый элемент которой может подвергаться отельным видам деструктивных воздействий и атак. Данные, поступающие от различных элементов КФС могут обладать индивидуальными свойствами. В связи с этим возникает задача идентификации состояния ИБ для классификаторов, обладающих своими компетенциями на подвыборках.

Пусть имеется выборка X, состоящая из значений признаков в m моментов времени, количество классификаторов n. По методу бутстрэпа (*bootstrap*) из всего множества объектов равновероятно выбирается N объектов с возвращением. Стоит отметить, что из-за возвращения некоторые объекты могут повторяться в выбранном множестве. Обозначим новую выборку через X_1. Повторяя процедуру n раз, сгенерируем n подвыборок X_1, X_2, …, X_n.

Общие шаги построения ансамбля параллельно работающих классификаторов алгоритма:

- Генерация с помощью бутстрэпа n выборок размера k для каждого классификатора a_1-a_n.
- Независимое обучение каждого элементарного классификатора (каждого алгоритма a_1-a_n, определенного на своем подпространстве).
- Независимая классификация каждой подвыборки X_1, X_2, …, X_n на каждом из подпространств.
- Принятие окончательного решения о принадлежности объекта одному из состояний ИБ.

В предложенном подходе окончательное решение о принадлежности элементов временного ряда определённому состоянию ИБ КФС принимается одним из следующих методов:

- Консенсус: если все элементарные классификаторы присвоили одну и ту же метку множеству значений признаков в момент времени t, то такой объект будет отнесён к выбранному классу. Консенсус достижим не всегда.
- Простое большинство: объекту присваивается метка того класса, который определило для него большинство элементарных классификаторов.

На рисунке 11 проиллюстрирована работа метода.

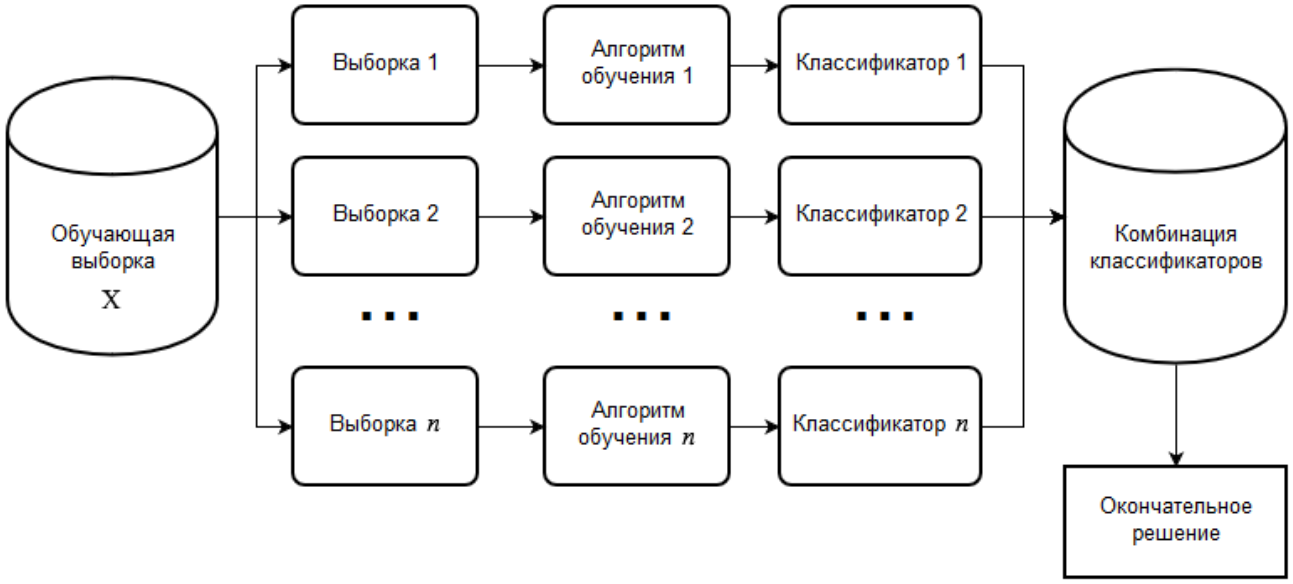

Рисунок 11 – Применение параллельно работающего ансамбля классификаторов

3.1.3 Улучшение показателей качества идентификации путём использования весовых коэффициентов Фишберна

Решение задачи, описанной в п. 3.1.1 позволяет идентифицировать состояние ИБ в момент времени t_i, однако с определённой вероятностью результат классификации c может не совпадать с реальным состоянием ИБ КФС, в таком случае имеется ложноположительное или ложноотрицательное срабатывание системы мониторинга объекта КФС.

Для таких случаев подходом, увеличивающим число верных идентификаций состояния ИБ, может стать одновременный учёт результатов классификации в моменты времени t_{i-n}, t_{i-2}, t_{i-1}, …, t_i. Однако с учётом распространения атаки при одинаковом весе состояний ИБ в каждой дискрете времени t результирующее состояние ИБ на временном отрезке $t \in [t_{i-n}, t_i]$ будет нивелировать различия во временной удалённости потенциального инцидента ИБ от исследуемого момента времени t_i (рисунок 12).

Рисунок 12 – Временной график идентификации атаки при равных значимостях

На практике, наиболее важными являются значения состояний ИБ, которые приближены к текущему, для этого предлагается ввести весовые коэффициенты, учитывающие степень предпочтения одних результатов идентификации другим (рисунок 13). Весовые коэффициенты должны удовлетворять следующим требованиям:

- учитывать временной отрезок идентификации N;
- любой коэффициент p_{i+1} должен быть меньше p_i ($\forall\, p_{i-1} < p_i$, $i \in [1, N]$).

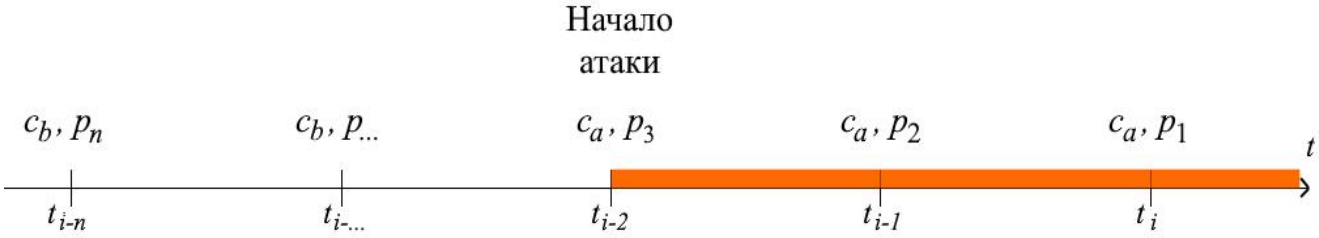

Рисунок 13 – Временной график идентификации атаки с учётом коэффициентов значимости

Для системы убывающего предпочтения, состоящей из N альтернатив, наилучшим образом подходит система весовых коэффициентов, снижающихся по правилу арифметической прогрессии. Весовые коэффициенты Фишберна - это рациональные дроби, в числителе которых расположены убывающие на единицу элементы натурального ряда от N до 1, а в знаменателе - сумма арифметической прогрессии N первых членов натурального ряда с шагом 1.

$$r_1 = N,\ r_i = r_{i-1} - 1, \tag{15}$$

$$K = \sum_{i=1}^{N} r_i, \tag{16}$$

$$p_i = \frac{r_i}{K}, \tag{17}$$

где: p_i - весовой коэффициент значимости результата идентификации по i-му временного ряду, N – временной отрезок идентификации (Δ).

Значения весовых коэффициентов Фишберна при Δ = 5 приведены в таблице 2.

Таблица 2 – Значения весовых коэффициентов Фишберна при Δ = 5

Время t_j	**Метка класса $c_{i,j}$ состояния ИБ КФС**	**Весовой коэффициент p_r (для Δ = 5)**	
t_{m-x}	-	-	-
…	…	…	…
t_{m-4}	$c_{i,m-4}$	p_5	1/15

Время t_j	**Метка класса $c_{i,j}$ состояния ИБ КФС**	**Весовой коэффициент p_r (для Δ = 5)**	
t_{m-3}	$c_{i,m-3}$	p_4	2/15
t_{m-2}	$c_{i,m-2}$	p_3	3/15
t_{m-1}	$c_{i,m-1}$	p_2	4/15
t_m	$c_{i,m}$	p_1	5/15

Результаты идентификации, полученные в разные моменты времени, усредняются с учётом их уровня значимости и более поздние состояния ИБ системы имеют больший вес. Таким образом, становится возможным сформулировать метод оценивания состояния ИБ элементов КФС, основанный на комбинированном подходе применения параллельно работающего ансамбля классификаторов и весовых коэффициентов Фишберна при анализе совокупности наиболее информативных признаков.

В начале процесса оценивания состояния ИБ элементов КФС формируется обучающая выборка из временных рядов, составленных из значений параметров функционирования КФС и соответствующих им меток состояний ИБ (классов). После чего, методом равномерного случайного сэмплинга с возвратом формируется n подвыборок.

Алгоритмы a_1-a_n на основе деревьев решений обучаются каждый на своей подвыборке независимо друг от друга. После этапа обучения анализируемые показатели за время Δ подаются на вход вышеуказанных классифицирующих алгоритмов. Каждый алгоритм a_1-a_n генерирует N ответов $x_t \rightarrow c$ на временном отрезке Δ, которые обобщаются на первом этапе с использованием весовых коэффициентов Фишберна, в данном случае метка класса определяется путём взвешенного обобщения результатов классификации на отрезке времени Δ. В случае равенства коэффициентов p для различных классов c выбирается тот класс, который был определён для более позднего момента времени.

Окончательное решение принимается за счёт обобщения результатов по каждому классификатору a_1-a_n и итоговый результат определяется простым большинством голосующих классификаторов, используются нечётные n, чтобы избежать случаев равного числа голосов для отличающихся классов c.

Реализация метода представлена на рисунке 14.

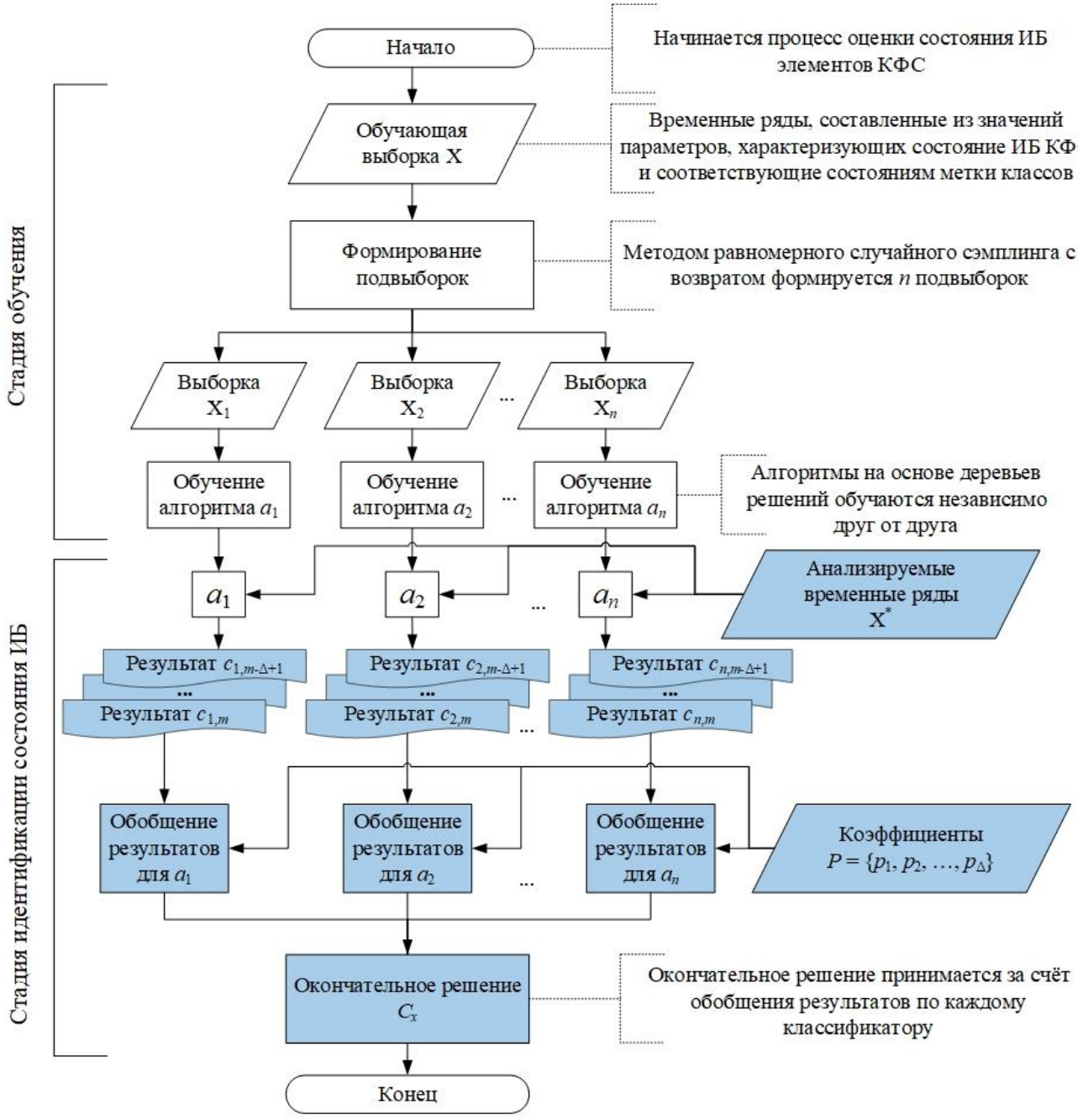

Рисунок 14 – Метод оценивания состояния ИБ элементов КФС, основанный на комбинированном подходе

Представленный метод позволяет повысить полноту и точность идентификации состояния ИБ элементов КФС за счёт параллельно работающих

классификаторов и весовых коэффициентов Фишберна при анализе совокупности информативных признаков, полученных из временных рядов, характеризующих функционирование КФС. Практическая применимость разработанного метода исследована в главе 4 и будет подробно рассмотрена в п. 4.4.3.

3.2 Методика идентификации состояния ИБ элементов КФС

Интеграция КФС в технологические процессы привела к необходимости создания новой методики идентификации состояния ИБ таких систем в условиях воздействия угроз нарушения их информационной безопасности.

В рамках задачи разработки методики идентификации состояния ИБ необходимо основываться на ключевых особенностях КФС [133]. Для ёмкого и эффективного выявления нарушений ИБ таких систем, разрабатываемая методика должна удовлетворять следующим требованиям:

1. Обработка поступающего сетевого трафика и выделение временных рядов должно производиться в режиме реального времени, с минимально возможными задержками, которые обусловлены вычислительными ограничениями контролирующих систем и передающих устройств. Такое требование имеет место в первую очередь для своевременного обнаружения атак и реагирования на них.

В случае апостериорной ИБ должен производится полный и всесторонний анализ временных рядов с целью выявления хода распространения инцидента.

2. Результат применения методики долен быть инвариантен к атакам и не зависеть от конкретного типа атаки, её сложности, ресурсоёмкости, способа реализации и других параметров.

3. Методика должна быть универсальной и по возможности применимой к устройствам разных типов. Здесь стоит отметить высокую разнородность компонентов КФС из-за которой конкретные способы детектирования могут не подходить для контролируемого устройства.

4. Результат применения методики должен быть известен в каждый момент времени с учётом частоты обновления данных мониторинга. Таким образом, реализуется возможность сравнивать полученные результаты в различные

моменты времени. Данное требование обусловлено необходимостью реагирования на инциденты не только в зависимости от времени их возникновения, но и от предполагаемой длительности потенциального деструктивного воздействия.

Таким образом, в настоящей работе предлагается идентифицировать состояния ИБ элементов КФС на основе анализа временных рядов, выявляющего отклонения текущего состояния ИБ системы от разрешенных. На основе предложенных методов становится возможным сформулировать методику идентификации нарушений информационной безопасности.

Исходное признаковое пространство $H = (f_1, f_2, \ldots, f_n)$ состоит из n источников данных о процессах хранения, обработки и передачи информации КФС. Имеется конечное множество состояний ИБ $\{C_0, C_1\} \subset C$, C_0 – множество меток классов безопасных состояний ИБ КФС, C_1 – множество меток классов аномальных (опасных) состояний ИБ, $\{c_1, c_2, \ldots, c_k\} \subset C_0$, $\{c_{k+1}, c_{k+2}, \ldots, c_l\} \subset C_1$, l – число идентифицируемых состояний ИБ КФС.

Методика включает в себя три стадии.

1. Этап формирования архива идентификаторов источников (АИИ).
2. Подготовительный этап.
3. Этап идентификации состояния ИБ.

При планировании системы выявления нарушений ИБ происходит выбор анализируемых элементов КФС. Непосредственно разработанная методика основывается на нижеследующей последовательности действий.

На первом этапе происходит моделирование различных состояний ИБ КФС при помощи запуска соответствующих программ или передачи управляющих команд. Целью является получение зависимостей количественных показателей информационных процессов КФС для различных состояний ИБ. Для корректного формирования АИИ требуются значения параметров функционирования КФС за продолжительное время, которые регистрируются при помощи датчиков или внутренних программно-аппаратных модулей.

Результатом этапа формирования обучающей базы является m временных рядов, сгруппированных по времени t, $X = \{\{x_1(t_1), x_2(t_1), \ldots, x_n(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_n(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\}$, после чего данные преобразуются (центрируются и нормируются) и подаются на вход формирователя информативных признаков.

Формирование уникального для конкретной КФС признакового описания состояний ИБ происходит по алгоритму, описанному в п. 2.3, в результате чего на выходе формируется отобранные идентификаторы источников (признаков) $H^* = (f_1, f_2, \ldots, f_s)$, которые заносятся в АИИ и подлежат замене только в случае изменения (дополнения, нового формирования) обучающей выборки.

Вторая стадия начинается с получения идентификаторов информативных признаков из АИИ, затем из исходных временных рядов исключаются все значения признаков, отсутствующих в АИИ и формируется кортеж данных $\hat{X} = \{\{x_1(t_1), x_2(t_1), \ldots, x_s(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_s(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_s(t_m)\}\}$, при этом информативности $I_{f_1} > I_{f_2} > \ldots > I_{f_s}$. Каждому моменту времени t поставлена в соответствие метка класса c, отражающая состояние ИБ.

Обучающая и тестовая выборки формируются из кортежа $\hat{X}$, причем 75 % полученных значений используются в качестве обучающего, 25 % в качестве тестового набора. Классифицирующие алгоритмы a_1-a_n обучаются параллельно и независимо друг от друга на подвыборках, сформированных по методу, подробно описанному в п. 3.1.3.

Завершающим этапом второй стадии является выбор временного отрезка идентификации состояния ИБ Δ. Решающим фактором для выбора Δ является максимизация F-меры результатов классификации для контролируемой КФС.

На заключительной стадии реализации методики, анализируемые данные, представляющие собой кортеж $X^* = \{\{x_1(t_{m-\Delta}), x_2(t_{m-\Delta}), \ldots, x_s(t_{m-\Delta})\}, \ldots, \{x_1(t_{m-1}), x_2(t_{m-1}), \ldots, x_s(t_{m-1})\}, \{x_1(t_m), x_2(t_m), \ldots, x_s(t_m)\}\}$ подаются на вход алгоритма, реализующего метод оценивания состояния ИБ элементов КФС, основанный на

комбинированном подходе. Полученные результаты ансамбля классификаторов для каждого момента времени по классификаторам a_1-a_n постобрабатываются при помощи весовых коэффициентов Фишберна, придающих больший вес более поздним результатам идентификации. Заключительным этапом методики является формирование на основе решающего правила итогового результата идентификации состояния ИБ элементов КФС.

Схема вышеописанной методики приведена на рисунке 15.

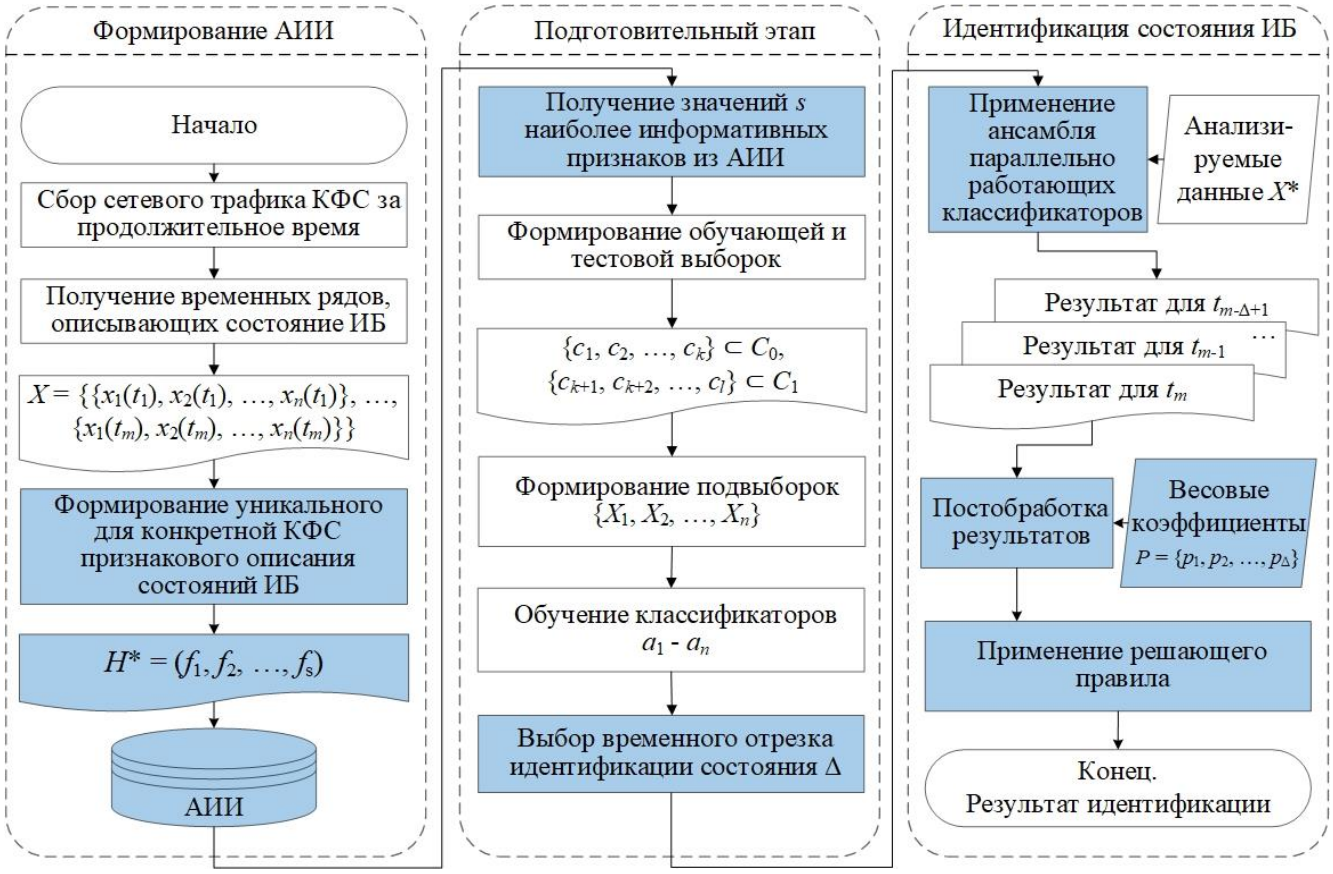

Рисунок 15 – Блок-схема методики идентификации состояния ИБ элементов КФС

Таким образом, на основе реализации алгоритма методики производится формирование решения о текущем состоянии ИБ системы и (при необходимости) восстановлении безопасного функционирования КФС и её информационных процессов.

Оперативное выявление нарушений ИБ КФС позволяет контролирующей системе или лицу, принимающему решение, принять меры реагирования на возможный инцидент ИБ с целью поддержания безопасного функционирования

КФС, что особенно важно для систем критической инфраструктуры и непрерывных производств, в которых простой технологического оборудования может принести серьёзный вред и финансовые потери организации.

3.3 Ограничения методики

Разработанная методика идентификации состояния ИБ элементов КФС максимизирует точность и полноту при условии ограничений на:

— тип и количество исследуемых КФС;

— количество различных состояний ИБ КФС и/или её элементов;

— неспособность классификатора сформировать корректный результат для состояния ИБ, если оно не было определено на этапе обучения;

— невозможность однозначно сделать вывод о том были ли нарушения функционирования КФС следствием атаки злоумышленника или возникли в результате воздействия случайных факторов;

— неспособность успешно выявить нарушения ИБ, если злоумышленник осведомлён о функционирующей системе и осуществляет целенаправленную подмену информации с датчиков, правдоподобно имитируя безопасное поведение КФС.

3.4 Выводы по главе 3

В третьей главе разработан метод оценивания состояния информационной безопасности элементов киберфизических систем и методика, использующая предложенный метод. Приведены схемы и алгоритмы реализации предложенных подходов. Одним из отличий КФС от классических информационных систем является их тесная интеграция в производственные и иные сложные технологические системы, поэтому в рамках задачи формирования методов и методики оценивания состояния ИБ учитывалась эта и другие особенности КФС.

Предложенный метод позволяет существенно повысить точность идентификации состояния ИБ элементов КФС как за счёт применения ансамбля параллельно работающих классификаторов, так и с помощью обобщения и

взвешенного усреднения результатов идентификации на временном отрезке, сокращая при этом ошибки из-за случайных отклонений параметров функционирования КФС.

Снижение вычислительных затрат, увеличение скорости идентификации состояния ИБ элементов КФС являются решающими факторами при осуществлении мониторинга и восстановлении безопасного функционирования КФС в режиме реального времени.

Разработанная методика характеризуется большей полнотой идентификации и меньшим временем принятия решения за счёт лишь однократной предобработки исходных данных обучающей и тестовой выборок на этапе формирования информативных признаков и дальнейшем применении классификаторов, работающих параллельно.

ГЛАВА 4. Экспериментальная апробация и анализ полученных результатов

4.1 Экспериментальный стенд КФС

Для целей исследования состояния ИБ анализировался сетевой трафик между системой управления и сбора данных (SCADA) и ПЛК. Апробация модели, метода и методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов заключались в проведении вычислительного эксперимента над набором данных [134] с целью практической реализации предложенного подхода. Исследователями из Сингапурского университета технологии и дизайна (Singapore University of Technology and Design) моделировались различные типы атак на компоненты экспериментального стенда киберфизической системы водоочистки (рисунок 16) [135].

Рисунок 16 – Слева: ультрафильтрация | Справа: общий вид КФС водоочистки

Процесс очистки воды является многостадийным и включает в себя шесть стадий P1-P6 (рисунок 17) [134]:

P1) хранение и подача неочищенной воды;

P2) дозирование химических реагентов;

P3) первичная обработка (ультрафильтрация, обратная промывка);

Р4) вторичная обработка (дехлорирование);

Р6) обратный осмос (ОО);

Р6) обратная промывка и очистка, передача очищенной воды.

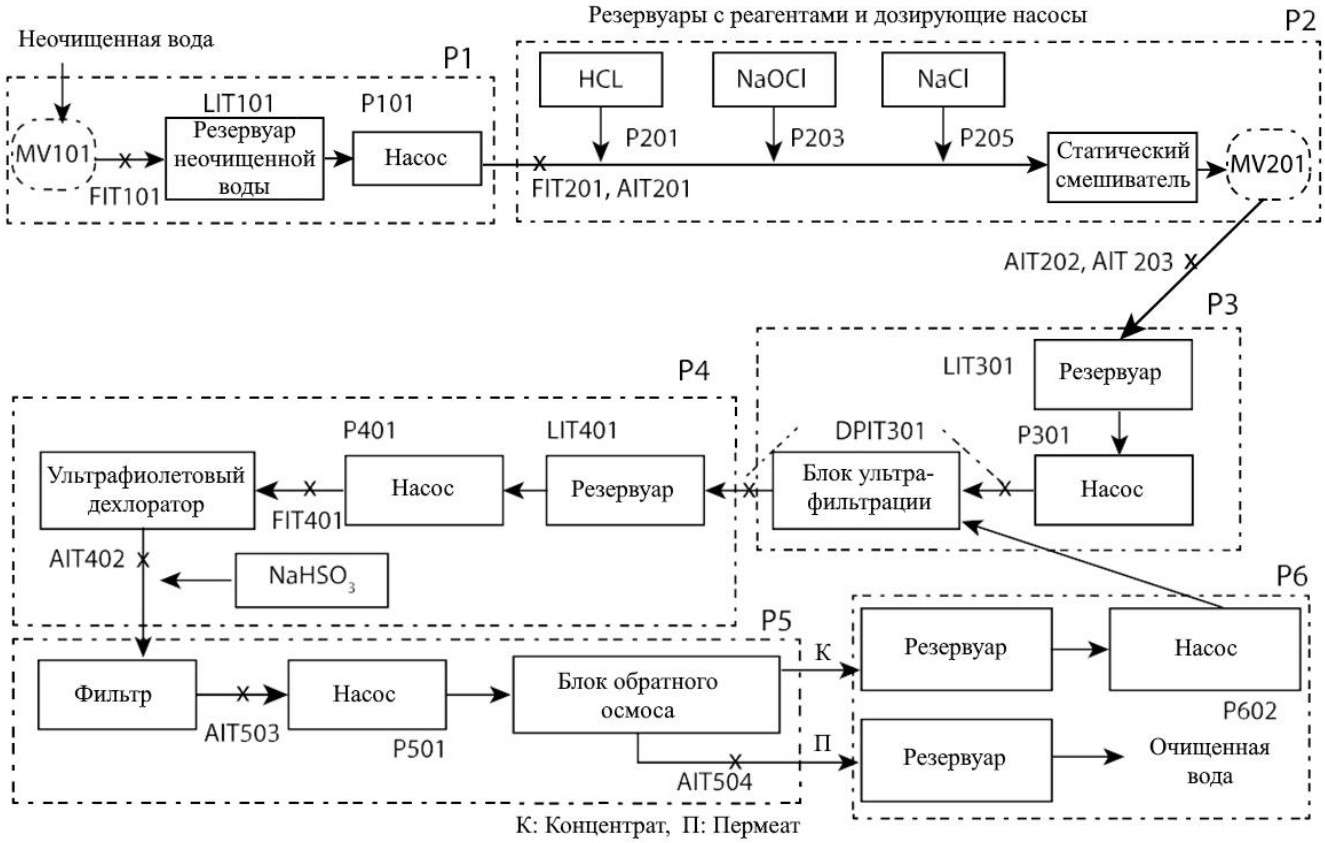

Рисунок 17 – Схема процессов и датчиков КФС водоочистки

Непосредственное управление процессами на каждом этапе осуществляется при помощи программируемых логических контроллеров, которые взаимодействуют с датчиками и исполнительными устройствами (актуаторами) физического уровня (рисунок 18).

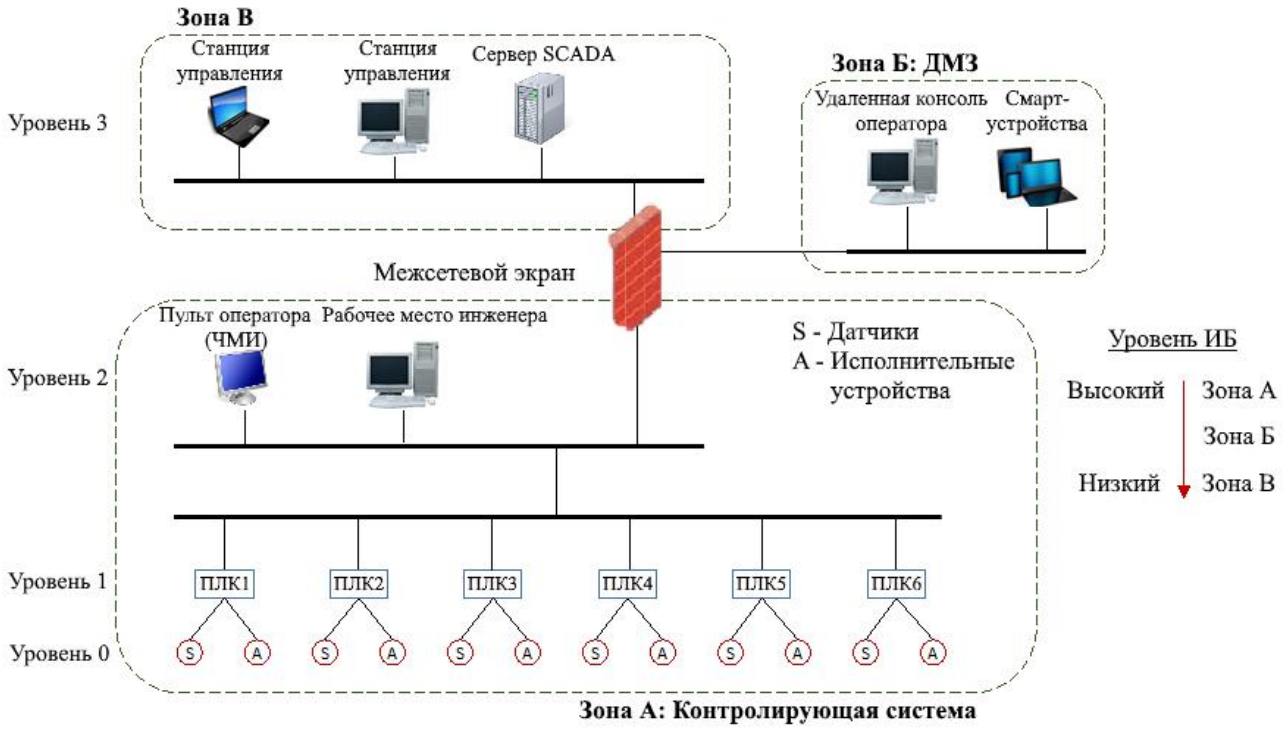

Рисунок 18 – Архитектура КФС водоочистки

Часть смоделированных атак осуществлялась путём перехвата и подмены пакетов сетевого трафика, которым обмениваются между собой система SCADA и ПЛК. В небезопасном состоянии ИБ КФС сетевые пакеты изменены и содержат модифицированные значения от датчиков. Данные сетевого трафика, которые важны для обнаружения нарушений ИБ элементов КФС, сведены в таблицу 3.

Таблица 3 – Описание полей пакетов анализируемого сетевого трафика

Поле	**Описание**
Дата	Дата события
Время	Время события
Источник	IP-адрес сервера
Тип	Тип журнала
Тип интерфейса	Тип сетевого интерфейса
Направление интерфейса	Направление данных: ведущий → ведомый (запрос), ведомый → ведущий (ответ)
Исходный IP	IP-адрес источника
IP-адрес назначения	IP-адрес назначения

Поле	Описание
Протокол	Сетевой протокол
IP-адрес источника прокси	Прокси-адрес источника
Название приложения	Название приложения
Код функции	Код функции Modbus
Описание функции	Описание функции Modbus
ID транзакции	Идентификатор транзакции Modbus
Тег SCADA	Идентификатор датчика или исполнительного механизма
Значение Modbus	Переданное значение
Сервисный / целевой порт	Номер порта IP-адреса назначения
Исходный порт	Номер порта исходного IP-адреса

КФС водоочистки состоит из следующего набора датчиков, обеспечивающих непрерывный мониторинг всех стадий процесса, и исполнительных устройств, поддерживающих функционирование системы, а также выполнение целевой функции, (x – номер подпроцесса, y – модуль подпроцесса) [134]:

- AITx0y

  − датчики проводимости, измеряющие способность водного раствора проводить электрический ток (мкСм/см). Эта способность определяется количеством ионов, например, хлорида натрия (NaCl) в воде;

  − pH-метры, измеряющие водородный показатель;

  − датчики окислительно-восстановительного потенциала (мВ);

  − ионоселективные электроды для определения жесткости воды;

- PITx0y − датчики давления (кПа);
- DPITx0y − датчики перепада давления (кПа);
- FITx0y − расходомеры, измеряющие поток воды ($м^3$/ч);
- LITx0y − датчики уровня воды (мм);
- MVx0y − моторизованные клапаны воды;
- Px0y

− приводные насосы;

− дозирующие насосы;

− питающие насосы;

- UV401 – актуатор для ультрафиолетового дехлорирования воды.

4.2 Обучающая и тестовая выборки

В предыдущих главах показано, что описание процесса функционирования КФС можно осуществить при помощи временных рядов - последовательностей значений сигналов, синхронизированных по времени и характеризующих работу системы [36]. Каждому временному ряду поставлена в соответствие метка класса *C*. Всего было проанализировано 944 919 временных рядов, регистрируемых раз в секунду в течение ~ 11 дней функционирования КФС, 7 дней при нормальной работе и 4 дня при реализации сценариев атак. Фрагмент массива данных обучающей выборки представлен на рисунке 19, каждая строка таблицы представляет собой временной ряд значений сигналов от различных источников.

Метка каласса	AIT501	AIT502	AIT503	AIT504	FIT501	FIT502	FIT503	FIT504	PIT501	PIT502	PIT503	FIT601
Normal	7,878621	145,1166	264,5475	12,03538	1,723789	1,279621	0,7352687	0,3077859	250,8652	1,649953	189,5988	0,000128
Normal	7,878621	145,1166	264,5475	12,03538	1,723789	1,297554	0,7352687	0,3077859	250,8652	1,649953	189,6789	0,000128
Normal	7,878621	145,1166	264,5475	12,03538	1,723404	1,293967	0,7352687	0,3086186	250,8812	1,649953	189,6789	0,00012
Normal	7,878621	145,0141	264,5475	12,03538	1,723404	1,281158	0,7352687	0,3086186	250,8812	1,649953	189,6148	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,723404	1,281158	0,7352687	0,3086186	250,8812	1,649953	189,5027	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,723404	1,272704	0,7352687	0,3086186	250,753	1,649953	189,5027	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,723404	1,270142	0,7352687	0,3086186	250,5928	1,649953	189,5027	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,723404	1,262329	0,7352687	0,3086186	250,5928	1,649953	189,5027	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,723404	1,270398	0,7352687	0,3086186	250,9132	1,649953	189,5027	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,726224	1,281158	0,7352687	0,3084905	250,9132	1,649953	189,5668	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,726352	1,276162	0,7352687	0,3081062	251,1055	1,649953	189,8231	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,726352	1,282183	0,7352687	0,3074016	251,1856	1,649953	189,9994	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,72725	1,275778	0,7352687	0,3066329	251,1856	1,649953	189,9994	0,00012
Normal	7,878621	144,8859	264,5475	12,03538	1,728275	1,272192	0,7352687	0,3066329	251,1856	1,649953	189,9994	0,00012
Normal	7,878621	144,8859	264,5475	12,26609	1,728275	1,282951	0,7352687	0,3066329	251,1856	1,649953	189,9994	0,000128
Normal	7,878621	144,8859	264,5475	12,26609	1,728275	1,282951	0,7352687	0,3066329	251,1856	1,649953	189,9994	0,000128
Normal	7,878621	144,8859	264,5475	12,26609	1,729172	1,291533	0,7373172	0,3066329	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,26609	1,729172	1,291533	0,7385975	0,30785	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,26609	1,729172	1,284745	0,7385975	0,3083624	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,26609	1,729172	1,288203	0,7385975	0,3083624	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,11228	1,729172	1,282823	0,7385975	0,3083624	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,11228	1,729172	1,281286	0,7385975	0,3083624	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,11228	1,729172	1,287306	0,7385975	0,3079781	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,11228	1,729172	1,283464	0,7385975	0,3065689	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,8859	264,5475	12,11228	1,729172	1,282439	0,7385975	0,3065689	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,729172	1,276547	0,7383414	0,3065689	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,729172	1,265659	0,7379573	0,3065689	251,1856	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,728788	1,262457	0,7361649	0,3065689	251,1535	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72725	1,27027	0,7357808	0,3065689	251,0414	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72725	1,271551	0,7348846	0,3065689	251,0414	1,649953	189,8872	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72725	1,278724	0,7348846	0,3065689	251,0414	1,649953	189,8071	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72725	1,299603	0,7348846	0,3065689	251,0414	1,649953	189,8071	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72725	1,302293	0,7348846	0,3075937	251,0414	1,649953	189,8071	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,725711	1,292814	0,7348846	0,3069532	250,9453	1,649953	189,5988	0,000128
Normal	7,878621	144,9116	264,5475	12,11228	1,72507	1,283592	0,7348846	0,3068251	250,8171	1,649953	189,5988	0,000128

Рисунок 19 – Фрагмент массива данных обучающей выборки

Исходные экспериментальные данные, состоящие из временных рядов и характерные для данного типа КФС разбивалась на 2 подвыборки – обучающую и тестовую. Большой объём экспериментальных данных позволял в дальнейших экспериментах 75 % полученных значений сигналов использовать в качестве обучающего, 25 % в качестве тестового набора.

Был собран сетевой трафик КФС и значения, полученные от физических источников (51 датчиков и исполнительных механизмов). Выборки были размечены в соответствии с нормальным и аномальными состояниями ИБ системы, всего реализована 41 атака на КФС водоочистки. Моделировались следующие типы деструктивных воздействий:

− модификация данных, поступающих от компонентов КФС;

− атаки отказа в обслуживании на компоненты экспериментальной КФС;

− подмена таблицы маршрутизации;

− переполнение таблицы маршрутизации;

− модификация аппаратного и программного обеспечения;

− активация программных и аппаратных закладок.

Атаки могут происходить на разных уровнях КФС, включать в себя несколько этапов, быть растянутыми по времени и затрагивать различные элементы КФС. В таблице 4 представлены типы атак, а в таблице 5 их полный список.

Таблица 4 – Типы атак на КФС водоочистки

Типы атак	**Количество атак**
Одностадийные и однонаправленные атаки	26
Одностадийные многонаправленные атаки	4
Многостадийные однонапрвленные атаки	2
Многостадийные и многонаправленные атаки	4
Атаки без воздействия на технологический процесс	5

Таблица 5 – Список проведённых атак на КФС водоочистки

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_1	MV-101	MV-101 закрыт	Перехват и модификация сетевых пакетов	Открытие клапана MV-101	Переполнение резервуара	Изменение диапазонов переменных FIT-101, LIT-101
c_2	P-102	P-101 включен, P-102 выключен		Включение P-102	Нарушение герметичности труб	Изменение диапазонов переменной FIT-201
c_3	LIT-101	Уровень воды между L и H	Активация программной закладки	Увеличение на 1 мм каждую секунду	Опустошение резервуара; повреждение P-101	Изменение диапазонов переменной P-101
c_4	MV-504	MV-504 закрыт	Активация аппаратной закладки	Открытие клапана MV-504	Нарушение последовательности выключения и сокращение срока службы установки обратного осмоса	Изменение диапазонов переменной FIT-504
c_5	Атака без воздействия на технологический процесс КФС					
c_6	AIT-202	Значение AIT-202 > 7.05	Модификация программного обеспечения	Подмена значения AIT-202 на 6	Выключение P-203; изменение качества воды	Изменение диапазонов переменной P-203. Изменение для

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
						AIT-504 зафиксировано через два часа
c_7	LIT-301	Уровень воды между L и H	Активация аппаратной закладки	Поднятие уровня воды выше HH	Остановка притока; опустошение резервуара; повреждение P-301	Изменение диапазонов переменных P-301, DPIT-301
c_8	DPIT-301	Значение DPIT < 40 кПа	Модификация данных, поступающих от компонентов КФС	Подмена значения DPIT > 40 кПа	Процесс обратной промывки запускается циклом; нормальная работа КФС прекращается; снижается уровень воды в резервуаре 401; повышается уровень воды в резервуаре 301	Изменение диапазонов переменных P-401, LIT-401
c_9	Атака без воздействия на технологический процесс КФС					
c_{10}	FIT-401	Значение FIT-401 > 1	Модификация аппаратного обеспечения	Подмена значения FIT-401 < 0.7	Выключение УФ-дехлоратора и насоса P-501	Значения остались в диапазоне допустимых, т.к. УФ-дехлоратор и насос P-501 не отключились
c_{11}	FIT-401	Значение FIT-401 > 1		Подмена значения FIT-401 на 0	Выключение УФ-дехлоратора и насоса P-501	Изменение диапазонов переменных AIT-402, P-501

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_{12}	Атака без воздействия на технологический процесс КФС					
c_{13}	MV-304	MV-304 открыт	Активация аппаратной закладки	Закрытие клапана MV-304	Остановка этапа 3 из-за изменения процесса обратной промывки	Значения остались в диапазоне допустимых, т.к. ультрафильтрация не остановилась из-за позднего закрытия MV-304
c_{14}	MV-303	MV-303 закрыт	Атака отказа в обслуживании	Исключение возможности открытия MV-303	Остановка этапа 3 из-за изменения процесса обратной промывки	Атака не удалась, т.к. резервуар 301 уже был заполнен
c_{15}	Атака без воздействия на технологический процесс КФС					
c_{16}	LIT-301	Уровень воды между L и H	Активация программной закладки	Уменьшение уровня воды на 1 мм каждую секунду	Переполнение резервуара	Изменение диапазонов переменных DPIT-301, P-301
c_{17}	MV-303	MV-303 закрыт	Атака отказа в обслуживании	Исключение возможности открытия MV-303	Остановка этапа 3 из-за изменения процесса обратной промывки	Изменение диапазонов переменных LIT-301, P-301
c_{18}	Атака без воздействия на технологический процесс КФС					
c_{19}	AIT-504	Значение AIT-504 < 15 мкСм/см	Перехват и модификация сетевых пакетов	Подмена значения AIT-504 на 16 мкСм/см	Установка обратного осмоса отключается через 30 минут. Вода должна пойти в канализацию	Атака не удалась

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_{20}	AIT-504	Значение AIT-504 < 15 мкСм/см	Перехват и модификация сетевых пакетов	Подмена значения AIT-504 на 255 мкСм/см		
c_{21}	MV-101, LIT-101	MV-101 открыт; LIT-101 между L и H	Атака отказа в обслужива-нии, переполнение таблицы маршрутиза-ции	Не закрывать MV-101; подмена значения LIT-101 на 700 мм	Переполнение резервуара	Изменение диапазонов переменных P-101, FIT-201
c_{22}	UV-401, AIT-502, P-501	UV-01 включен; AIT-502 < 150; P-501 включен	Атака отказа в обслужива-нии, модификация данных	Остановка UV-401; подмена значения AIT-502 на 150; P-501 остаётся включен	Возможное повреждение установки обратного осмоса	P-501 не может быть включен; Сниженный выход у FIT-502
c_{23}	P-602, DIT-301, MV-302	Значение DPIT-301 < 0.4 бар; MV-302 открыт; P-602 выключен	Активация программной закладки	Подмена значения DPIT-301 > 0.4 бар; MV-302 остаётся открыт; P-602 остаётся выключен	Остановка КФС	Изменение диапазонов переменных P-101, P-201, P-203, P-205, P-301, UV-401, P-401, P-501, P-602
c_{24}	P-203, P-205	P-203 включен; P-205 включен	Атака отказа в обслужива-нии	Выключение P-203 и P-205	Изменение качества воды	Изменение диапазонов переменных

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
						P-101, LIT-301; резервуар T-101 переполнился
c_{25}	LIT-401, P-401	Значение LIT-401 < 1000; P-402 включен	Перехват и модификация сетевых пакетов	Подмена значения LIT-401 на 1000; P402 остаётся включен	Опустошение резервуара	Изменение диапазонов переменных AIT-402, P-501
c_{26}	P-101, LIT-301	P-101 выключен; P-102 включен; LIT-301 между L и H	Переполне-ние таблицы маршрутиза-ции	P-101 постоянно включен; подмена значения LIT-301 на 801 мм	Опустошение резервуара 101; переполнение резервуара 301	Изменение диапазонов переменных LIT-101, LIT-301, DPIT-301
c_{27}	P-302, LIT-401	P302 включен, LIT-401 между L и H	Активация программной закладки	P-302 постоянно включен; подмена значения LIT-401 на 600 мм	Переполнение резервуара	Изменение диапазонов переменных LIT-301, LIT-401
c_{28}	P-302	P302 включен	Атака отказа в обслужива-нии	Выключение P-302	Остановка притока в резервуар T-401	Изменение диапазонов переменной LIT-401
c_{29}	P-201, P-203, P-205	P-201 закрыт; P-203 закрыт; P-205 закрыт	Перехват и модификация сетевых пакетов	Открыть P-201; открыть P-203; открыть P-205	Потеря реагентов, три дозирующих насоса не запустятся из-за механической блокировки	Изменение диапазонов переменной AIT-201

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_{30}	LIT-101, P-101, MV-201	P-101, MV-101, MV-201 выключены; LIT-101, LIT-301 между L и H	Модификация аппаратного обеспечения	Включение P-101, MV-101 постоянно; подмена значения LIT-101 на 700 мм	Опустошение резервуара 101; переполнение резервуара 301; запуск P-102, т.к. уровень LIT-301 низкий	Изменение диапазонов переменных LIT-101, AIT-201, AIT-203, LIT-301
c_{31}	LIT-401	Уровень воды между L и H	Модификация данных, поступающих от компонентов КФС	Подмена значения LIT-401 меньше L	Переполнение резервуара	Изменение диапазонов переменных AIT-402, LIT-401
c_{32}	LIT-301	Уровень воды между L и H		Подмена значения LIT-301 выше HH	Опустошение резервуара; повреждение P-302	Изменение диапазонов переменных DPIT-301, LIT-401, P-302
c_{33}	LIT-101	Уровень воды между L и H		Подмена значения LIT-101 выше H	Опустошение резервуара; повреждение P-101	Изменение диапазонов переменных AIT-201, AIT-203
c_{34}	P-101	P-101 включен	Подмена таблицы маршрутиза-ции	Выключение P-101	Остановка оттока	Изменение диапазонов P-102. Отток не прекратился, потому что КФС включила P-102

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_{35}	P-101; P-102	P-101 включен; P-102 выключен	Активация программной закладки	Выключение P-101; не допускать включения P-102	Останавливается отток	Изменение диапазонов переменных AIT-201, FIT-201, AIT-203
c_{36}	LIT-101	Уровень воды между L и H	Модификация программного обеспечения	Подмена значения LIT-101 меньше LL	Переполнение резервуара	Изменение диапазонов переменных P-101, FIT-201
c_{37}	P-501, FIT-502	P-501 включен; FIT-502 в допустимом диапазоне	Перехват и модификация сетевых пакетов	Выключение P-501; подмена значения FIT-502 на 1.29	Сниженный выход	Изменение диапазонов P-501; FIT-502 снизил значение до 0.8; частота P-501 возросла с 10 Гц до 28.5 Гц
c_{38}	AIT-402, AIT-502	В допустимом диапазоне	Модификация данных, поступающих от компонентов КФС	Подмена значения AIT-402 на 260; подмена значения AIT-502 на 260	Вода поступает в канализацию из-за большой концентрации реагента	Изменение диапазонов переменных AIT-503, P-501
c_{39}	FIT-401, AIT-502	В допустимом диапазоне		Подмена значения FIT-401 на 0.5 подмена значения AIT-502 на 140 мВ	УФ-дехлоратор отключится, и вода поступит в установку обратного осмоса	Изменение диапазонов переменных AIT-402, AIT-503

№	Напра-вление атаки	Начальное состояние	Вид воздействия	Описание атаки	Ожидаемое воздействие или намерение злоумышленника	Проявление во временных рядах
c_{40}	FIT-401	В допустимом диапазоне	Активация программной закладки	Подмена значения FIT-401 на 0	УФ-дехлоратор отключится, и вода поступит в установку обратного осмоса	Изменение диапазонов переменных P-402, AIT-402
c_{41}	LIT-301	Уровень воды между L м H		Уменьшение значения на 0.5 мм в секунду	Переполнение резервуара	Изменение диапазонов переменных DPIT-301, P-301

4.3 Формирование признакового описания состояния ИБ

Цель вычислительного эксперимента – применение алгоритма формирования признакового описания состояния информационной безопасности элементов киберфизических систем для реально существующей КФС.

В настоящей работе для целей анализа временных рядов, характеризующих функционирование КФС, использовалось программное обеспечение Matlab R2021a. Исходные данные для реализации разработанного комплексного подхода, включающего модель, метод и методику, представляли собой численный двумерный массив 944 919 x 51, каждый элемент массива X задан двумя индексами, индексом строки и индексом столбца. В строках расположены значения временных рядов, регистрируемых раз в секунду, в свою очередь, столбцы упорядочены по источникам получения информации от КФС.

Перечень источников получения информации о функционировании КФС: FIT101, LIT101, MV101, P101, P102, AIT201, AIT202, AIT203, FIT201, MV201, P201, P202, P203, P204, P205, P206, DPIT301, FIT301, LIT301, MV301, MV302, MV303, MV304, P301, P302, AIT401, AIT402, FIT401, LIT401, P401, P402, P403, P404, UV401, AIT501, AIT502, AIT503, AIT504, FIT501, FIT502, FIT503, FIT504, P501, P502, PIT501, PIT502, PIT503, FIT601, P601, P602, P603.

На первом этапе реализации алгоритма формирования информативных признаков применяется разложение при помощи стандартной функции Matlab [*loadings*,*scores*,*latent*,*tsquared*,*explained*,*mu*] = pca(X, *'NumComponents'*, 51), где:

- *loadings* – матрица нагрузок;
- *scores* – матрица счетов;
- *latent* – вектор-столбец, содержащий значения дисперсий ГК, то есть собственные значения ковариационной матрицы X;
- *tsquared* – вектор-столбец, который представляет собой сумму квадратов стандартизованных счетов для каждого временного ряда (Т-квадрат распределения Хотеллинга);

- *explained* – вектор-столбец, содержащий значения объяснённой дисперсии для заданного в *NumComponents* числа ГК;
- *mu* – средние значения переменных в X, возвращенные как вектор-строка.

Особый интерес для анализа и формирования информативных признаков представляют переменные *loadings* и *explained*. Поскольку *explained* представляет собой столбец, в котором содержатся частные значения дисперсии по каждой ГК отдельно, то для получения совокупных значений в цикле производится суммирование q первых элементов по формуле:

$$\mathrm{ERV}_q = \sum_{i=1}^{q} explained(i),\ q = 1, \ldots, n. \qquad (18)$$

Зависимость совокупной объяснённой дисперсии от количества ГК представлена на рисунке 20.

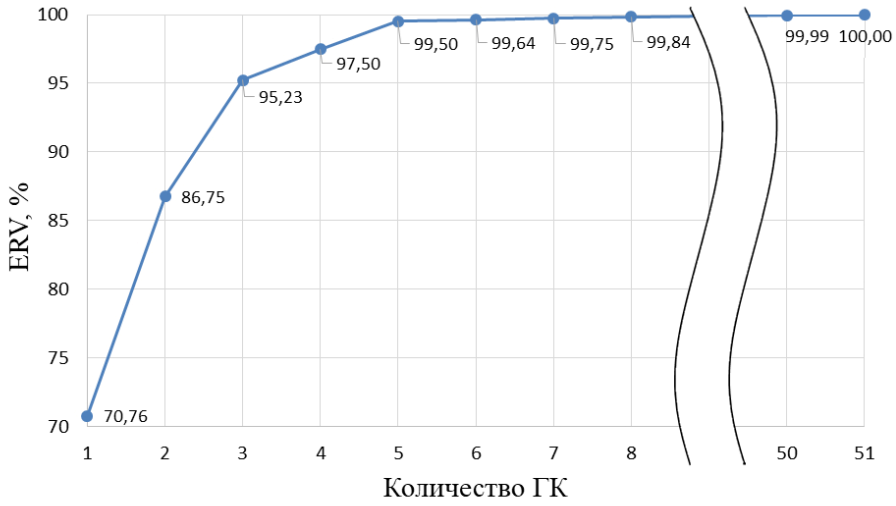

Рисунок 20 – Зависимость совокупной объяснённой дисперсии от количества ГК для исследуемой КФС водоочистки

ГК упорядочиваются по величинам ERV. Как видно из графика (рисунок 20), значения объяснённой дисперсии резко увеличиваются при ГК с первой по пятую, затем идёт монотонное медленное увеличение вплоть до 51-ой ГК. Исходя из этого можно сделать вывод, что бóльшую часть разброса экспериментальных данных можно объяснить существенно меньшим числом источников в пространстве главных компонент. Разработанная модель подразумевает использование МГК для

вычисления информативности признаков с целью сокращения вычислительных затрат.

Дальнейшим шагом является определение количества ГК, по которым будет рассчитана информативность признаков для каждого источника. В листинге 1 представлен алгоритм, по переменной *explained* возвращающий количество ГК при заданном значении ε (E) равном 95.5.

Листинг 1 – Алгоритм выбора количества ГК для расчёта информативности

```
01  E = 95.5;
02  sum_explained = 0;
03  idx = 0;
04  while sum_explained < E
05       idx = idx + 1;
06       sum_explained = sum_explained + explained(idx);
07  end
08  idx
```

Результатом выполнения программы над анализируемым набором данных будет значение количества ГК (переменная idx), равное 5. Разработанное ПО, включающее в себя реализацию разработанных модели, метода и методики, зарегистрировано в реестре программ для ЭВМ и представлено в источнике [136].

Для непосредственного расчёта информативности используется массив *loadings*, строки которого упорядочены по источникам f_i, а столбцы содержат значения нагрузок **P** для каждой из *k* главных компонент. Старшинство ГК определяется бóльшим значением величины объяснённой дисперсии. На рисунке 21 представлен график нагрузок для двух старших ГК, по мере удаления от начала координат и увеличения абсолютных значений координат точки информативность соответствующего источника увеличивается, подписаны только наиболее информативные источники. Стоит отметить, что при разном количестве ГК (*k*) результаты расчёта информативности отличаются не существенно, главное влияние оказывают пять старших ГК.

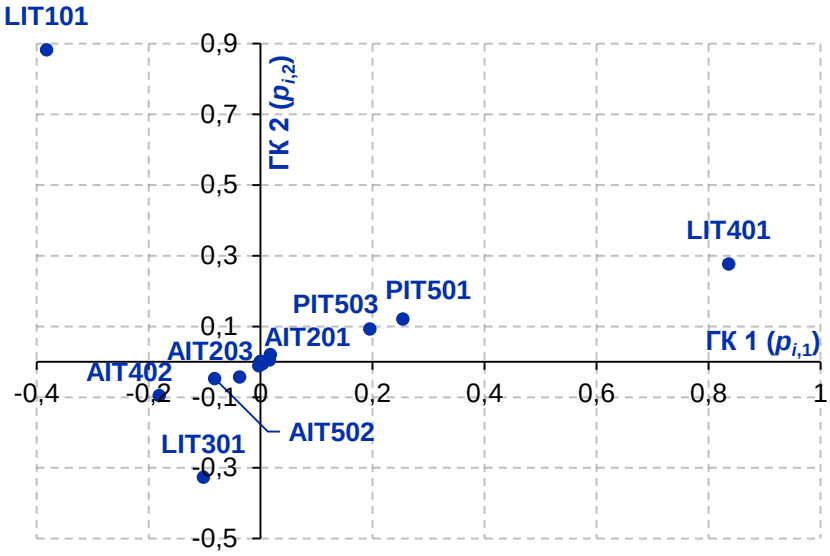

Рисунок 21 – График нагрузок при осуществлении атак на КФС

Информативность признаков по разработанному алгоритму рассчитана по формуле (12) и представлена в таблице 6. Серым цветом выделены наиболее информативные (по правилу Кайзера) признаки.

Таблица 6 – Значения информативности для 51 признака

f_i	LIT401	LIT101	LIT301	AIT201	PIT501	PIT503	AIT402
I_{f_i}	0,99913	0,99913	0,99896	0,94786	0,67211	0,51464	0,48828
f_i	AIT203	AIT502	DPIT301	AIT504	AIT503	FIT201	FIT101
$I(v_i)$	0,31012	0,22888	0,04848	0,02570	0,01251	0,00883	0,00726
f_i	FIT301	PIT502	FIT401	FIT501	MV201	P101	P205
I_{f_i}	0,00573	0,00558	0,00485	0,00476	0,00366	0,00361	0,00361
f_i	P203	FIT502	MV101	P501	UV401	P402	AIT202
I_{f_i}	0,00360	0,00352	0,00290	0,00289	0,00289	0,00272	0,00266
f_i	P302	MV302	P201	MV304	FIT503	AIT501	FIT504
I_{f_i}	0,00262	0,00259	0,00253	0,00216	0,00210	0,00095	0,00092
f_i	MV303	FIT601	P102	P602	MV301	AIT401	P403
I_{f_i}	0,00011	0,00010	0,00008	0,00006	0,00005	0,00002	0,00001

f_i	P204	P206	P202	P301	P401	P404	P502
$I(v_i)$	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000
f_i	P601	P603					
I_{f_i}	0,00000	0,00000					

Из 51 источника информации о функционировании КФС информативность девяти оказалась больше средней информативности, составившей $\bar{I} = 0{,}12410$, что позволило существенно сократить количество используемых для построения модели классификации признаков, уменьшив тем самым вычислительные затраты на обработку массива данных и увеличив скорость реагирования на инциденты ИБ.

Модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем, была применена для временных рядов, полученных в результате функционирования КФС водоочистки в безопасном и в потенциально опасных состояниях ИБ.

Таким образом, в результате применения разработанного алгоритма становится возможным выделить наиболее информативные признаки, используемые в дальнейшем в системах управления информационной безопасностью (*Security Information Management*) и управления событиями безопасности (*Security Event Management*).

4.4 Определение показателей качества идентификации состояния ИБ элементов КФС при использовании разработанных подходов

4.4.1 Система оценки показателей качества идентификации состояния ИБ элементов КФС

Поскольку разработанные метод и методика идентификации состояния ИБ элементов КФС базируются на классификации, то качество предложенных подходов зависит от полноты и точности проведённой классификации. В работе было использовано несколько подходов к оценке качества классификации, среди которых: матрица несоответствий (*confusion matrix*), точность (*precision*), полнота (*recall*), F-мера, площадь под ROC-кривой (AUC – *area under ROC curve*).

Результаты классификации демонстрируются при помощи матрицы несоответствий, для бинарной классификации состояний ИБ её структура приведена в таблице 7.

Таблица 7 – Матрица несоответствий для случая бинарной классификации

Генеральная совокупность		Реальное состояние ИБ	
		Небезопасное состояние	Безопасное состояние
Прогнозируемое состояние ИБ	Прогнозируемое состояние небезопасное	Истинно положительное (True Positive)	Ложно положительное (False Positive)
	Прогнозируемое состояние безопасное	Ложно отрицательное (False Negative)	Истинно отрицательное (True Negative)

В свою очередь, для бинарной классификации аномалий ИБ (по классам $\{C_0, C_1\} \subset C$) ROC-кривая позволяет оценить качество классификации и отображает зависимость доли истинно положительных классификаций от доли ложно положительных классификаций при варьировании порога решающего правила.

Количественную интерпретацию даёт площадь под ROC-кривой (AUC) — площадь, ограниченная ROC-кривой и осью доли ложных положительных классификаций. Чем выше показатель $AUC \in [0, 1]$, тем качественнее классификатор. На практике, от 0,5 («бесполезный» классификатор) до 1,0 («идеальная» модель).

В случае многоклассовой классификации матрица несоответствий принимает расширенный вид, показанный в таблице 8.

Таблица 8 – Матрица несоответствий для случая многоклассовой классификации

Генеральная совокупность		Реальное состояние ИБ			
		Состояние 1 c_1	Состояние 2 c_2	…	Состояние n c_n
Прогнозируемое состояние ИБ	Состояние 1 c_1	T_1	$F_{1,2}$	…	$F_{1,n}$
	Состояние 2 c_2	$F_{2,1}$	T_2	…	$F_{2,n}$
	…	…	…	…	…
	Состояние n c_n	$F_{n,1}$	$F_{n,2}$	…	T_n

Точность идентификации *accuracy* – отношение суммы верно идентифицированных небезопасных (True Positive) и безопасных (True Negative) состояний ИБ к общему объёму исследуемых состояний ИБ N, участвовавших в идентификации.

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN} = \frac{TP+TN}{N} \quad (19)$$

Для случая многоклассовой классификации состояний ИБ формула (19) принимает вид:

$$accuracy = \frac{\sum T_n}{\sum T_n + \sum F_n} = \frac{T_1 + T_2 + \cdots + T_n}{N}. \quad (20)$$

Стоит отметить, что некорректно использовать показатель *accuracy* в случае несбалансированной обучающей выборки. Даже при значении вышеуказанного показателя близком к единице, классификатор может определять некоторые из классов неудовлетворительно, если количество временных рядов этих классов в обучающей выборки мало.

Одним из выходов является создание сбалансированной обучающей выборки, но в данном случае у классификатора будет отсутствовать информация об относительной частоте и продолжительности атак. Данная информация при прочих равных может оказаться решающей для принятия правильного решения. В

этой связи, в настоящей работе были использованы нижеописанные показатели качества идентификации состояния ИБ КФС.

Точность идентификации состояния ИБ КФС в пределах класса (21) – это доля состояний ИБ, действительно принадлежащих данному классу, относительно всего количества состояний ИБ, которые алгоритм отнес к этому классу.

$$precision = \frac{TP}{TP+FP} \tag{21}$$

Полнота идентификации состояния ИБ КФС (22) – это доля верно идентифицированных классификатором состояний ИБ, принадлежащих определённому классу, относительно всего количества состояний ИБ этого класса в тестовой выборке.

$$recall = \frac{TP}{TP+FN} \tag{22}$$

F-мера представляет собой гармоническое среднее между точностью (21) и полнотой (22):

$$F = 2 \bullet \frac{precision \bullet recall}{precision + recall} \tag{23}$$

Формула (23) придает одинаковый вес точности и полноте, поэтому F-мера будет изменяться одинаково при изменении как точности, так и полноты.

4.4.2 Определение показателей качества идентификации при различном числе информативных признаков

С целью экспериментального подтверждения правила отбора количества наиболее информативных признаков на основе сравнения информативности каждого признака со средней информативностью, проведена сравнительная оценка AUC и F-меры при всех возможных значениях *s*, результаты эксперимента представлены на рисунке 22. При проведении эксперимента и построении графика в первую очередь использовались признаки с большей информативностью, вычисленной по формуле (12).

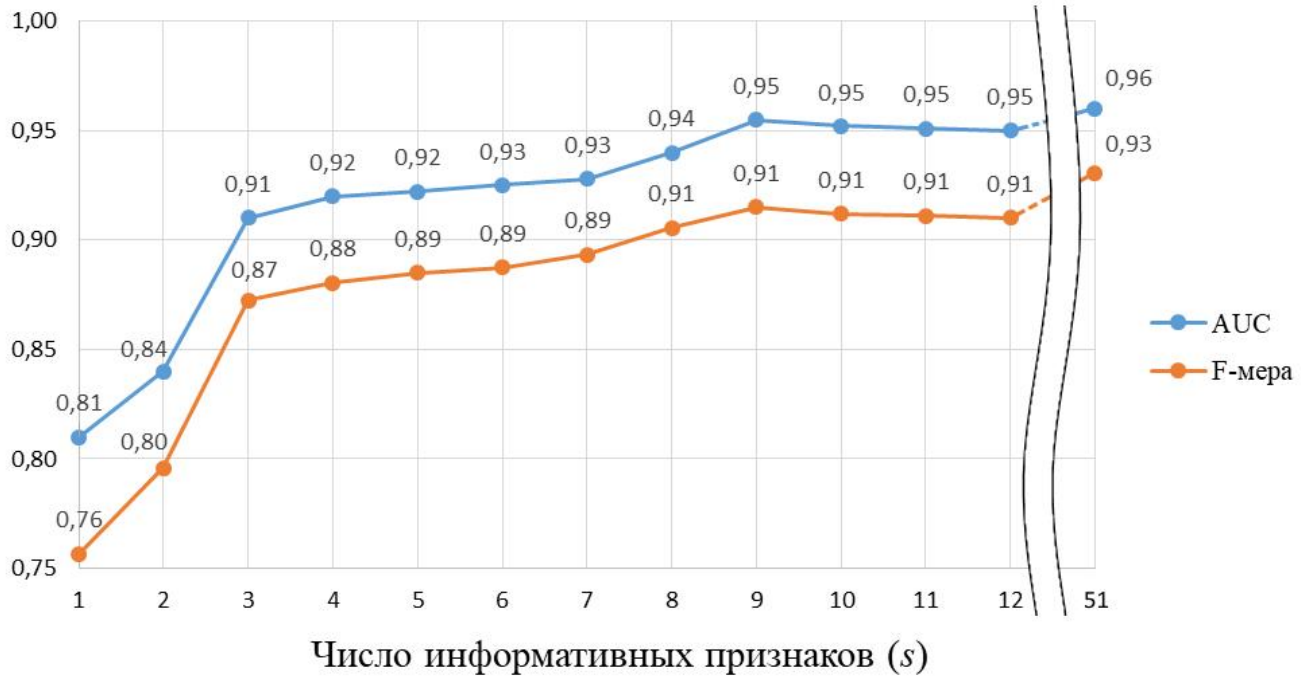

Рисунок 22 – Оценивание качества классификации при варьировании числа информативных признаков

Как было показано в п. 4.3 у 9 признаков, составляющих признаковое описание состояния ИБ КФС информативность выше средней, одновременно с этим на графике (рисунок 22) прослеживается локальный экстремум как у AUC, так и у F-меры при значении s, равном 9, что порождает второй возможный подход к выбору числа наиболее информативных признаков путём максимизации показателей качества идентификации состояния ИБ. Для различных КФС результат выбора s по модели, предложенной в п. 2.3 и путём максимизации показателей качества идентификации состояния ИБ далеко не всегда будет полностью совпадать. В работе был выбран именно критерий, описанный в п. 2.3, поскольку он позволяет сократить вычислительные затраты и существенно уменьшить время на принятие решения (выбор s). Эксперимент также показал, что характеристики классификации зависят не только от числа информативных признаков, но и от порядка их использования – предпочтительнее обучать классификатор на значениях наиболее информативных признаков.

При $s = 51$ показатель AUC увеличился всего на 0,01, а F-мера на 0,02 по сравнению с $s = 9$ что позволяет говорить о том, что большая часть источников

содержит шумовые данные и не способствует существенному увеличению качества классификации. В подтверждение этого равным образом свидетельствуют монотонный рост показателей качества идентификации и отсутствие значительных изменений при значениях $s > 9$.

На этапе обучения модели также производилась оценка временных затрат, заключающаяся в измерении времени, затраченного на обучение классификаторов на основе деревьев решений для разного количества признаков, по которым осуществлялось оценивание состояния ИБ.

Эксперимент показал закономерное увеличение времени обучения классификатора a_1 (для других параллельно работающих классификаторов наблюдалась аналогичная картина) при увеличении числа информативных признаков (рисунок 23).

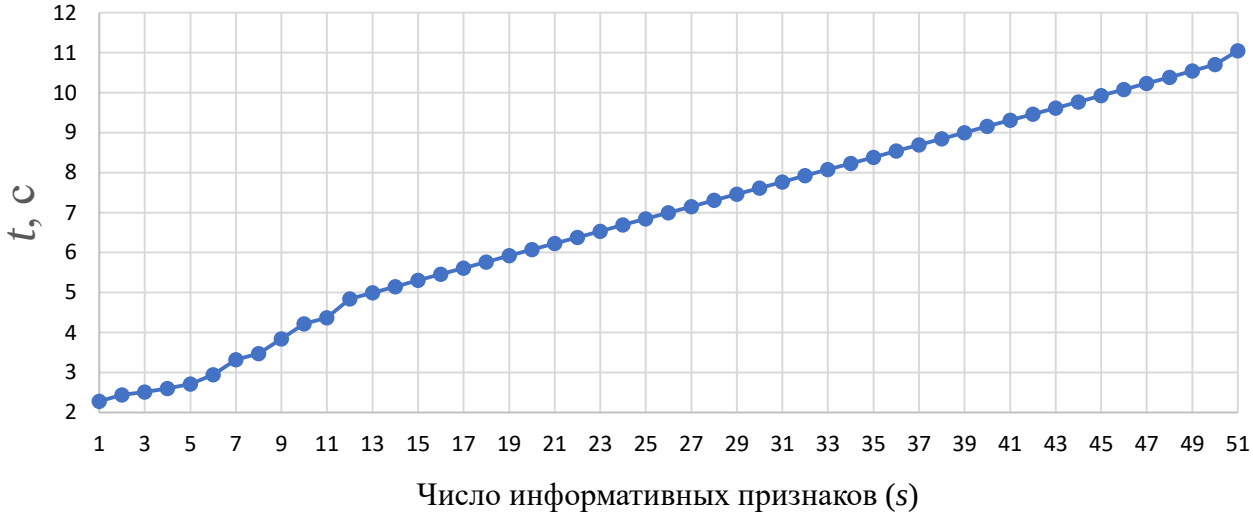

Рисунок 23 – Зависимость времени обучения классификатора a_1 от числа информативных признаков (s)

В случае крупномасштабных КФС снижение размерности признакового пространства приобретает особую актуальность из-за огромного количества данных, поступающих от систем мониторинга, требующих несоизмеримо высоких вычислительных мощностей для их обработки.

При количестве признаков, составляющих признаковое описание состояния ИБ согласно п. 4.3, а именно 9 для исследуемой КФС время, затраченное на

обучение модели, составило 3,84 с, что более чем в 3,5 раза быстрее, чем обучение на полном признаковом пространстве, включающим 51 признак.

Дерево решений (классификатор a_1) при девяти информативных признаках для случая бинарной классификации приняло вид, показанный на рисунке 24.

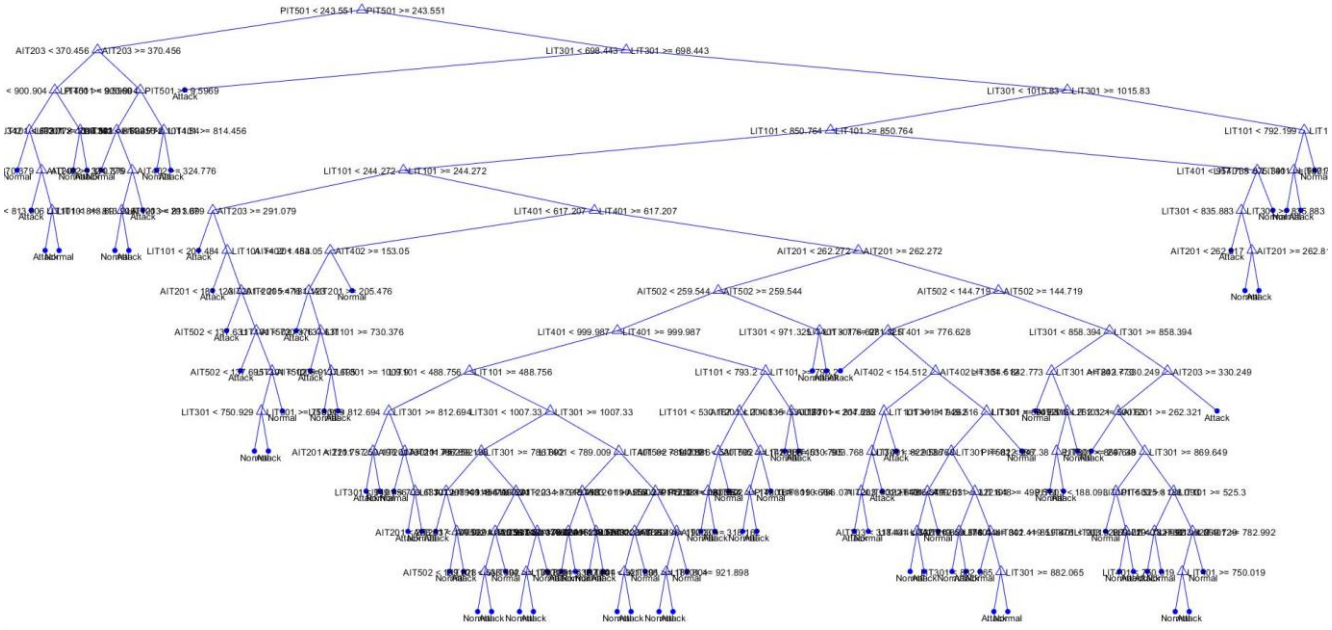

Рисунок 24 – Общий вид одного из деревьев решений

ROC-кривая идентификации состояния ИБ ансамблем параллельно работающих классификаторов при использовании признакового описания состояния ИБ (s = 9) представлена на рисунке 25.

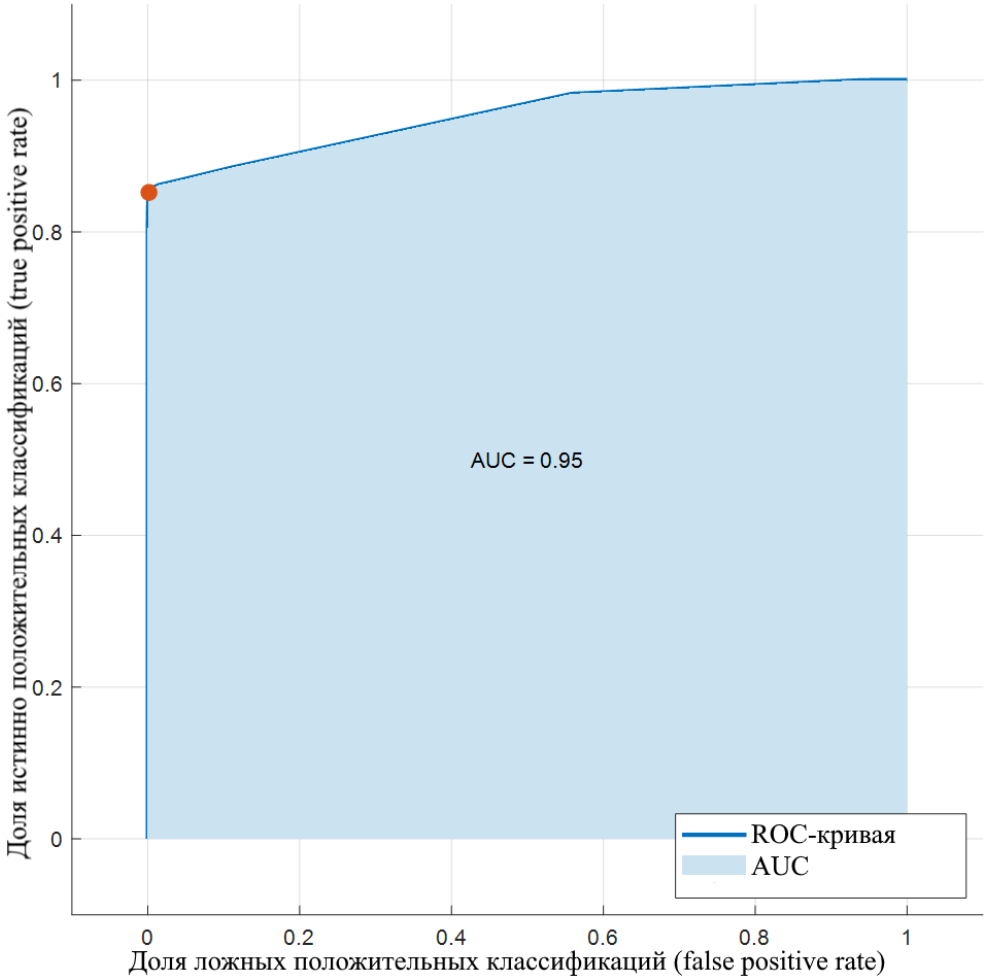

Рисунок 25 – ROC-кривая идентификации состояния ИБ при s = 9

Результаты бинарной классификации состояния ИБ КФС представлены в виде матриц несоответствий в таблице 9. C_0 – множество меток классов безопасных состояний ИБ КФС, C_1 – множество меток классов аномальных (опасных) состояний ИБ.

Таблица 9 – Матрица несоответствий, полученная в результате бинарной классификации состояний ИБ при s = 9 (а) и s = 51 (б), и характеристики классификации

(а) s = 9, AUC = 0,95		Истинный класс	
		C_1	C_0
Прогнозируемый класс	C_1	11634 10,34 % TP	148 0,13 % FP
	C_0	2021 1,80 % FN	98676 87,73 % TN
Точность			0,987
Полнота			0,852
F-мера			0,915

(б) s = 51, AUC = 0,96		Истинный класс	
		C_1	C_0
Прогнозируемый класс	C_1	12070 10,73 % TP	97 0,09 % FP
	C_0	1585 1,41 % FN	98727 87,77 % TN
Точность			0,992
Полнота			0,884
F-мера			0,935

Для случая сформированного признакового описания:

- ошибки первого рода (ложноположительные) 0,13 %, ошибки второго рода (ложноотрицательные) 1,80 %;
- полнота идентификации 0,852, что существенно ниже, чем на всём доступном наборе признаков и на фоне несбалансированной обучающей выборки демонстрирует недостаточную способность алгоритма, состоящего лишь из ансамбля параллельно работающих классификаторов (без постобработки) распознавать атаки.

4.4.3 Определение показателей качества идентификации при использовании весовых коэффициентов Фишберна

Постобработка результатов идентификации состояния ИБ КФС требует определения значения временного отрезка для расчёта весовых коэффициентов

Фишберна. С целью установления оптимального значения была проведена серия экспериментов, в которой последовательно при фиксированном значении $s = 9$ варьировалась величина временного отрезка (Δ) и вычислялись показатели качества идентификации при каждом значении Δ. Для этого, тестовая выборка, состоящая из 25 % исходных временных рядов, разделялась на Δ кластеров $X = \{\{x_1(t_1), x_2(t_1), \ldots, x_s(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_s(t_2)\}, \ldots, \{x_1(t_\Delta), x_2(t_\Delta), \ldots, x_s(t_\Delta)\}, \ldots, \{x_1(t_{m-\Delta}), x_2(t_{m-\Delta}), \ldots, x_s(t_{m-\Delta})\}, \ldots, \{x_1(t_{m-1}), x_2(t_{m-1}), \ldots, x_s(t_{m-1})\}, \{x_1(t_m), x_2(t_m), \ldots, x_s(t_m)\}\}$. Для каждого из кластеров X_i независимо определялась метка класса состояния ИБ. После применения весовых коэффициентов Фишберна итоговая метка класса присваивалась всем временным рядам i-го кластера.

Результаты приведены в виде графика на рисунке 26.

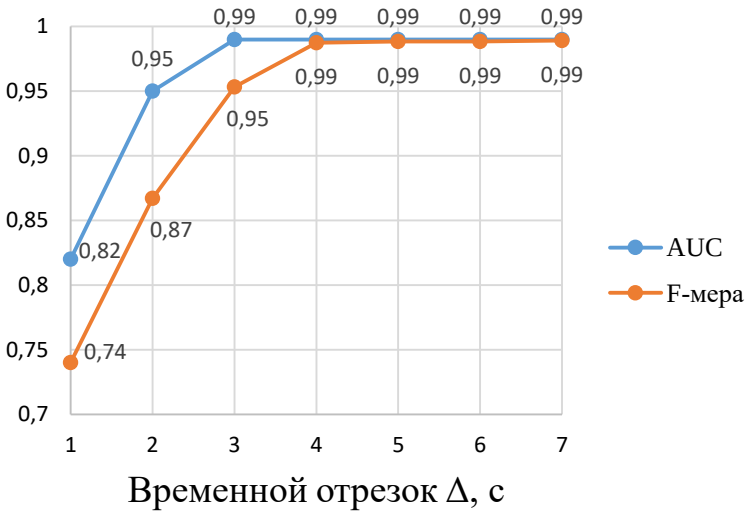

Рисунок 26 – Зависимость характеристик идентификации состояния ИБ от величины временного отрезка Δ при $s = 9$

Исходя из анализа результатов можно сделать вывод о том, что уже при значении $\Delta = 5$ наблюдается выход на плато показателей качества идентификации и дальнейшее увеличение временного отрезка не имеет смысла.

Цель второй серии экспериментов данного пункта – определить полноту, точность, F-меру идентификации, а также построить ROC-кривую, комплексно применяя при этом разработанный подход с учётом определённых ранее оптимальных параметров. Показатели качества идентификации состояния ИБ и

матрицы несоответствий после применения постобработки результатов классификации при помощи весовых коэффициентов Фишберна на отрезке времени Δ = 5 представлены в таблице 10.

Таблица 10 – Матрица несоответствий для бинарной классификации состояний ИБ при *s* = 9 (а) и *s* = 51 (б) и характеристики классификации после постобработки (Δ = 5)

(а) *s* = 9, AUC = 0,99		Истинный класс	
		C_1	C_0
Прогнозируемый класс	C_1	13638 12,12 % TP	26 0,02 % FP
	C_0	17 0,02 % FN	98798 87,84 % TN
Точность			0,998
Полнота			0,998
F-мера			0,998

(б) *s* = 51, AUC = 0,99		Истинный класс	
		C_1	C_0
Прогнозируемый класс	C_1	13645 12,13 % TP	10 0,01 % FP
	C_0	10 0,01 % FN	98814 87,85 % TN
Точность			0,999
Полнота			0,999
F-мера			0,999

Для случая сформированного признакового описания:

- ошибки первого рода 0,02 %, ошибки второго рода 0,02 %;
- полнота идентификации 0,998, что существенно выше, чем до применения постобработки результатов (таблица 9).

ROC-кривая идентификации состояния ИБ ансамблем параллельно работающих классификаторов при использовании признакового описания состояния ИБ (*s* = 9) и постобработки при Δ = 5 представлена на рисунке 27.

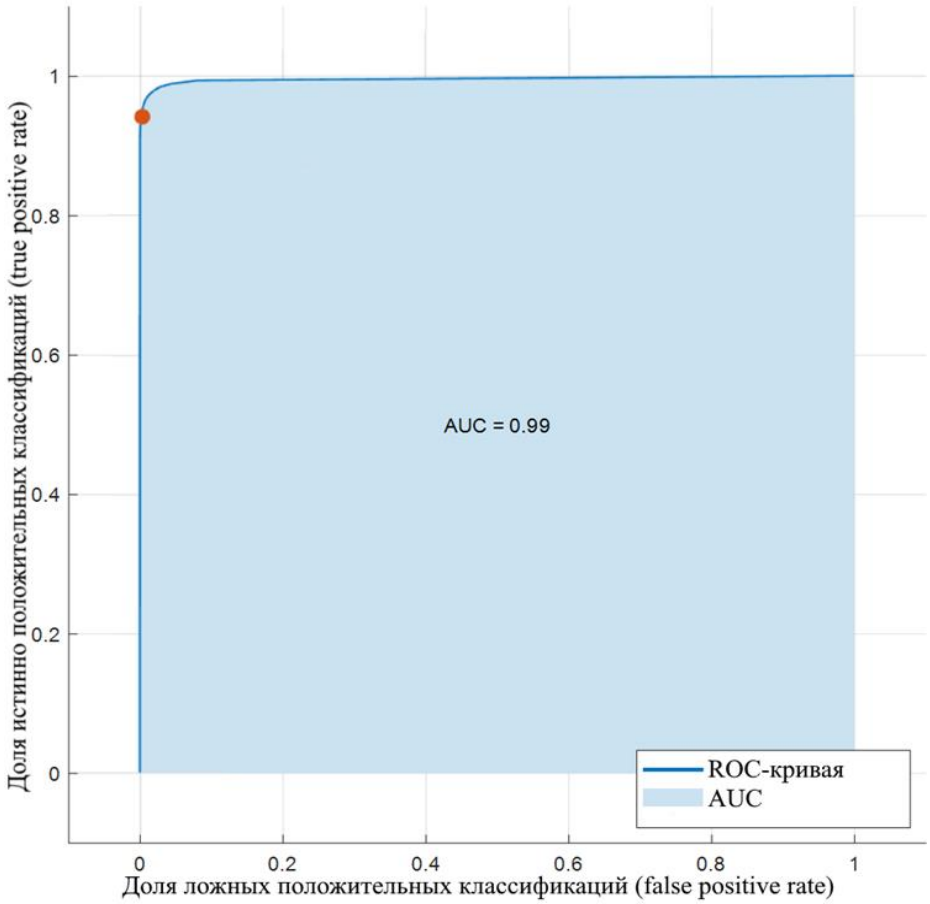

Рисунок 27 – ROC-кривая идентификации состояния ИБ при $s = 9$ с постобработкой ($\Delta = 5$)

Полученные результаты демонстрируют применимость разработанного метода и алгоритма, а также дают возможность провести многоклассовую классификацию на всей доступной детализации проведённых на КФС атак, описание которых дано в таблице 5. Таким образом, применение описанного метода позволяет повысить точность идентификации атак спуфинга (фальсификации данных) и отказа в обслуживании (флуд, атака по типу «воронка»).

4.4.4 Определение итоговых показателей качества идентификации на основе предложенной методики и сравнение полученных результатов

Произведено сравнение результатов проведённого исследования с результатами, полученными независимыми исследователями на идентичном наборе исходных данных.

В таблицу 11 сведены фамилии исследователей и применяемые ими методы.

Таблица 11 – Исследования, с которыми произведено сравнение результатов

Авторы исследования	**Применяемый метод**	**Обозначение**	**Источник**
Kravchik M., Shabtai A.	Одномерные свёрточные нейронные сети (one-dimensional convolutional neural networks)	1D СНС (1D CNN)	[137]
Shalyga D., Filonov P., Lavrentyev A.	Многослойный перцептрон (multilayered perceptron)	МП (MLP)	[138]
	Свёрточные нейронные сети (convolutional neural networks)	СНС (CNN)	
	Рекуррентные нейронные сети (recurrent neural networks)	РНС (RNN)	
Inoue J., Yamagata Y., Chen Y., Poskitt C.M., Sun J.	Глубинные нейронные сети (deep neural networks)	ГНС (DNN)	[139]
	Одноклассовый метод опорных векторов (one-class support vector machines)	МОВ (OCSVM)	
Kravchik M., Shabtai A.	Автоэнкодер (autoencoder)	АК (AE)	[140]
Elnour M., Meskin N., Khan K., Jain R.	Изолирующие леса (isolation forests)	ИЛ (IF)	[141]
Li D., Chen D., Jin B., Shi L., Goh J., Ng S.K.	Генеративно-состязательные сети (generative adversarial networks)	ГСНС (GAN)	[142]
Gomez A., Maimo L.,	Нейронные сети с долгой краткосрочной памятью	LSTM ИНС (LSTM NN)	[143]

Авторы исследования	Применяемый метод	Обозначение	Источник
Celdran A, Clemente F.	(long short-term memory neural networks)		

На рисунке 28 представлена диаграмма точности (*precision*). Обозначения методов в столбцах (рисунки 28 - 30) приведены согласно сокращениям в таблице 11. Три последних столбца на нижеследующих диаграммах отображают результаты диссертационной работы в сравнении с результатами других исследователей для набора экспериментальных данных [135]. Столбец «s = 9» содержит результаты для числа информативных признаков, составляющего признаковое описание состояния ИБ КФС (без постобработки), столбец «s = 51» – для всего доступного признакового пространства (без постобработки), а крайний правый столбец – результат комплексного применения методики при s = 9 и Δ = 5.

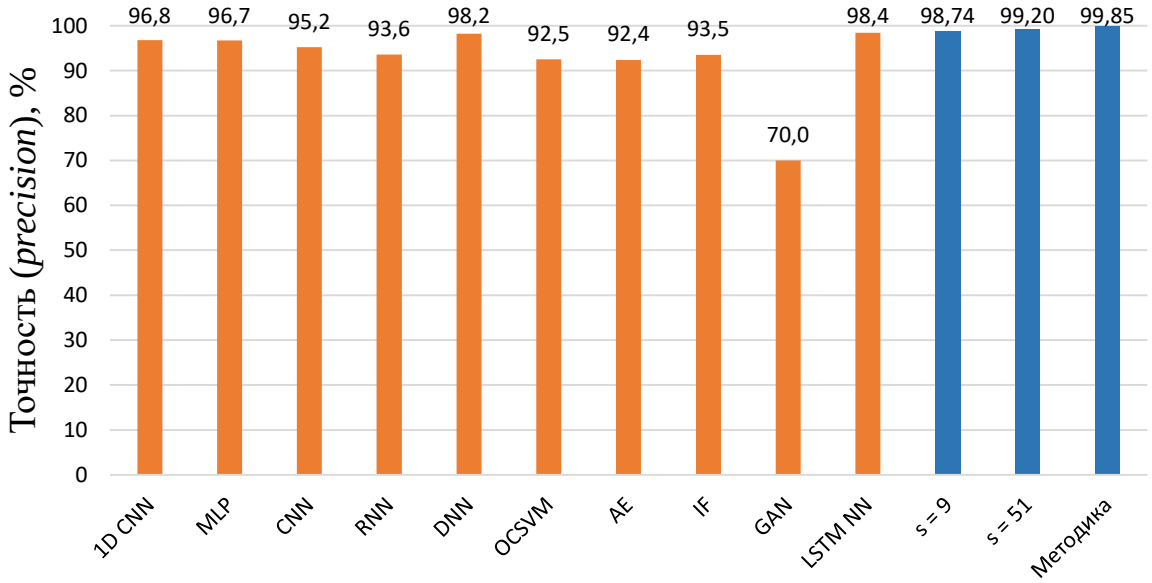

Рисунок 28 – Сравнение точности идентификации состояния ИБ

Как видно из диаграммы, точность идентификации состояния ИБ элементов КФС с применением методики существенно выше, чем в работах других исследователей, применивших иные по природе классификаторы и методы предварительной обработки данных. Разработанная методика позволила также повысить полноту (*recall*) идентификации состояния ИБ КФС (рисунок 29).

Методики с высокой полнотой классификации предпочтительнее для распознавания ранее неизвестных типов аномалий [144].

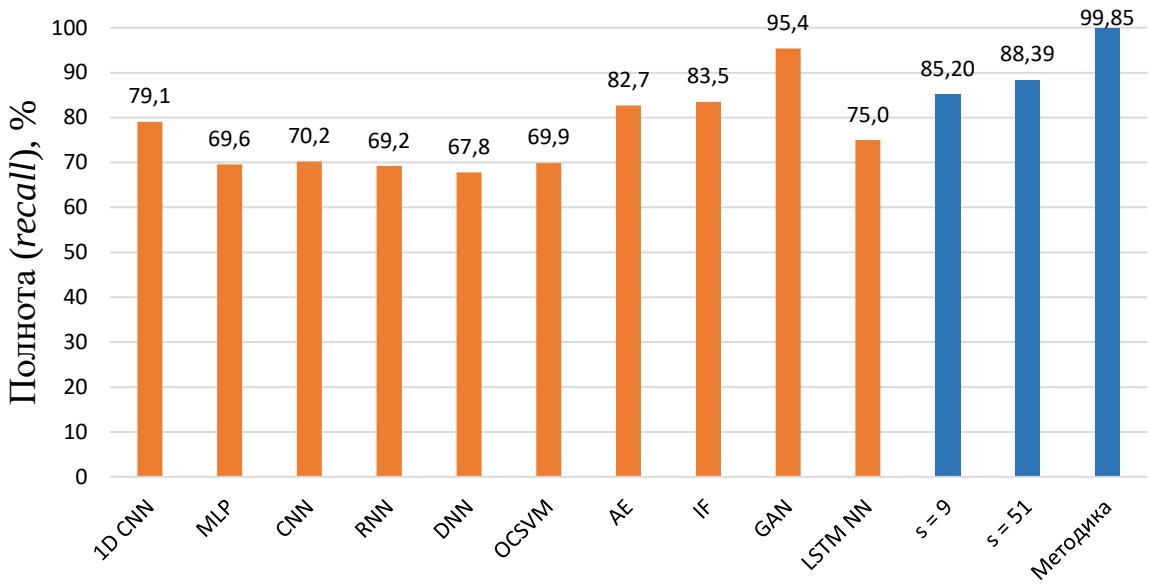

Рисунок 29 – Сравнение полноты идентификации состояния ИБ

При анализе диаграмм стоит отметить, что проанализированные работы других исследователей характеризуются недостаточной полнотой идентификации состояний ИБ КФС, что является существенным недостатком, поскольку такие модели могут идентифицировать значительное число атак на КФС как безопасные состояния ИБ. F-мера закономерно выравнивается за счёт точности идентификации (рисунок 30).

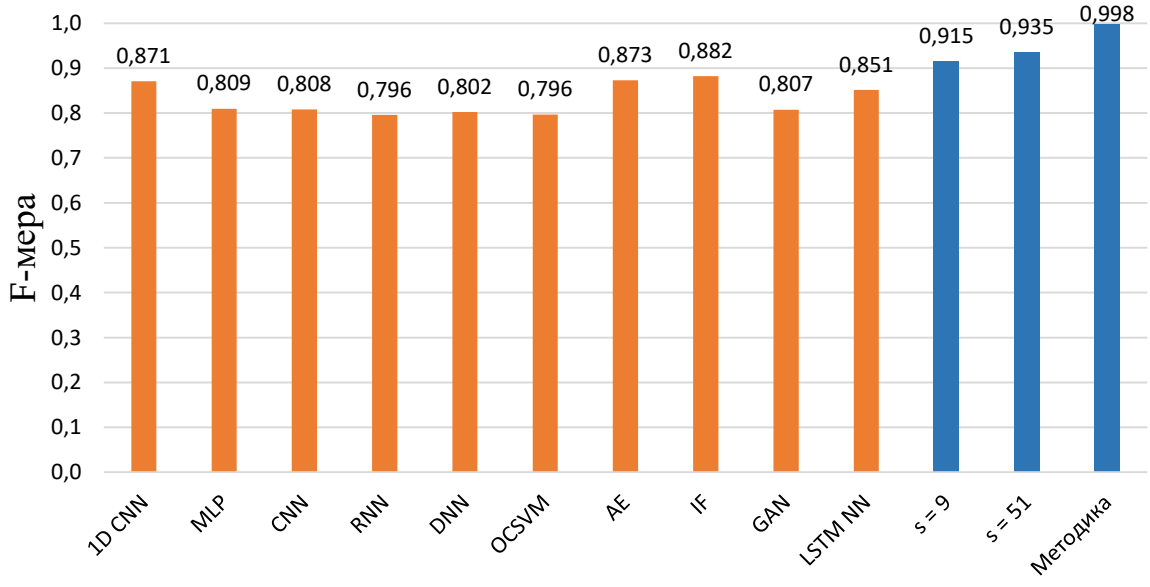

Рисунок 30 – Сравнение F-меры идентификации состояния ИБ

Заключительным этапом эксперимента являлась проверка возможности корректно идентифицировать атаки различного типа на КФС и её отдельные элементы. В таблице 12 приведены результаты для классов c_1 – c_{41}, детальное описание атак приведено в таблице 5.

Таблица 12 – Сравнение полноты идентификации различных подходов

Состояние	**DNN** [139]	**RNN** [138]	**OCSVM** [139]	**1D CNN** [137]	**IF** [141]	**LSTM NN** [143]	**Разработанная методика**
c_1	-	-	-	0,99	0,01	-	0,99
c_2	-	-	-	1,00	0,29	1,00	1,00
c_3	-	-	-	0,23	1,00	-	1,00
c_4	-	-	0,04	-	-	-	0,94
c_6	0,95	0,72	0,72	0,90	1,00	-	1,00
c_7	0,91	-	0,89	1,00	1,00	0,97	1,00
c_8	0,98	0,93	0,92	1,00	1,00	0,95	1,00
c_{10}	0,98	1	0,43	1,00	1,00	1,00	1,00
c_{11}	0,99	0,98	1,00	1,00	1,00	1,00	1,00
c_{13}	-	-	-	-	-	-	0,97
c_{14}	-	-	-	-	0,06	-	0,96
c_{16}	0,60	-	-	0,24	0,55	-	0,97
c_{17}	-	-	-	0,63	0,64	0,56	0,95
c_{19}	0,97	0,12	0,13	-	0,45	-	0,99
c_{20}	-	0,85	0,85	1,00	0,45	-	0,97
c_{21}	0,98	-	0,02	0,91	-	-	0,99
c_{22}	0,98	0,99	1,00	1,00	1,00	1,00	1,00
c_{23}	0,71	0,88	0,88	1,00	0,82	0,94	1,00
c_{24}	0,92	-	-	0,17	0,34	0,53	0,98
c_{25}	0,29	-	0,01	0,02	1,00	0,01	0,96
c_{26}	0,99	-	-	1,00	0,17	1,00	0,99

Состояние	**DNN** [139]	**RNN** [138]	**OCSVM** [139]	**1D CNN** [137]	**IF** [141]	**LSTM NN** [143]	**Разработанная методика**
c_{27}	-	-	-	0,06	-	0,31	0,97
c_{28}	0,03	0,94	0,94	1,00	1,00	0,97	1,00
c_{29}	0,87	-	-	-	1,00	-	1,00
c_{30}	0,83	-	-	1,00	-	1,00	1,00
c_{31}	0,78	-	-	0,30	1,00	0,34	1,00
c_{32}	0,33	-	0,91	0,94	1,00	0,25	1,00
c_{33}	0,84	-	-	0,89	0,43	0,25	0,98
c_{34}	-	-	-	0,99	-	0,67	1,00
c_{35}	-	-	-	-	0,95	-	0,97
c_{36}	0,81	-	0,12	0,88	0,93	0,89	0,99
c_{37}	0,84	1,00	1,00	0,90	1,00	0,92	1,00
c_{38}	0,77	0,92	0,93	0,86	1,00	0,01	1,00
c_{39}	0,84	0,94	-	0,91	1,00	0,92	1,00
c_{40}	0,78	0,93	0,93	1,00	1,00	1,00	1,00
c_{41}	-	-	0,36	0,64	0,63	0,53	0,98

Таким образом, при помощи серии экспериментов продемонстрированы результаты, достаточные для практического применения разработанной методики в системах мониторинга состояния ИБ КФС. Значения полноты идентификации инцидентов ИБ свидетельствуют о том, что многие классы атак идентифицируются без ошибок. За счёт применения разработанного подхода удалось существенно повысить точность идентификации деструктивных информационных воздействий и сократить время, затраченное на обработку сигнальной информации от элементов КФС.

4.5 Использование результатов исследования для повышения защищённости КФС от внешних воздействий

Проведённое исследование направлено на развитие подходов к выявлению нарушений ИБ КФС на основе анализа временных рядов, отражающих информационные и физические процессы КФС, что позволяет усовершенствовать и дополнить модели, методы, методики общей теории ИБ, и в последующем использовать разработанные модель, метод и методику в системах, обеспечивающих бесперебойное выполнение целевой функции КФС.

Поскольку ключевой задачей функционирования КФС является бесперебойное выполнение целевых функций, выявление нарушений ИБ КФС представляет собой важную и необходимую в сегодняшних реалиях задачу. До применения методики реализация угрозы с использованием уязвимостей системы со стороны злоумышленника может быть произведена, как показано на рисунке 31.

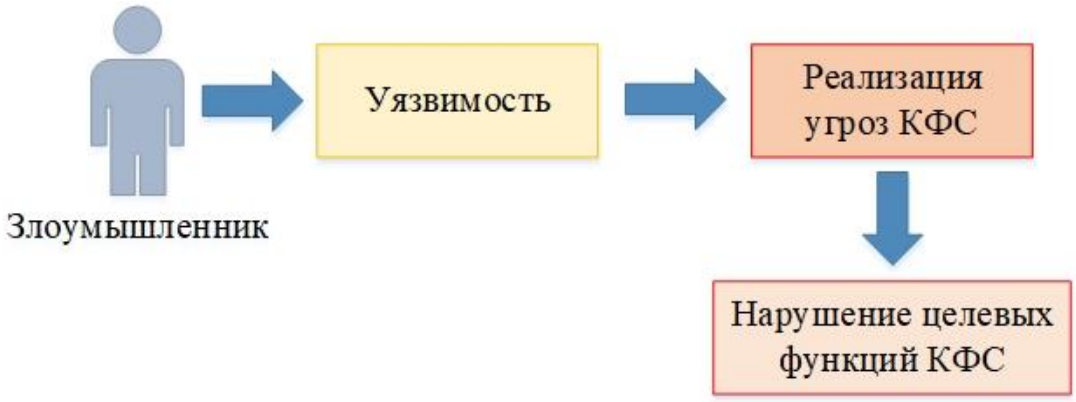

Рисунок 31 – Воздействие злоумышленника на КФС

В общем виде рассматривая множество состояний ИБ КФС, необходимо обратиться к рисунку 32, где представлены 4 базовых состояния ИБ.

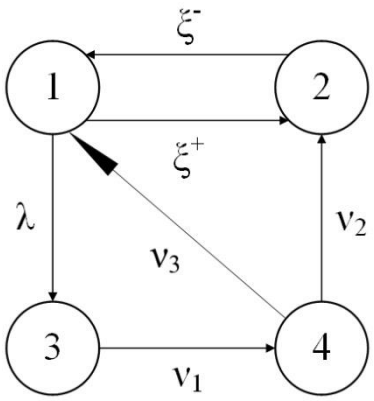

Рисунок 32 – Граф состояний ИБ

Базовое состояние 1 – это состояние ИБ КФС в начальный момент времени, при котором КФС начинает функционирование, а контролирующая система - мониторинг.

Базовое состояние 2 – это состояние ИБ, которое характеризует достижение целевой функции КФС. В состоянии 2 существует несколько вариантов развития ситуации:

- срыв выполнения целевой функции (ζ^-) при успешной реализации угроз КФС. В случае срыва выполнения задач система окажется в состоянии 1;
- ζ^+ характеризуется корректной работой системы идентификации состояния ИБ, КФС остается в состоянии 2.

λ – характеризует внешнее воздействие на КФС. Базовое состояние 3 требует задействования ресурсов КФС, или привлеченных к решению специалистов. В любом случае (реализация угроз злоумышленника или случайное воздействие) система оказывается в состоянии 4.

ν_1 – характеризует частоту мониторинга состояния ИБ;

ν_2 – характеризует частоту реагирования системы идентификации состояния ИБ с учётом задействованных ресурсов;

ν_3 – характеризует частоту срыва устранения негативного воздействия на КФС.

Базовое состояние 4 − это ситуация при которой принимаются меры по полученным данным мониторинга. Из состояния 4 происходит переход в состояние 1 при неблагоприятном исходе. В случае корректного и своевременного реагирования на инцидент ИБ происходит переход в наиболее благоприятное состояние 2.

Применение разработанной методики способно предотвратить описанные сценарии воздействия злоумышленника и случайных факторов. Предлагаемая методика идентификации состояния ИБ может быть применена с целью оценивания защищённости КФС от информационных угроз, путем внедрения в качестве технической меры по аудиту ИБ КФС в период эксплуатации (рисунок 33).

Рисунок 33 – Схема возможного повышения степени защищённости КФС

Необходимо отметить смежные задачи, решаемые разработанной методикой:

- выявление нарушений, вызванных случайными воздействиями на КФС и не связанных с умышленными действиями вероятных нарушителей;
- выявления отклонений в параметрах функционирования, вызванные износом технологических узлов КФС.

Обладая полной и актуальной информацией о текущем состоянии ИБ объекта становится возможным существенно повысить степень защищённости КФС, ускорить быстроту реагирования на инциденты (в том числе с использованием

динамического переконфигурирования, обеспечивающего возвращение системы в устойчивое состояние ИБ), снизив тем самым влияние неблагоприятных факторов на функционирование КФС. Результатом применения разработанного подхода для проактивной ИБ является повышение степени защищённости КФС.

В том случае, если инцидент ИБ уже произошёл, разработанная методика может применяться в качестве апостериорной защиты, которая помогает найти виновного в выявленном инциденте. Результатом применения методики в данном случае является выработка защитных мер, снижающих вероятность подобных инцидентов в процессе дальнейшей эксплуатации (рисунок 34).

Рисунок 34 – Цикл обеспечения ИБ КФС, учитывающий разработанные методы

В работах [145-147] представлен подход к обеспечению информационной и функциональной безопасности различных объектов на основе принципа обратной

связи. Исследования данного подхода могут являться следующим этапом в задаче разработки и реализации систем комплексного обеспечения ИБ элементов КФС. На рисунке 35 показана возможность применения разработанных методов анализа временных рядов КФС и методики идентификации состояния ИБ элементов КФС в рамках концепции поддержания устойчивого функционирования КФС в условиях воздействия угроз.

Рисунок 35 – Концепция поддержания устойчивого функционирования КФС на основе принципа обратной связи

Временная схема реализации основных элементов предлагаемого подхода представлена на рисунке 36: (а) – среднее время выполнения целевой функции КФС $T_э$, (б) – среднее время проявления проблемы $\Delta t_{ПП}$, (в) – среднее время идентификации проблемы $\Delta t_{ИП}$, (г) – среднее время нейтрализации проблемы $\Delta t_{НП}$.

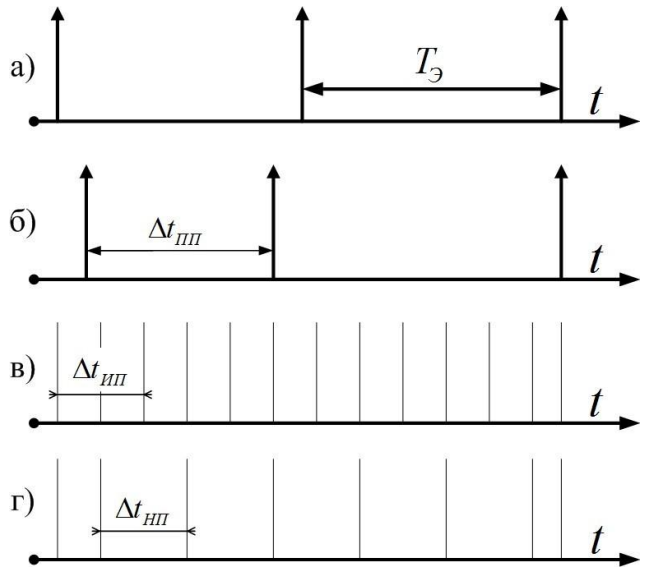

Рисунок 36 – Временная схема реализации основных элементов подхода комплексного обеспечения безопасного функционирования КФС

Технология динамической защиты, включающая в том числе разработанную методику идентификации состояния ИБ элементов КФС достаточно сложна в реализации, и её внедрение является перспективной задачей.

4.6 Выводы по главе 4

В четвёртой главе показана экспериментальная реализация методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов, использующая методы их обработки. Полнота и точность идентификации при применении методики оценена на основе серии экспериментов. Произведено сравнение показателей качества идентификации с результатами других исследователей, применивших различные методы предобработки и последующей классификации временных рядов, характеризующих функционирование КФС.

Приведены ограничения методики, к которым можно отнести количество различных состояний ИБ КФС в обучающей выборке и, исходя из этого, неспособность классификатора сформировать корректный результат для состояния ИБ, если оно не было определено на этапе обучения.

Разработаны практические рекомендации по применению методики для повышения защищённости КФС, включающие в себя варианты получения

сигнальной информации о параметрах функционирования системы, а также использования исполнительных ресурсов системы для нейтрализации угрозы и возвращения системы в безопасное состояние ИБ.

Сформулированы перспективы области исследования, состоящие в разработке методов реагирования на выявленные нарушения ИБ КФС на основе принципа обратной связи.

Достоинствами данного подхода является возможность быстрой адаптации под конкретный тип КФС с применением различного математического аппарата и методов машинного обучения с целью получения заданной полноты и точности идентификации состояния ИБ. Дальнейшие исследования в данной области могут быть связаны с интеграцией разработанной методики в системы комплексного обеспечения информационно-функциональной безопасности КФС.

Таким образом, предложенные модель, метод и методика являются как новой альтернативой, так и дополнением к существующим программным и программно-аппаратным средствам, и использоваться для выявления нарушений ИБ КФС. При необходимости и соответствующей настройке, контролирующая система может блокировать небезопасные состояния ИБ устройств в режиме реального времени.

ЗАКЛЮЧЕНИЕ

В диссертационной работе решена задача повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз. Решённая задача имеет важное значение для совершенствования моделей, методов и средств обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.

Основные научные результаты, составляющие **итоги** выполненного исследования:

1. Проанализированы существующие подходы к выявлению нарушений ИБ КФС, показаны достоинства и недостатки рассмотренных методов.
2. Разработана модель угроз информационной безопасности объектов исследования, определены угрозы ИБ, характерные для различных типов КФС.
3. Разработан алгоритм, способный из доступного числа параметров КФС выявить наиболее информативные для данной КФС и использовать их для формирования признакового описания состояния ИБ КФС.
4. Разработан метод оценивания состояния ИБ элементов КФС, основанный на применении ансамбля параллельно работающих классификаторов и весовых коэффициентов Фишберна в качестве постобработки результатов классификации.
5. Разработана методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности и полноты, уменьшив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС.
6. Разработан прототип программного обеспечения, реализующий оценивание защищённости КФС от информационных угроз на основе анализа временных рядов;

7. Применимость разработанных модели, метода и предложенной методики идентификации состояния ИБ КФС обоснована при помощи вычислительного эксперимента. Произведена оценка характеристик классификации и сравнение с существующими методами.

Все выносимые на защиту результаты являются новыми и получены соискателем самостоятельно. При совокупном применении разработанных модели, метода и методики достигается значение F-меры 0,998 что на 0,116 превышает наиболее результативный из представленных на сегодняшний день в мировой научной литературе подход на основе изолирующих лесов [141].

Даны **рекомендации** по использованию результатов исследования для повышения защищённости КФС от внешних информационных воздействий. Разработанная методика, а также модель и метод, направленный на повышение полноты и точности идентификации состояния ИБ, могут быть применены на предприятиях промышленности и при выполнении научных исследований. Разработанные алгоритмы могут быть использованы в системах управления событиями информационной безопасности, системах обнаружения атак, поскольку они представляют собой инструмент мониторинга инцидентов информационной безопасности КФС.

В качестве **перспектив дальнейшей разработки темы** можно указать исследования, связанные с разработкой методов и методик противодействия выявленным нарушениям ИБ на основе принципа обратной связи в режиме реального времени, а также апробацию разработанного прототипа программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз, на принципиально других типах КФС.

Полученные результаты соответствуют паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АСУ	Автоматизированные системы управления
БС	Байесовская сеть
ГК	Главная компонента
ДМЗ	Демилитаризованная зона
ИБ	Информационная безопасность
ИНС	Искусственная нейронная сеть
ИС	Информационные системы
КФС	Киберфизическая система
МГК	Метод главных компонент
ПЛК	Программируемый логический контроллер
ПО	Программное обеспечение
СЗИ	Средства защиты информации
ЧМИ	Человеко-машинный интерфейс
СММ	Скрытая марковская модель
AUC	Area under ROC curve
DDoS	Distributed Denial of Service
ERV	Explained Residual Variance
KICS	Kaspersky Industrial CyberSecurity
ROC	Receiver operating characteristic
SCADA	Supervisory Control And Data Acquisition

СПИСОК ЛИТЕРАТУРЫ

1. Бажаев Н.А., Кривцова И.Е., Лебедев И.С. Исследование доступности удаленных устройств беспроводных сетей // Научно-технический вестник информационных технологий, механики и оптики. –2016. –Т. 16. – № 3. – С. 467–473.

2. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. -2018. - № 2 (26).

3. Постановление Правительства РФ от 18.04.2016 N 317 "О реализации Национальной технологической инициативы".

4. Ронжин А.Л., Басов О.О., Соколов Б.В., Юсупов Р.М. Концептуальная и формальная модели синтеза киберфизических систем и интеллектуальных пространств // Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59. – № 11. – С. 897-905.

5. Sanfelice R. G. Analysis and Design of Cyber-Physical Systems. A Hybrid Control Systems Approach // Cyber-Physical Systems: From Theory to Practice / Rawat D., Rodrigues J., Stojmenovic I. — CRC Press. — 2016. — ISBN 978-1-4822-6333-6.

6. Киберфизическая система — Википедия [сайт]. URL: https://ru.wikipedia.org/wiki/Киберфизическая_система (дата обращения 07.07.2020).

7. Сухопаров М.Е., Семенов В.В., Лебедев И.С., Гаранин А.В. Подход к анализу состояния узлов «Индустрии 4.0» на основе поведенческих паттернов // Наукоемкие технологии в космических исследованиях Земли -2020. - Т. 12. - № 5. С. 83-91.

8. Платунов А.Е. Встраиваемые системы управления // Control Engineering Россия. -2013. - Т. 43. - № 1. - С. 16-24.

9. Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A. Watch me, but don’t touch me! Contactless control flow monitoring via electromagnetic emanations // Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security. -2017. - C. 1095-1108.

10. Boggs N., Chau J. C., Cui A. Utilizing electromagnetic emanations for out-of-band detection of unknown attack code in a programmable logic controller // Proc. SPIE 10630, 2018.

11. Riley R., Graham J. T., Fuller R. M., Baldwin R. O., Fisher A. Generalization of algorithm recognition in rf side channels between devices // Proc. SPIE 10630, 2018.

12. Werner F. T., Djordjevi´c A. R., Ol´can D. I., Prvulovic M., Zaji´c A. Experimental validation of localization method for finding magnetic sources on iot devices // International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018, pp. 413–418.

13. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. М.: Стандартинформ, 2014. 22 с.

14. Xiao Y., Xu W., Jia Z., Ma Z., Qi D. Nipad: a non-invasive power-based anomaly detection scheme for programmable logic controllers // Frontiers Inform. Technol. Electron. Eng. -2017. - Т. 18. -№. 4. -С. 519–534. doi: 10.1631/FITEE.1601540.

15. Kocher P., Jaffe J., Jun B. Introduction to differential power analysis and related attacks // Proc. CRYPTO'98, 1998. LNCS 1109, P. 104–113.

16. Leyden J. Polish teen derails tram after hacking train network // The Register. - 2008. -№ 11.

17. Slay J., Miller M. Lessons learned from the Maroochy water breach // Proc. Int. Conf. Critical Infrastructure Protection. - 2007. - С. 73–82.

18. Falliere N., Murchu L. O., Chien E. W32. Stuxnet dossier // Symantec Security Response. - 2011. -T. 5. -№ 6. -C. 29.

19. Bertino E., Islam N. Botnets and Internet of Things security // Computer. - 2017. - T. 50. -№ 2. -C. 76–79. doi: 10.1109/MC.2017.62.

20. Zhang N. Understanding IOT security through the data crystal ball: Where we are now and where we are going to be // arXiv Preprint. -2017. -№ 1703.09809.

21. Петров В.В. Исследование самоподобной структуры телетрафика беспроводной сети / В.В. Петров, В.В. Платов // Радиотехнические тетради. - 2004. - № 30. - С. 58-62.

22. Abdulmalik H., Jingqiang L., Fengjun L., Bo L. Cyber-Physical Systems Security – A Survey // IEEE Internet of Things Journal –2017. –Т. 4 –№ 6. –С. 1802-1831.

23. Hutter M., Schmidt J.-M. The temperature side channel and heating fault attacks // Proc. Int. Conf. Smart Card Research and Advanced Applications, 2013, pp. 219–235.

24. Genkin D., Shamir A., Tromer E. Rsa key extraction via low-bandwidth acoustic cryptanalysis // Proc. Int. Cryptology Conf., 2014, pp. 444–461.

25. Kuhn M. Optical Time-Domain Eavesdropping Risks of CRT Displays // Proc. of the 2002 Symposium on Security and Privacy, 2002, pp. 3–18.

26. Минзов А.С., Невский А.Ю., Баронов О. Ю. Информационная безопасность в цифровой экономике // ИТНОУ: информационные технологии в науке, образовании и управлении. – 2018. №3 (7). – С. 52-59.

27. Водяхо А.И., Осипов В.Ю., Жукова Н.А., Червонцев М.А. Когнитивные технологии в управлении мониторингом // Научно-техническая информация. Серия 2: Информационные процессы и системы. № 4. 2019. С. 1-12.

28. Semenov V.V., Sukhoparov M.E., Lebedev I.S. Approach to the State Analysis of Industry 4.0 Nodes Based on Behavioral Patterns. Lecture Notes in Computer Science. Vol. 12336. 2020. pp. 273-282.

29. Ворона В.А., Костенко В.О. Способы и средства защиты информации от утечки по техническим каналам // Comput. Nanotechnol. -2016. - № 3. - С. 208–223.

30. Семенов В.В., Лебедев И.С., Сухопаров М.Е. Подход к классификации состояния информационной безопасности элементов киберфизических систем с использованием побочного электромагнитного излучения // Научно-технический вестник информационных технологий, механики и оптики -2018. -№1(113). -С.98-105.

31. Павленко Е.Ю. Обеспечение информационной безопасности киберфизических систем на основе принципа гомеостаза: дис. … канд. техн. наук. СПбПУ Петра Великого, Санкт-Петербург, 2018.

32. Zegzhda D.P. Sustainability as a criterion for information security in cyberphysical systems / D. P. Zegzhda // Automatic Control and Computer Sciences. – 2016. – № 8. – С. 813-819.

33. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: Стандартинформ, 2018. 20 с.

34. Sukhoparov M.E., Lebedev I.S., Semenov V.V. Information Security State Analysis of Elements of Industry 4.0 Devices in Information Systems. Lecture Notes in Computer Science. Vol. 12525. 2020. pp. 119-125.

35. Королев В.И. Методология построения модели угроз безопасности территориально-распределенных объектов / В. И. Королев // Технология техносферной безопасности: интернет-журнал. –2013. – № 2 (48).

36. Семенов В.В., Лебедев И.С., Сухопаров М.Е. Идентификация состояния отдельных элементов киберфизических систем на основе внешних поведенческих характеристик // Прикладная информатика -2018. - Т. 13. - № 5(77). - С. 72-83.

37. Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. – 2020. – № 5 (19). – С. 1050-1088.

38. Викснин И.И. Модель обеспечения информационной безопасности киберфизических систем // Наука и бизнес: пути развития -2018. - № 2(80). - С. 15-20.

39. Dzung D., Naedele M., Von Hoff T.P. Security for industrial communication systems // Proc. IEEE, 2005, 93, (6), pp. 1152–1177.

40. ГОСТ ISO/IEC 27001 Information technology – security techniques – information security management systems – requirements, 2013.

41. Semenov V.V., Sukhoparov M.E., Lebedev I.S. Approach to Side Channel-Based Cybersecurity Monitoring for Autonomous Unmanned Objects // Lecture Notes in Computer Science, 2019, Vol. 11659, pp. 278-286.

42. Сухопаров М.Е., Семенов В.В., Салахутдинова К.И., Лебедев И.С. Выявление аномального функционирования устройств индустрии 4.0 на основе поведенческих паттернов // Проблемы информационной безопасности. Компьютерные системы - 2020. - № 1. - С. 96-102.

43. Сухопаров М.Е., Семенов В.В., Салахутдинова К.И., Лебедев И.С. Выявление аномалий функционирования телекоммуникационных устройств на основе локальных сигнальных спектров // Проблемы информационной безопасности. Компьютерные системы -2020. - № 2. - С. 29-34.

44. Stouffer K., Falco J., Scarfone K. Guide to industrial control systems (ICS) security // NIST Spec. Publ., 2011, 800, (82), pp. 29–32.

45. NIST Cybersecurity Framework Framework for improving critical infrastructure cybersecurity, 2014.

46. ГОСТ IEC 62351 Security standards for the power system information infrastructure, 2014.

47. Pfleeger C., Pfleeger S. Security in Computing (4th Edition) // Prentice Hall PTR, Upper Saddle River, NJ, USA, 2006.

48. Семенов В.В., Арустамов С.А. Выявление рисков нарушений информационной безопасности киберфизических систем на основе анализа цифровых сигналов // Научно-технический вестник информационных технологий, механики и оптики -2020. -Т.20. - №5(129). -С. 770-772.

49. Barman S. Writing Information Security Policies. // New Riders, 2002.

50. Cheminod M., Durante L., Valenzano A. Review of security issues in industrial networks // IEEE Trans. Ind. Inf., 2013, 9, (1), pp. 277–293.

51. Peng Y., Lu T., Liu J. Cyber-physical system risk assessment // Proc. 9th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing. – 2013. – С. 16–18.

52. Chilenski M., Cybenko G., Dekine I., Kumar P., Raz G. Control flow graph modifications for improved rf-based processor tracking performance // Proc. SPIE 10630-13, 2018.

53. Семенов В.В., Салахутдинова К.И., Лебедев И.С., Сухопаров М.Е. Выявление аномальных отклонений при функционировании устройств киберфизических систем // Прикладная информатика -2019. - Т. 14. - № 6(84). - С. 114-122.

54. Sabaliauskaite G., Mathur A.P. Aligning cyber-physical system safety and security // Proc. 1st Asia - Pacific. Conf. Complex Systems Design & Management, Singapore, 2015, pp. 41–53.

55. Nourian A., Madnick S. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet // IEEE Trans. Dependable Secur. Comput., 2018, 15, (1), pp. 2–13.

56. Grunske L., Colvin R., Winter K. Probabilistic model-checking support for FMEA // Proc. 4th Int. Conf. Quantitative Evaluation of Systems (QEST 2007), Edinburgh, 2007, pp. 119–128.

57. Ebeling C.E. An introduction to reliability and maintainability engineering // Waveland Press, Long Grove, Illinois, 1997, 2nd edn. 2009.

58. Dunjó J., Fthenakis V., Vílchez J.A. Hazard and operability (HAZOP) analysis. a literature review // J. Hazard. Mater., 2010, 173, (1–3), pp. 19–32.

59. Kennedy R., Kirwan B. Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems // Saf. Sci., 1998, 30, (3), pp. 249–274.

60. Banerjee A., Venkatasubramanian K.K., Mukherjee T. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems // Proc. IEEE, 2012, 100, (1), pp. 283–299.

61. Lee D.A., Lee J.S., Cheon S.W. Application of system-theoretic process analysis to engineered safety features-component control system // Proc. 37th Enlarged Halden Programme Group (EHPG) meeting, Storefjell, Norway, 2013.

62. Huang K., Zhou C., Tian Y.C. Application of Bayesian network to data-driven cyber-security risk assessment in scada networks // Proc. 27th Int. Telecommunication Networks and Applications Conf. (ITNAC), Melbourne, VIC, 2017, pp. 1–6.

63. Zhang Q., Zhou C., Tian Y.C. A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems // IEEE Trans. Ind. Inf., 2018, 14, (6), pp. 2497–2506.

64. Zhang Q., Zhou C., Xiong N. Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems // IEEE Trans. Syst., Man, Cybern.: Syst., 2016, 46, (10), pp. 1429–1444.

65. Li X., Zhou C., Tian Y.C. Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems // IEEE Trans. Ind. Inf., 2018, 14, (2), pp. 608–618.

66. Wu W., Kang R., Li Z. Risk assessment method for cyber security of cyber physical systems // Reliability Systems Engineering (ICRSE). – 2015. – V. 1. – P. 1618–1622.

67. Лившиц И.И., Молдовян А.А. Актуальные задачи обеспечения информационной безопасности в процессе жизненного цикла информационных систем // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). – 2014. – С. 623-630.

68. Созинова Е. Н. Применение экспертных систем для анализа и оценки информационной безопасности // Молодой ученый. – 2011. – № 10 (33). – Т. 1. – С. 64-66.

69. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М.: Стандартинформ, 2011. 51 с.

70. РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. М., 2009. 23 с.

71. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим

аудит и сертификацию систем менеджмента информационной безопасности. Введ. 2009-10-01. М.: Стандартинформ, 2010. 40 с.

72. Павленко Е.Ю., Штыркина А.А., Зегжда Д.П. Оценка устойчивости киберфизических систем на основе спектральной теории графов // Проблемы информационной безопасности. Компьютерные системы. -2019. - № 1. - С. 60-68.

73. Cardenas A., Amin S., Sinopoli B. et al. Challenges for securing cyber physical systems // Workshop on future directions in cyber-physical systems security, 2009.

74. Семенов В.В., Сухопаров М.Е. Методика выявления рисков нарушений информационной безопасности киберфизических систем // Методы и технические средства обеспечения безопасности информации -2020. - № 29. - С. 31-32.

75. Semenov V.V., Lebedev I.S., Sukhoparov M.E., Salakhutdinova K.I. Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State // Lecture Notes in Computer Science, 2019, Vol. 11660, pp. 104-112.

76. Rockwell Automation MicroLogix 1100 PLC Overflow Vulnerability [сайт]. URL: https://ics-cert.us-cert.gov/advisories/ICSA-16-026-02 (дата обращения 20.10.2020).

77. Wang X., Zhou Q., Harer J., Brown G., Qiu S., Dou Z., Wang J., Hinton A., Gonzalez C. A., Chin P. Deep learning-based classification and anomaly detection of side-channel signals // Proc. SPIE 10630, 2018.

78. Heller K. A. , Svore K. M., Keromytis A. D., Stolfo S. J. “One class support vector machines for detecting anomalous windows registry accesses,” in Proc. Workshop Data Mining for Computer Security, vol. 9, 2003.

79. Qiao Y., Xin X., Bin Y., Ge S. “Anomaly intrusion detection method based on HMM” Electron. Lett., vol. 38, no. 13, pp. 663–664, 2002.

80. Ryan J. Lin M.-J., Miikkulainen R. Intrusion detection with neural networks // Advances Neural Inform. Process. Syst., 1998, pp. 943–949.

81. Сухопаров М.Е., Семенов В.В., Лебедев И.С. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации -2018. № 27. - С. 59-60.

82. Семенов В.В., Лебедев И.С. Обработка сигнальной информации в задачах мониторинга информационной безопасности автономных объектов беспилотных систем // Научно-технический вестник информационных технологий, механики и оптики -2019. - Т. 19. - № 3(121). С. 492-498.

83. Meleshko A.V., Desnitsky V.A., Kotenko I.V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems // IOP Conference Series: Materials Science and Engineering, 2020, Vol. 709, pp. 033034.

84. 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. - 2019. - №. 2. - С. 156–163.

85. Зегжда Д.П. Программа для оценки безопасности киберфизической системы на основе вычисления показателя Херста / Д.П. Зегжда, Е.Ю. Павленко, Д.С. Лаврова, А.В. Ярмак. – Свидетельство о государственной регистрации программы для ЭВМ № 2019610598 от 14.01.2019.

86. Isozaki Y. et al. Detection of cyber attacks against voltage control in distribution power grids with PVs // IEEE Transactions on Smart Grid. – 2016. – Т. 7. – №. 4. – С. 1824-1835.

87. Narang P., Sikdar B. Anomaly detection in diurnal CPS monitoring data using a local density approach // Network Protocols (ICNP), 2016 IEEE 24th International Conference on. – IEEE, 2016. – С. 1-5.

88. Harada Y. et al. Log-based anomaly detection of CPS using a statistical method // arXiv preprint arXiv:1701.03249. – 2017.

89. Agrawal H., Chen R., Hollingsworth J. K., Hung C., Izmailov R., Koshy J., Liberti J., Mesterharm C., Morman J., Panagos T., Pucci M., Sebuktekin I., Alexander S., Tsang S. Casper: an efficient approach to detect anomalous code execution from unintended electronic device emissions // Proc. SPIE 10630, 20 (2018).

90. Nazari A., Sehatbakhsh N., Alam M., Zajic A., Prvulovic M. Eddie: Em-based detection of deviations in program execution // Proc. 44th Annu. Int. Symp. Computer Architecture, 2017, pp. 333–346.

91. Котенко И.В., Крибель А.М., Лаута О.С., Саенко И.Б. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети // Электросвязь. – 2020. – № 12. – С. 54-59.

92. Лаврова Д.С. Подход к разработке SIEM-системы для Интернета Вещей / Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. - СПб.: Изд-во Политехн. ун-та. - 2016. - №2. - С. 50-60.

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

94. Etigowni S., Tian D. J., Hernandez G., Zonouz S., Butler K. “CPAC: Securing critical infrastructure with cyber-physical access control” in Proc. 32nd Annu. Conf. Computer Security Applications, 2016, pp. 139–152.

95. Mulder J., Schwartz M., Berg M., Van Houten J. R., Mario J., Urrea M. A. K., Clements A. A., Jacob J. “Weaselboard: Zero-day exploit detection for

programmable logic controllers” Sandia National Laboratories, Albuquerque, NM, Rep. SAND2013-8274, 2013.

96. Шелухин О. И., Тенякшев А. М., Осин А. В. Фрактальные процессы в телекоммуникациях. – Закрытое акционерное общество Издательство Радиотехника, 2003.

97. Doukhan P., Oppenheim G., Taqqu M. (ed.). Theory and applications of long-range dependence. – Springer Science & Business Media, 2002.

98. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. – 2021. – № 1. – С. 36-44.

99. Зегжда Д.П., Зегжда П.Д., Калинин М.О. Универсальный метод обнаружения кибератак на глобальные информационные системы поддержки цифровой экономики // Методы и технические средства обеспечения безопасности информации -2019. - № 28. - С. 48-49.

100. Молдовян А.А., Молдовян Н.А. Способы и алгоритмы псевдовероятностного шифрования с разделяемым ключом // Труды СПИИРАН. – 2018. – № 6 (61). – С. 5.

101. Sehatbakhsh N., Nazari A., Zajic A., Prvulovic M. Spectral profiling: Observer-effect-free profiling by monitoring em emanations // 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), 2016, pp. 1–11.

102. Graham J. T., Riley R., Baldwin R., Fisher A. Block-level algorithm classification based on rf side-channel // Proc.SPIE 10630, 7, 2018.

103. Dey M., Nazari A., Zajic A., Prvulovic M. Emprof: Memory profiling via em-emanation in iot and hand-held devices // 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), 2018, pp. 881–893.

104. Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем / Д. П. Зегжда, Е. Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы. -2017. -№ 3. -С. 9-23.

105. Asfaw B. Host-based anomaly detection for pervasive medical systems // Risks and Security of Internet and Systems (CRiSIS), 5th International Conference – IEEE, 2010. – pp. 1-8.

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

107. Jones A., Kong Z., Belta C. Anomaly detection in cyber-physical systems: A formal methods approach // Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on. – IEEE, 2014. – С. 848-853.

108. Kosek A. M. Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model // 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG). – IEEE, 2016. – С. 1-6.

109. Васильев Ю.С., Зегжда П.Д., Зегжда Д.П. Обеспечение безопасности автоматизированных систем управления технологическими процессами на объектах гидроэнергетики // Известия Российской академии наук. Энергетика. –2016. – № 3. – С. 49-61.

110. Осипов В.Ю., Жукова Н.А., Климов Н.В. Программа автоматического многоуровневого синтеза моделей объектов мониторинга – Свидетельство о государственной регистрации программы для ЭВМ № 2019663233 от 10.10.2019..

111. KasperskyOS | На страже киберфизического мира [сайт]. URL: https://os.kaspersky.ru/ (дата обращения 03.05.2020).

112. Кибербезопасность электроэнергетической инфраструктуры [сайт]. URL: https://ics.kaspersky.ru/media/KICS-for-Energy-WhitePaper-RU.pdf (дата обращения 03.05.2020).

113. Документация по Microsoft Endpoint Configuration Manager | Microsoft Docs [сайт]. URL: https://docs.microsoft.com/ru-ru/mem/configmgr/ (дата обращения 03.05.2020).

114. Symantec Enterprise Security Manager™. Security Update 17 User's Guide [сайт]. URL: https://www.symantec.com/avcenter/security/ESM/u_17.pdf (дата обращения 03.05.2020).

115. Sukhoparov M. E., Semenov V. V., Salakhutdinova K. I., Lebedev I. S. Identification of Anomalies in the Operation of Telecommunication Devices Based on Local Signal Spectra // Automatic Control and Computer Sciences, 2020. Vol. 54(8), pp. 1001–1006.

116. Kuhn M. G., Anderson R. J. Soft tempest: hidden data transmission using electromagnetic emanations // Information Hiding 1998, LNCS 1525, P. 124–142.

117. Hayashi Y.I. и др. Introduction to the Special Section on Electromagnetic Information Security // IEEE Transactions on Electromagnetic Compatibility. 2013. С. 539–546.

118. Quisquater J. J., Samyde D. Electromagnetic analysis (EMA): measures and countermeasures for smart cards // Proc. E-smart 2001, LNCS 2140, P. 200–210.

119. Sukhoparov M.E., Semenov V.V., Salakhutdinova K.I., Boitsova E.P., Lebedev I.S. The State Identification of Industry 4.0 Mechatronic Elements Based on Behavioral Patterns. Lecture Notes in Computer Science. Vol. 12525. 2020. pp. 126-134.

120. Сухопаров М.Е., Семенов В.В., Лебедев И.С. Модель поведения для классификации состояния информационной безопасности автономного объекта // Проблемы информационной безопасности. Компьютерные системы -2019. - № 4. - С. 26-34.

121. Семенов В.В. Мониторинг информационной безопасности беспилотных транспортных средств с использованием цифрового акселерометра // Информационные технологии -2020. - Т. 26. - № 7. - С. 424-430.

122. Семенов В.В., Арустамов С.А. Обобщённая модель функционирования киберфизических систем, учитывающая риски нарушений информационной безопасности // Научно-технический вестник Поволжья -2020. - № 9. - С. 67-70.

123. Антипов С.Г., Фомина М.В. Проблема обнаружения аномалий в наборах временных рядов // Программные продукты и системы – 2012. – № 2. – С. 78-82.

124. Шелухин О. И., Осин А. В. Мультифрактальные свойства трафика реального времени // Электротехнические и информационные комплексы и системы. – 2006. – Т. 2. – №. 3.

125. Временной ряд — Википедия [сайт]. URL: https://ru.wikipedia.org/wiki/Временной_ряд (дата обращения 23.08.2020).

126. Медведникова М. М. Использование метода главных компонент при построении интегральных индикаторов // Машинное обучение и анализ данных. – 2012. – Т. 1. – №. 3. – С. 292-304.

127. Кирсанов Д.О. Потенциометрические мультисенсорные системы на основе фосфор- и азотсодержащих экстрагентов и их аналитические возможности: дис. … д-ра хим. наук. С-Пб гос. университет, Санкт-Петербург, 2014.

128. Bishop C. M. Pattern Recognition and Machine Learning // Information Science and Statistics, Springer, NY, USA. 2006.

129. Zissis D., Lekkas D. Addressing cloud computing security issues // Future Generation computer systems. – 2012. – Т. 28. – №. 3. – С. 583-592.

130. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова; под редакцией О. И. Шелухина. — Москва: Горячая линия-Телеком, 2018. — 220 с.

131. Kruegel C., Toth T. Using decision trees to improve signature-based intrusion detection // In Proceedings of the 6th International Workshop on the Recent Advances in Intrusion Detection. — Springer, 2003. — pp. 173–191.

132. E. Cagli, C. Dumas, E. Prouff Convolutional neural networks with data augmentation against jitter-based countermeasures // Proc. Int. Conf. Cryptographic Hardware and Embedded Systems, 2017, pp. 45–68.

133. Semenov V.V., Sukhoparov M.E., Lebedev I.S. Identification of Abnormal Functioning of Devices of Cyber-Physical Systems. Lecture Notes in Computer Science. Vol. 12525. 2020. pp. 3-10.

134. Secure Water Treatment – iTrust [сайт]. URL: https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/ (дата обращения 06.10.2020).

135. Goh J., Adepu S., Junejo K.N., Mathur A. A dataset to support research in the design of secure water treatment systems // International Conference on Critical Information Infrastructures Security, Springer, 2016, pp. 88-99.

136. Семенов В.В. Программа для определения состояния информационной безопасности отдельных компонентов вычислительных систем / В.В.

Семенов. – Свидетельство о государственной регистрации программы для ЭВМ № 2019618203 от 26.06.2019.

137. Kravchik M., Shabtai A. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks // Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy; Association for Computing Machinery: New York, USA – 2018.

138. Shalyga D., Filonov P., Lavrentyev A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization // arXiv 2018, arXiv:1807.07282.

139. Inoue J., Yamagata Y., Chen Y., Poskitt C.M., Sun J. Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning // Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW). – 2017, pp. 1058–1065.

140. Kravchik M., Shabtai A. Efficient cyber attacks detection in industrial control systems using lightweight neural networks // arXiv 2019, arXiv: 1907.01216.

141. Elnour M., Meskin N., Khan K., Jain R. A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems // IEEE Access. – 2020. V. 8, pp. 36639–36651.

142. Li D., Chen D., Jin B., Shi L., Goh J., Ng S.K. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks // Artificial Neural Networks and Machine Learning — ICANN2019: Text and Time Series. — 2019, pp. 703–716.

143. Gomez A., Maimo L., Celdran A, Clemente F. MADICS: A Methodology for Anomaly Detection in Industrial Control Systems // Symmetry – 2020. – V. 12. – № 10.

144. Гайфулина Д. А., Котенко И. В. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий Интернета вещей // Информационно-управляющие системы. – 2021. №1. – С. 28-37.

145. Бурлов В.Г., Маньков В.Д., Полюхович М.А. Основы технологии управления процессами обеспечения безопасности эксплуатации электроустановки // Информационные технологии и системы: управление, экономика, транспорт, право -2019. - № 1(33). - С. 173-181.

146. Burlov V., Mankov V., Polyukhovich M. Safety management of the electric power supply process of the construction site, taking into account the qualification of the manager // IOP Conference Series: Materials Science and Engineering – 2020. – V. 890 (1).

147. Костарева К.Ю., Бурлов В.Г., Джалалванд А. Разработка модели управления процессами обеспечения безопасности веб-сайта // Информационные технологии и системы: управление, экономика, транспорт, право -2019. - № 2(34). - С. 199-204.

ПРИЛОЖЕНИЯ

Приложение 1. Модель угроз информационной безопасности для различных типов КФС

Таблица 1 – Модель угроз ИБ АСУ

Мотив	Источник	Цель	Вектор атаки	Последствие
Преступные угрозы	Злоумышленник, знакомый с системой	Удалённое управление АСУ	Беспроводные сети	Нарушение работы АСУ
	Финансово-мотивированные потребители	Уменьшение счета за коммунальные услуги	Вмешательство в физическое оборудование или ввод ложных данных	Финансовые потери поставщика услуг
Политически мотивированный шпионаж	Спецслужбы	Разведывательные операции, нацеленные на критическую инфраструктуру страны	Распространение вредоносного ПО	Нарушения конфиденциальности критических данных
Политически мотивированные угрозы	Враждебное государство или нация	Кибервойна	Дистанционная атака критически важной инфраструктуры	Отказ компонентов КФС, или загрязнение окружающей среды
Физические угрозы	Злоумышленник	Подделка датчика, измеряющего температуру конкретной среды	Умышленное охлаждение или нагревание датчика	Отправка ложных измерений в центр управления

Таблица 2 – Модель угроз ИБ «умных» сетей электроснабжения

Мотив	Источник	Цель	Вектор атаки	Последствие
Преступные угрозы	Потребитель	Обман биллинговой системы коммунального предприятия	Изменение показаний интеллектуальных счётчиков	Финансовые потери поставщика услуг
	Преступник	Кража имущества в отсутствие владельца	Информация о присутствии жильцов дома, добытая от интеллектуального счётчика	Имущественные и (или) финансовые потери владельца
Финансово-мотивированные угрозы	Коммунальные компании	Личная информация клиентов для определения привычек и типов бытовой техники	Анализ потребления электроэнергии	Нарушение конфиденциальности, продажа данных потребителей рекламным агентствам
Политически мотивированные угрозы	Враждебное государство или нация	Кибервойна против энергосистемы	Удаленный доступ к инфраструктуре интеллектуальных сетей	Крупномасштабные отключения, помехи или финансовые потери

Таблица 3 – Модель угроз ИБ медицинских устройств

Мотив	Источник	Цель	Вектор атаки	Последствие
Преступные угрозы	Злоумышленник	Нанести вред пациенту или повлиять на его состояние здоровья	Беспроводные сети для ввода или повторной передачи ранее захваченных	Изменение состояния устройства и ожидаемых операций, что

Мотив	Источник	Цель	Вектор атаки	Последствие
			законных команд	приведет к ухудшению здоровья
			Блокировка сигналов, которыми обмениваются медицинские устройства	Недоступность устройства и невозможность выполнять функции
Шпионские угрозы	Злоумышленник	Выявить наличие заболевания, тип медицинского устройства или другую информацию	Перехват сообщений медицинского устройства пациента с помощью беспроводных средств	Нарушение неприкосновенности частной жизни и конфиденциальности
	Злоумышленник	Получить несанкционированный доступ к медицинским данным	Проникновение в сети между вовлеченными законными сторонами	
Политически мотивированные угрозы	Враждебное государство или нация	Политические деятели	Атака на медицинские устройства, по беспроводной связи	Потенциальное критическое состояние здоровья или возможная смерть

Таблица 4 – Модель угроз ИБ «умных» транспортных средств (Smart Cars)

Мотив	**Источник**	**Цель**	**Вектор атаки**	**Последствие**
Преступные угрозы	Злоумышленник	Электронный блок управления	Уязвимости беспроводных интерфейсов	Столкновение или потеря контроля ТС
Угрозы конфиденциальности	Злоумышленник	Перехват личных разговоров в автомобиле	Уязвимости блока управления телефоном	Вторжение в личную жизнь
Отслеживание угроз	Злоумышленник или сотрудник правоохрани-тельных органов	Отслеживание ТС	Навигационная система GPS	Нарушение конфиденциаль-ности
Профилирование угроз	Производители автомобилей	Выявление некоторых привычек вождения и нарушения правил дорожного движения	Сохранение информации бортовых журналов ТС	Нарушение конфиденциаль-ности (без согласия водителя)
Политически мотивированные угрозы	Враждебное государство или нация	Транспортные системы и их пассажиры	ТС, которые уязвимы для полного дистанционного управления	Крупно-масштабные столкновения и критические травмы

Приложение 2. Копии зарегистрированных свидетельств на результаты интеллектуальной деятельности

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019618203

Программа для определения состояния информационной безопасности отдельных компонентов вычислительных систем

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (RU)***

Автор: ***Семенов Виктор Викторович (RU)***

Заявка № **2019617217**
Дата поступления **14 июня 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***26 июня 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Приложение 3. Копии актов внедрения

УТВЕРЖДАЮ

Первый заместитель директора

СПбФ АО «НПК «Тристан»

_____ И.Н. Соловьев

«___» июня 2021 г.

АКТ
об использовании результатов диссертационной работы
Семенова Виктора Викторовича
«Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов»

Комиссия в составе: председателя – заместителя директора по ПО, к.т.н. Шахпароняна Артёма Павловича, членов комиссии: ведущего научного сотрудника, к.т.н. Гринько Сергея Васильевича и старшего научного сотрудника, к.т.н. Сухопарова Михаила Евгеньевича составила настоящий акт в том, что нижеперечисленные научные результаты диссертационной работы Семенова Виктора Викторовича:

- метод идентификации состояния информационной безопасности на основе бэггинга деревьев решений с использованием весовых коэффициентов Фишберна в качестве постобработки результатов классификации;
- методика идентификации состояния информационной безопасности элементов киберфизических систем;

используются в работе отдела проектирования и разработки программного обеспечения Санкт-Петербургского филиала АО «НПК «ТРИСТАН» для мониторинга состояния информационных производственных систем с целью минимизации количества существующих уязвимостей системы и предотвращения возможных атак на отдельные устройства. Практическое использование результатов диссертационной работы Семенова В.В. позволяет достичь заданной точности идентификации, сократив при этом временные затраты и вычислительные мощности, затрачиваемые на обработку многомерных данных, поступающих от систем мониторинга информационной безопасности киберфизических систем.

Председатель комиссии:
заместитель директора по ПО,
к.т.н. _____ (подпись) А.П. Шахпаронян

Члены комиссии:

ведущий научный сотрудник,
к.т.н. _____ (подпись) С.В. Гринько

старший научный сотрудник,
к.т.н. _____ (подпись) М.Е. Сухопаров

МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ «САНКТ-ПЕТЕРБУРГСКИЙ ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК» (СПб ФИЦ РАН)

14 линия В.О., д. 39, Санкт-Петербург, 199178
Телефон: (812) 328-34-11, факс: (812) 328-44-50, E-mail: info@spcras.ru, https://spcras.ru/
ОКПО 04683303, ОГРН 1027800514411, ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ
заместитель директора
по научной работе СПб ФИЦ РАН

_____ С.В. Кулешов
«28» июня 2021

А К Т
об использовании результатов диссертационной работы
Семенова Виктора Викторовича
«Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов»
в научно-исследовательской работе СПб ФИЦ РАН

Комиссия в составе: председателя – д.т.н., профессора Искандерова Юрия Марсовича, членов комиссии: д.т.н., профессора Лебедева Ильи Сергеевича и Свистуновой Александры Сергеевны, составила настоящий акт в том, что научные результаты, полученные Семеновым Виктором Викторовичем в рамках выполнения диссертационной работы «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов», а именно:

- модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем;
- метод оценивания состояния информационной безопасности элементов киберфизических, основанный на комбинированном подходе применения параллельно работающего ансамбля классификаторов и весовых коэффициентов Фишберна при анализе совокупности наиболее информативных признаков;

были внедрены в следующих научных проектах, выполненных или выполняемых в СПб ФИЦ РАН:

- проект по программе Президиума РАН № 0073-2018-0007 «Разработка масштабируемых устойчивых алгоритмов построения семантических моделей больших данных и их использование для решения прикладных задач кластеризации и машинного обучения», 2018, 2019 гг;

- проект по программе Президиума РАН № 0073-2018-0008 «Теория и распределенные алгоритмы самоорганизации группового поведения агентов в автономной миссии», 2018-2019 гг;
- НИОКТР № 0073-2019-0001 «Теоретические основы и алгоритмические модели когнитивного управления, взаимодействия и анализа состояния групп гетерогенных робототехнических комплексов», 2019, 2020 гг.

Реализация положений, выносимых на защиту в диссертационной работе, позволила повысить оперативность идентификации состояния информационной безопасности элементов киберфизических систем без существенной потери точности за счёт уменьшения размерности обрабатываемых данных и идентификации состояния ИБ на основе решающего правила, учитывающего значения временных рядов, полученные за предшествующие моменты времени. Комиссия отмечает теоретическую и практическую значимость полученных в диссертационной работе научных результатов.

Председатель комиссии:
заведующий лабораторией
интеллектуальных систем, д.т.н., проф. _____ (подпись) Ю.М. Искандеров

Члены комиссии:
главный научный сотрудник лаборатории
интеллектуальных систем, д.т.н., проф. _____ (подпись) И.С. Лебедев

младший научный сотрудник лаборатории
интеллектуальных систем _____ (подпись) А.С. Свистунова

Приложение 4. Список публикаций автора по теме диссертации

Публикации в научных изданиях, входящих в перечень российских рецензируемых журналов (рекомендованные ВАК при Минобрнауки РФ)

1. **Семенов В.В.** Мониторинг информационной безопасности беспилотных транспортных средств с использованием цифрового акселерометра // Информационные технологии -2020. - Т. 26. - № 7. - С. 424-430.

2. **Семенов В.В.**, Арустамов С.А. Выявление рисков нарушений информационной безопасности киберфизических систем на основе анализа цифровых сигналов // Научно-технический вестник информационных технологий, механики и оптики -2020. - Т. 20. - № 5(129). - С. 770-772.

3. Сухопаров М.Е., **Семенов В.В.**, Лебедев И.С., Гаранин А.В. Подход к анализу состояния узлов «Индустрии 4.0» на основе поведенческих паттернов // Наукоемкие технологии в космических исследованиях Земли -2020. - Т. 12. - № 5. С. 83-91.

4. Сухопаров М.Е., Лебедев И.С., **Семенов В.В.** Использование амплитудно-частотных характеристик побочных излучений для анализа состояния информационной безопасности // Проблемы информационной безопасности. Компьютерные системы -2020. - № 4. С. 53-57.

5. Сухопаров М.Е., **Семенов В.В.**, Лебедев И.С., Бойцова Э.П. Идентификация состояния мехатронных элементов "Индустрии 4.0" на основе поведенческих паттернов // Информация и космос -2020. - № 4. - С. 83-89.

6. Сухопаров М.Е., **Семенов В.В.**, Салахутдинова К.И., Лебедев И.С. Выявление аномалий функционирования телекоммуникационных устройств на основе локальных сигнальных спектров // Проблемы информационной безопасности. Компьютерные системы -2020. - № 2. - С. 29-34.

7. Сухопаров М.Е., **Семенов В.В.**, Салахутдинова К.И., Лебедев И.С. Выявление аномального функционирования устройств Индустрии 4.0 на основе поведенческих паттернов // Проблемы информационной безопасности. Компьютерные системы - 2020. - № 1. - С. 96-102.

8. Сухопаров М.Е., **Семенов В.В.**, Лебедев И.С. Модель поведения для классификации состояния информационной безопасности автономного объекта // Проблемы информационной безопасности. Компьютерные системы -2019. - № 4. - С. 26-34.

9. **Семенов В.В.**, Салахутдинова К.И., Лебедев И.С., Сухопаров М.Е. Выявление аномальных отклонений при функционировании устройств киберфизических систем // Прикладная информатика -2019. - Т. 14. - № 6(84). - С. 114-122.

10. **Семенов В.В.**, Лебедев И.С., Сухопаров М.Е. Идентификация состояния отдельных элементов киберфизических систем на основе внешних поведенческих характеристик // Прикладная информатика -2018. - Т. 13. - № 5(77). - С. 72-83.

11. **Семенов В.В.**, Лебедев И.С., Сухопаров М.Е. Подход к классификации состояния информационной безопасности элементов киберфизических систем с использованием побочного электромагнитного излучения // Научно-технический вестник информационных технологий, механики и оптики -2018. - Т. 18. - № 1(113). - С. 98-105.

Публикации, которые приравниваются к рецензируемым научным изданиям

12. **Семенов В.В.** Программа для определения состояния информационной безопасности отдельных компонентов вычислительных систем / В.В. Семенов. – Свидетельство о государственной регистрации программы для ЭВМ № 2019618203 от 26.06.2019.

Публикации в научных изданиях, входящих в международные реферативные базы данных и системы цитирования (Web of Science и Scopus)

13. **Semenov V.V.**, Sukhoparov M.E., Lebedev I.S. Identification of Abnormal Functioning of Devices of Cyber-Physical Systems // Lecture Notes in Computer Science, 2020, Vol. 12525, pp. 3-10. (**WoS/Scopus** – **Q3**).

14. **Semenov V.V.**, Sukhoparov M.E., Lebedev I.S. Approach to the State Analysis of Industry 4.0 Nodes Based on Behavioral Patterns // Lecture Notes in Computer Science / Interactive Collaborative Robotics, 2020, Vol. 12336, pp. 273-282. (**WoS/Scopus** – **Q3**).

15. Sukhoparov M.E., **Semenov V.V.**, Salakhutdinova K.I., Lebedev I.S. Identification of Anomalies in the Operation of Telecommunication Devices Based on Local Signal Spectra // Automatic Control and Computer Sciences, 2020, Vol. 54(8), pp. 1001–1006. (**WoS/Scopus** – **Q3**).

16. Sukhoparov M.E., Lebedev I.S., **Semenov V.V.** Information Security State Analysis of Elements of Industry 4.0 Devices in Information Systems // Lecture Notes in Computer Science, 2020, Vol. 12525, pp. 119-125. (**WoS/Scopus** – **Q3**).

17. Sukhoparov M.E., **Semenov V.V.**, Salakhutdinova K.I., Boitsova E.P., Lebedev I.S. The State Identification of Industry 4.0 Mechatronic Elements Based on Behavioral Patterns // Lecture Notes in Computer Science, 2020, Vol. 12525, pp. 126-134. (**WoS/Scopus** – **Q3**).

18. Salakhutdinova K.I., Sukhoparov M.E., Lebedev I.S., **Semenov V.V.** Comparative Analysis of Approaches to Software Identification. Software Engineering Perspectives in Intelligent Systems // Advances in Intelligent Systems and Computing, 2020, Vol. 1295, pp. 72-78. (**WoS/Scopus** – **Q3**).

19. **Semenov V.V.**, Lebedev I.S., Sukhoparov M.E., Salakhutdinova K.I. Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State // Lecture Notes in Computer Science, 2019, Vol. 11660, pp. 104-112. (**WoS/Scopus** – **Q2**).

20. **Semenov V.V.**, Sukhoparov M.E., Lebedev I.S. Approach to Side Channel-Based Cybersecurity Monitoring for Autonomous Unmanned Objects // Lecture Notes in Computer Science / Interactive Collaborative Robotics, 2019, Vol. 11659, pp. 278-286. (**WoS/Scopus** – **Q2**).

21. **Semenov V.**, Sukhoparov M., Lebedev I. An Approach to Classification of the Information Security State of Elements of Cyber-Physical Systems Using Side

Electromagnetic Radiation // Lecture Notes in Computer Science, 2018, Vol. 11118, pp. 289-298. (**WoS/Scopus** – **Q2**).

Публикации в иных изданиях

22. **Семенов В.В.** Оценивание состояния информационной безопасности на основе анализа временных рядов // Научно-технический вестник Поволжья -2021. - № 10. - С. 127-129.

23. **Семенов В.В.**, Лебедев И.С. Обработка сигнальной информации в задачах мониторинга информационной безопасности автономных объектов беспилотных систем // Научно-технический вестник информационных технологий, механики и оптики -2019. - Т. 19. - № 3(121). - С. 492-498.

24. **Семенов В.В.**, Сухопаров М.Е. Методика выявления рисков нарушений информационной безопасности киберфизических систем // Методы и технические средства обеспечения безопасности информации -2020. - № 29. - С. 31-32.

25. **Семенов В.В.**, Арустамов С.А. Обобщённая модель функционирования киберфизических систем, учитывающая риски нарушений информационной безопасности // Научно-технический вестник Поволжья -2020. - № 9. - С. 67-70.

26. **Семенов В.В.** Метод мониторинга состояния информационной безопасности беспилотных транспортных средств // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция (Санкт-Петербург, 23-25 октября 2019 г.): материалы конференции -2019. - С. 323-324.

27. **Семенов В.В.**, Лебедев И.С., Сухопаров М.Е. Идентификация состояния информационной безопасности беспилотных транспортных средств с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации -2019. - № 28. - С. 46-47.

28. **Семенов В.В.**, Лебедев И.С. Анализ состояния информационной безопасности объектов транспортных систем // Региональная информатика

(РИ-2018): Материалы конференции (Санкт-Петербург, 24-26 октября 2018 г.) - 2018. - С. 324-325.

29. Сухопаров М.Е., **Семенов В.В.**, Лебедев И.С. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации -2018. - № 27. - С. 59-60.