*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

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург – 2022

Работа выполнена в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) в лаборатории интеллектуальных систем.

**Научный руководитель:** **ЛЕБЕДЕВ Илья Сергеевич**,
доктор технических наук, профессор, главный научный сотрудник лаборатории интеллектуальных систем Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

**Официальные оппоненты:** **ПРИМАКИН Алексей Иванович**,
доктор технических наук, профессор, начальник кафедры специальных информационных технологий Федерального государственного казенного образовательного учреждения высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»

**ПАВЛЕНКО Евгений Юрьевич**,
кандидат технических наук, доцент Института кибербезопасности и защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

**Ведущая организация:** Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Защита состоится «12» мая 2022 г. в 14 часов 00 минут на заседании диссертационного совета 24.1.206.01, созданного на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) по адресу: 199178, Санкт-Петербург, 14-ая линия В.О., 39, каб. 401. Факс: (812)-328-44-50, тел: (812)-328-34-11.

С диссертацией можно ознакомиться в отделе аспирантуры (каб. 315) и на сайте Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) http://www.spiiras.nw.ru/dissovet/

Автореферат разослан «29» марта 2022 г.

Учёный секретарь
диссертационного совета 24.1.206.01
кандидат технических наук **Абрамов Максим Викторович**

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**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 представлялись на следующих 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.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертации, определены объект, предмет и цель исследования, сформулированы основные задачи, научная новизна и практическая значимость полученных результатов, а также положения, выносимые на защиту. Приведено краткое содержание диссертации по главам и описана апробация результатов исследования.

В **первой главе** дана общая характеристика исследуемых объектов, проведён анализ современного состояния задачи обеспечения ИБ КФС, построена модель угроз при функционировании КФС. Рассмотрены решения, подходы и методы оценивания защищённости и выявления нарушений ИБ КФС, предлагаемые ведущими отечественными и зарубежными исследователями, а также известными в сфере безопасности информационных технологий компаниями.

Тесная интеграция современных киберфизических систем с производственно-технологическими системами и объектами критической информационной инфраструктуры требует совершенствования процессов мониторинга. Для обработки большого количества данных, поступающих от систем мониторинга, необходимы значительные вычислительные мощности. В этой связи актуальным является снижение размерности признакового пространства при сохранении приемлемой точности мониторинга.

Применительно к КФС, понятие ИБ одновременно с традиционным обеспечением целостности, конфиденциальности и доступности данных, циркулирующих в системе дополняется необходимостью поддержания конечной целевой функции системы в условиях информационных угроз и атак.

Появление отказов, сбоев отдельных объектов КФС 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 средств выявления нарушений ИБ, анализирующих состояние ИБ системы по информации, полученной из временных рядов, составленных из значений параметров КФС и объективно отражающих её состояние информационной безопасности.

Отмечено, что большинство имеющихся на сегодняшний день работ сосредоточено на анализе состояния либо физической, либо информационной составляющей КФС. Исходя из анализа современных исследований и коммерческих решений, можно сделать вывод о том, что в настоящее время в мире отсутствуют сложившиеся комплексные подходы идентификации состояния ИБ КФС.

Выявление угроз нарушений ИБ, характерных для исследуемых объектов, является одним из ключевых этапов решения поставленной задачи. Основными угрозами для КФС являются несанкционированные изменения или разрушение информации, атаки на её целостность. Как правило, целью злоумышленника является получение доступа к удалённому управлению КФС или прекращение функционирования системы.

Модель оценивания состояния информационной безопасности элементов КФС реализуется на основе анализа совокупности процессов оценивания различных факторов:

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

где:

- $P_i$ – процессы оценивания ИБ на основе конфиденциальности целостности и доступности для информационной составляющей, включающие обнаружение уязвимостей по информационным и физическим компонентам;

- $P_f$ – процессы оценивания согласованности информационной и физической составляющей с учетом их взаимовлияния, свойств масштабируемости;
- $P_c$ – процессы оценивания влияния информационных атак на систему управления.

Выполнен вычислительный эксперимент для подтверждения применимости разработанного подхода. Параметры, получаемые в результате анализа сетевого трафика КФС и формируемые от множества источников, синхронизируются по времени и объединяются во временные ряды. В эксперименте использовались временные ряды, полученные из сетевого трафика между системой управления и сбора данных (SCADA) и программируемыми логическими контроллерами (ПЛК) исследовательского стенда КФС водоочистки. Потоки данных, создаваемые измерительными компонентами, такими как удаленные терминальные блоки SCADA, передают телеметрические данные от элементов КФС в систему управления событиями безопасности ИБ. В свою очередь, команды от главной контролирующей системы передаются обратно к подключенным компонентам, реализуя тем самым закрытие процесса контура управления.

Во **второй главе** сформулирована постановка задачи исследования, предложена модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем.

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 $\mu$, способный соотнести элементы множества $X$ с одним из известных классов, соотнесённых с состоянием ИБ:

$$\mu: X \rightarrow C, \qquad (2)$$

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.

Процесс выявления аномалий основан на том, что изменения в анализируемых временных рядах показывают возможные отклонения от разрешённых (безопасных) состояний ИБ системы. Ключевым деструктивным фактором является получение злоумышленником возможности влиять на физические и производственные процессы посредством информационных воздействий.

Признаковое пространство, описывающее состояние ИБ исследуемых объектов должно позволять одинаково точно идентифицировать все состояния ИБ, используемые при обучении модели. Исходное признаковое пространство $H = (f_1, f_2, \ldots, f_n)$ представляет собой набор возможных параметров КФС, которые могут включать в себя как характеристики информационных процессов, так и данные о протекающих физических процессах (например, информацию с датчиков).

Метод анализа главных компонент (МГК) широко используется для понижения размерности исходных данных. В большинстве исследований МГК

применяется в качестве предобработки, в этом случае исходное многомерное признаковое пространство преобразуется в пространство главных компонент (ГК), заменяющее исходное. В отличие от других работ, в диссертации МГК применяется как инструмент для вычисления информативности каждого признака (источника информации о процессах КФС).

Матрица данных **X** содержит сгруппированные временные ряды и представляет собой результаты измерения некоторых параметров, характеризующих информационные или физические процессы объекта КФС во времени. Каждая строка матрицы **X** – временной ряд предобработанных (центрированных и правильно нормированных) данных, число строк – $m$ (количество векторов данных), число столбцов – $n$ (исходная размерность пространства данных).

Разложение матрицы **X** при помощи МГК представимо в следующем виде:

$$\mathbf{X} = \mathbf{T}\mathbf{P}^{\mathrm{T}} + \mathbf{E}, \tag{3}$$

где **T** – матрица счетов (*scores*), **P** – матрица нагрузок, **E** – матрица остатков.

$$\mathbf{P} = \begin{pmatrix} p_{1,1} & p_{1,2} & \dots & p_{1,k} \\ p_{2,1} & p_{2,2} & \dots & p_{2,k} \\ \dots & \dots & \dots & \dots \\ p_{n,1} & p_{n,2} & \dots & p_{n,k} \end{pmatrix}. \tag{4}$$

Для вычисления информативности признаков необходимо решить задачу выбора числа ГК ($k$), для чего последовательно при каждом $k$, начиная с 1 рассчитываются значения объяснённой дисперсии ERV по формуле:

$$\mathrm{ERV} = 1 - \sum_{t=1}^{m}\sum_{j=1}^{n} e_{t,j}^2 \Big/ \sum_{t=1}^{m}\sum_{j=1}^{n} x_{t,j}^2, \tag{5}$$

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:

$$I_{f_i} = \sqrt{\sum_{j=1}^{k} \mathrm{p}_{i,j}^2} \tag{6}$$

Идентификаторы источников упорядочиваются по информативности $I_{f1} \geqslant I_{f2} \geqslant \dots \geqslant I_{fs}$ и по правилу Кайзера выбирается $s$ источников $H^* = (f_1, f_2, \dots, f_s)$, информативность которых больше средней информативности: $I_{f_i} > \frac{1}{n}\sum_{i=1}^{n} I_{f_i}$. Идентификаторы $H^*$заносятся в архив и участвуют в дальнейшем построении модели классификации. Блок-схема алгоритма представлена на рисунке 1.

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

$$c(t) = \mu(x_{t,1}, x_{t,2}, \dots, x_{t,s}),\ c \in C,\ x_{t,i} \in D_f,\ s << n, \tag{7}$$

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


Рисунок 1 – Блок-схема алгоритма формирования признакового описания состояния ИБ элементов КФС

Применимость разработанной модели и её эффективность подтверждена при помощи результатов серии экспериментов, которые рассмотрены в главе 4.

В **третьей главе** разработан 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. С целью увеличения числа верных идентификаций состояния ИБ производился одновременный учёт результатов классификации в моменты времени $t_{i-n}$, $t_{i-2}$, $t_{i-1}$, …, $t_i$. На практике, наиболее важными являются значения состояний ИБ, которые приближены к текущему, для этого введены весовые коэффициенты, учитывающие степень предпочтения одних результатов идентификации другим. Весовые коэффициенты должны быть вычислены для всего временного отрезка идентификации $N$, при этом каждый коэффициент $p_{i+1}$ должен быть меньше $p_i$ ($\forall\ p_{i-1} < p_i,\ i \in [1, N]$).

$$r_1 = N;\ r_i = r_{i-1} - 1;\ K = \sum_{i=1}^{N} r_i;\ p_i = \frac{r_i}{K}, \qquad (8)$$

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

Результаты оценивания состояния ИБ, полученные в разные моменты времени, усредняются с учётом их уровня значимости и более поздние состояния ИБ системы имеют больший вес. В работе применён и исследован алгоритм на основе деревьев решений, который относится к группе логических классификаторов. 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 $\Delta$ подаются на вход вышеуказанных классифицирующих алгоритмов. Каждый алгоритм $a_1$-$a_n$ генерирует $N$ ответов $x_t \rightarrow c$ на временном отрезке $\Delta$, которые обобщаются на первом этапе с использованием весовых коэффициентов Фишберна.

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 2.

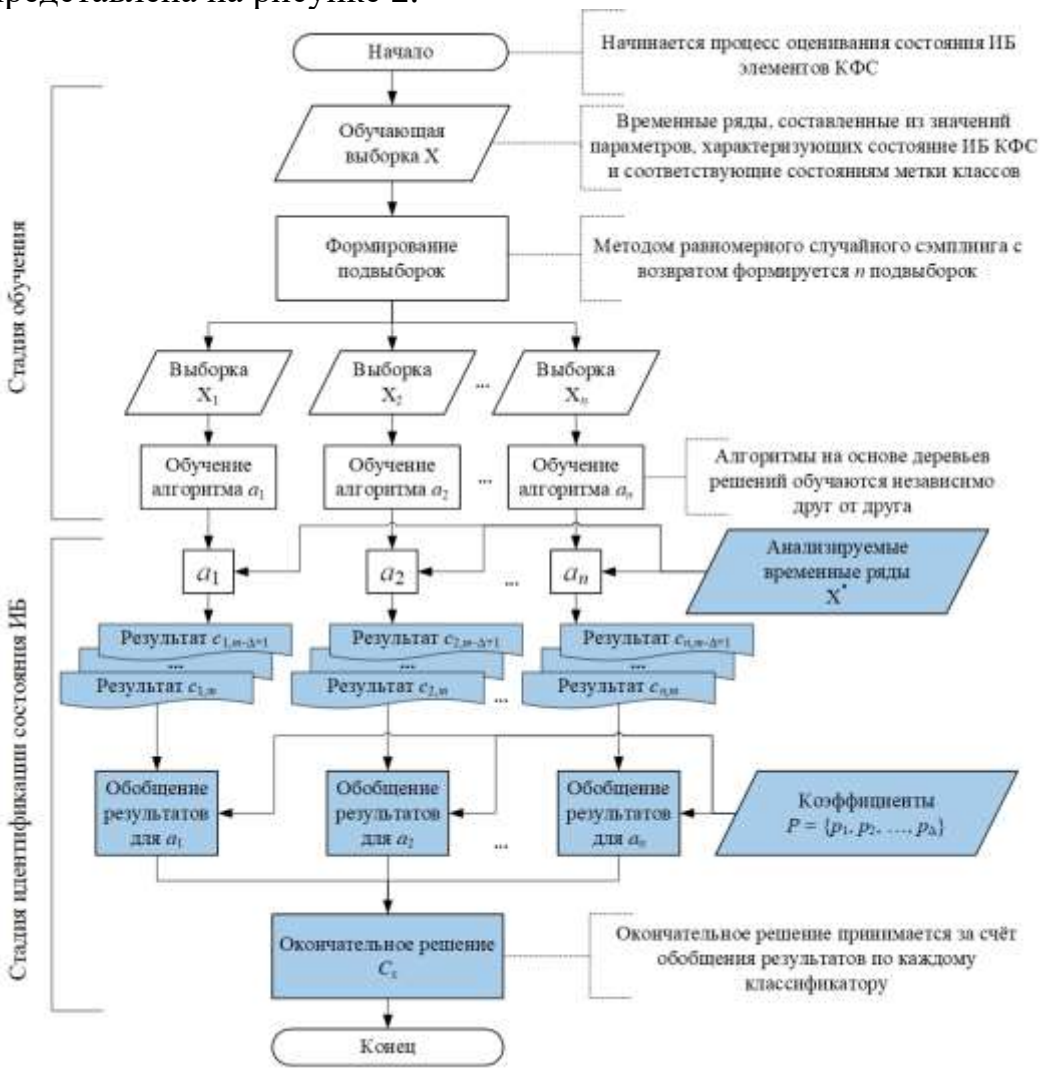



Рисунок 2 – Метод оценивания состояния ИБ элементов КФС, основанный на комбинированном подходе

Третьим результатом, выносимым на защиту, является методика, которая включает в себя 3 стадии: 1) Этап формирования архива идентификаторов источников (АИИ) по алгоритму, изображённому на рисунке 1.

2) Подготовительный этап, на котором: формируются обучающая и тестовая выборки и подвыборки из кортежа $\hat{X} = \{\{x_1(t_1), x_2(t_1), \ldots, x_s(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_s(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_s(t_m)\}\}$, при этом информативности $I_{f_1} > I_{f_2} > \ldots > I_{f_s}$; происходит обучение классификаторов и выбор временного отрезка $\Delta$ идентификации состояния ИБ. 3) Этап идентификации состояния ИБ, на котором применяется ансамбль параллельно работающих классификаторов на основе деревьев решений и производится постобработка результатов с применением весовых коэффициентов Фишберна на выбранном отрезке идентификации. Блок-схема методики представлена на рисунке 3.

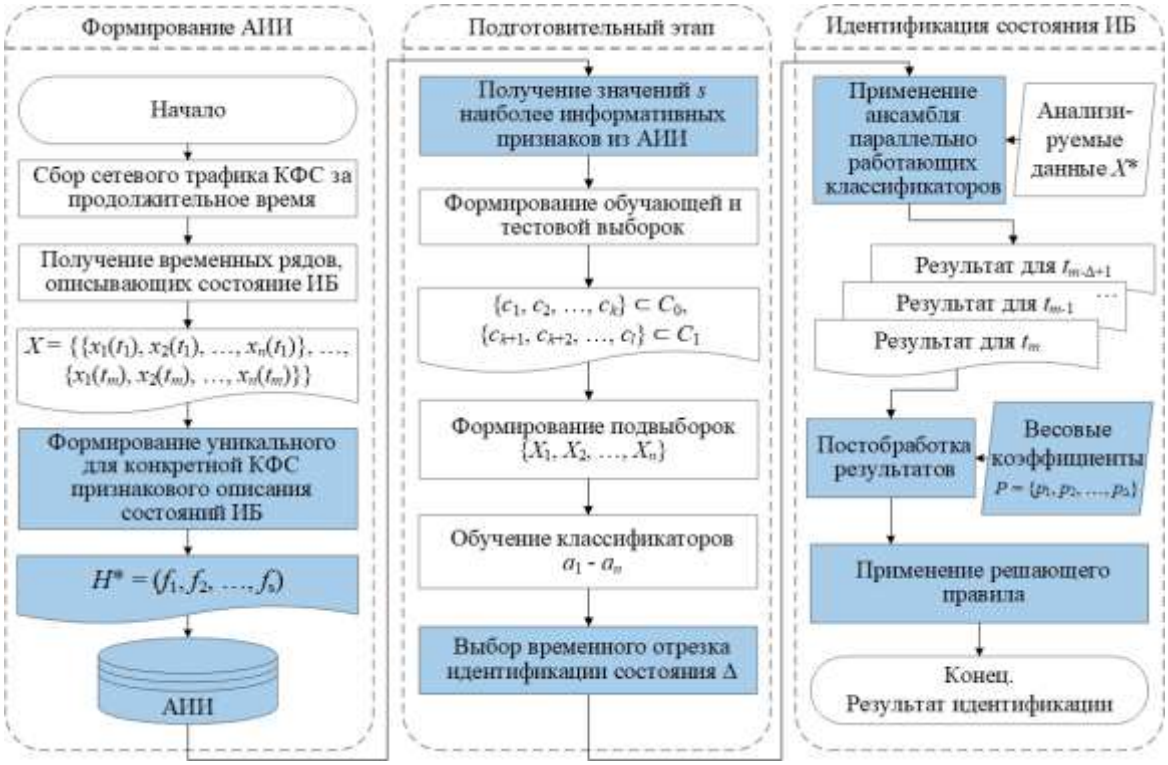
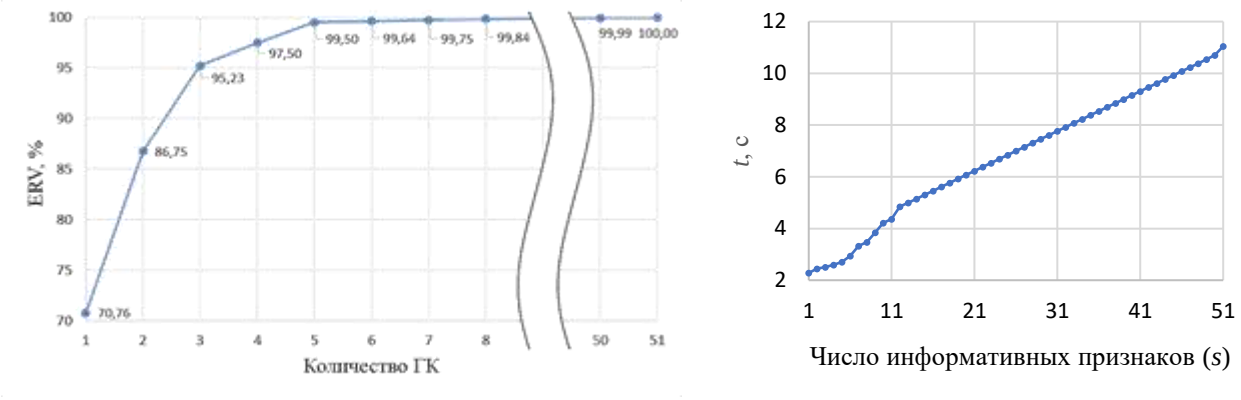



Рисунок 3 – Блок-схема методики идентификации состояния ИБ элементов КФС

В работе представлены ограничения, накладываемые на методику и условия её использования.

В **четвёртой главе** продемонстрирована экспериментальная реализация разработанных модели, метода и методики. Были проанализированы временные ряды, формируемые из сетевого трафика между SCADA и ПЛК исследовательского стенда КФС водоочистки за ~ 11 дней, при этом была реализована 41 атака разных типов. Показано, что бóльшую часть полезной информации несёт лишь малое количество ГК (рисунок 4а), что позволяет судить о наличии небольшого числа признаков, при помощи которых можно получить объективную информацию о состоянии ИБ исследуемой КФС, существенно сократив при этом временные затраты на обработку данных мониторинга состояния ИБ (рисунок 4б).




(а) (б)

Рисунок 4 – Зависимость объяснённой дисперсии от количества ГК (а) и времени обучения от числа информативных признаков (*s*) для КФС водоочистки

В таблице 1 представлены результаты эксперимента на основе анализа 944 919 временных рядов, формируемых раз в секунду.

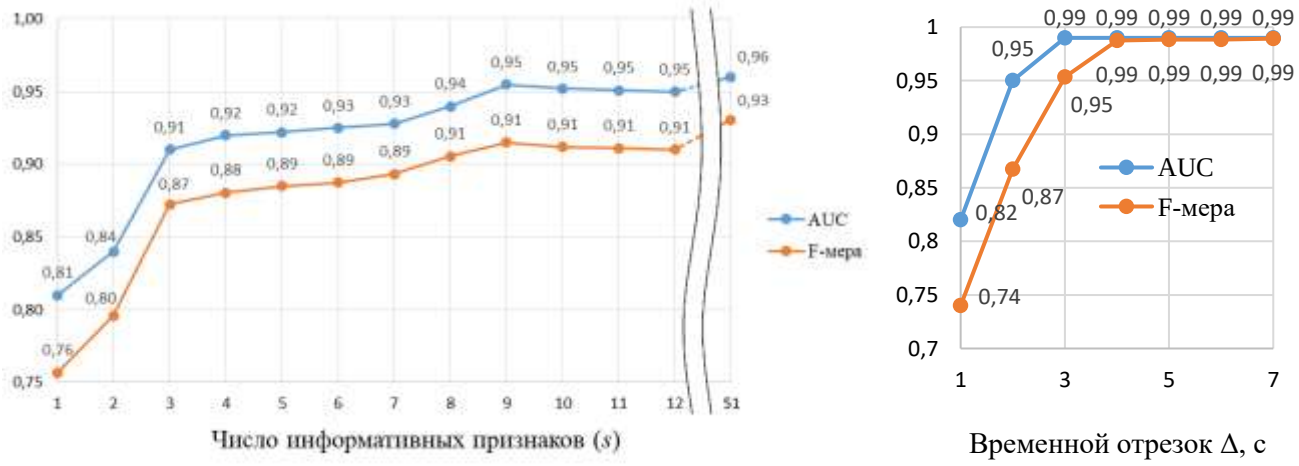
Таблица 1 – Информативность отобранных наиболее информативных признаков

| $f_i$ | LIT401 | LIT101 | LIT301 | AIT201 | PIT501 | PIT503 | AIT402 | AIT203 | AIT502 |
|---|---|---|---|---|---|---|---|---|---|
| $I_{f_i}$ | 0,99913 | 0,99913 | 0,99896 | 0,94786 | 0,67211 | 0,51464 | 0,48828 | 0,31012 | 0,22888 |

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.

В диссертации приведено пять способов оценки показателей качества идентификации состояния ИБ КФС: матрица несоответствий (*confusion matrix*), точность (*precision*), полнота (*recall*), F-мера, AUC (площадь под ROC-кривой), позволяющих производить оценивание результатов, полученных с применением алгоритмов машинного обучения, а также сравнивать результаты с другими исследованиями.

Исследованы зависимости характеристик классификации от числа информативных признаков (рисунок 5а) и от временного отрезка идентификации (рисунок 5б). Найдено оптимальное значение Δ, равное 5.




(а) (б)

Рисунок 5 – Показатели качества идентификации

Произведено сравнение результатов проведённого исследования с результатами, полученными независимыми исследователями на идентичном наборе исходных данных (таблица 2).

Таблица 2 – Сравнение результатов исследования

| Метод идентификации | Точность, % | Полнота, % | F-мера |
|---|---|---|---|
| Одномерные свёрточные нейронные сети (1D CNN) | 96,8 | 79,1 | 0,871 |
| Многослойный перцептрон (MLP) | 96,7 | 69,6 | 0,809 |
| Свёрточные нейронные сети (CNN) | 95,2 | 70,2 | 0,808 |
| Рекуррентные нейронные сети (RNN) | 93,6 | 69,2 | 0,796 |
| Глубинные нейронные сети (DNN) | 98,2 | 67,8 | 0,802 |
| Одноклассовый метод опорных векторов (OCSVM) | 92,5 | 69,9 | 0,796 |
| Автоэнкодер (AE) | 92,4 | 82,7 | 0,873 |
| Изолирующие леса (IF) | 93,5 | 83,5 | 0,882 |
| Генеративно-состязательные сети (GAN) | 70,0 | 95,4 | 0,807 |
| Нейронные сети с долгой краткосрочной памятью (LSTM NN) | 98,4 | 75,0 | 0,851 |
| **Разработанный подход** | | | |
| $s = 51$, $\Delta = 1$ | 99,20 | 88,39 | 0,935 |
| $s = 9$, $\Delta = 1$ | 98,74 | 85,20 | 0,915 |
| $s = 9$, $\Delta = 5$ (методика) | 99,85 | 99,85 | 0,998 |

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 идентификации состояния ИБ КФС. Методики с высокой полнотой классификации предпочтительней для распознавания ранее неизвестных типов аномалий.

Заключительным этапом исследования являлась проверка возможности корректно идентифицировать атаки различных типов на КФС и её отдельные элементы. Было распознано 36 информационных атак различных типов на КФС со значениями полноты идентификации 0,94 – 1,00. Для большинства классов полнота была максимальной.

В **заключении** приведены выводы и результаты, полученные автором в ходе выполнения работы, даны рекомендации по применению разработанных методов оценивания защищённости киберфизических систем от информационных угроз.

## 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.

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 РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

**Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук**

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.

*Автореферат диссертации*

СЕМЕНОВ
Виктор Викторович

# МОДЕЛЬ И МЕТОД ОЦЕНИВАНИЯ ЗАЩИЩЁННОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ОТ ИНФОРМАЦИОННЫХ УГРОЗ НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ

Текст автореферата размещен на сайтах:
Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации
https://vak.minobrnauki.gov.ru/
Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»
http://www.spiiras.nw.ru/dissovet/

Подписано в печать "___" _____ 2022 г.
Формат 60x84 1/16. Бумага офсетная. Печать офсетная.
Усл.печ.л. 1,0. Тираж 100 экз.
Заказ № ___