ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.206.01,
СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ «САНКТ-ПЕТЕРБУРГСКИЙ
ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
РОССИЙСКОЙ АКАДЕМИИ НАУК»
МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ
НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 12.05.2022 г. № 1

О присуждении Семенову Виктору Викторовичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» принята к защите 27 января 2022 г. (протокол заседания № 1) диссертационным советом 24.1.206.01, созданном на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Минобрнауки России №105/нк от 11 апреля 2012 г. (с изменениями согласно приказам №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г., №467/нк от 4 августа 2020 г., №804/нк от 16 декабря 2020 г., №561/нк от 03 июня 2021 г., №384/нк от 19 апреля 2022 г.).

Соискатель Семенов Виктор Викторович, «15» января 1993 года рождения, в 2020 г. окончил очную аспирантуру в Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский университет ИТМО» по направлению подготовки 10.06.01 «Информационная безопасность» (диплом об окончании аспирантуры 107824 № 4741047). С 2018 года по настоящее время Семенов Виктор Викторович работает

младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена в лаборатории интеллектуальных систем Санкт-Петербургского института информатики и автоматизации Российской академии наук Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Министерства науки и высшего образования Российской Федерации.

Научный руководитель — доктор технических наук, профессор ЛЕБЕДЕВ Илья Сергеевич, основное место работы: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), лаборатория интеллектуальных систем, главный научный сотрудник.

Официальные оппоненты:

ПРИМАКИН Алексей Иванович, доктор технических наук, профессор, Федеральное государственное казенное образовательное учреждения высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации», кафедра специальных информационных технологий, начальник кафедры;

ПАВЛЕНКО Евгений Юрьевич, кандидат технических наук, Федеральное государственное автономное образовательное учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Институт кибербезопасности и защиты информации, доцент

дали **положительные** отзывы на диссертацию.

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

адмирала С.О. Макарова), г. Санкт-Петербург в своем положительном отзыве, подписанном Соколовым Сергеем Сергеевичем, доктором технических наук, доцентом, кафедра комплексного обеспечения информационной безопасности, заведующий кафедрой; Ныркovым Анатолием Павловичем, доктором технических наук, профессором, кафедра комплексного обеспечения информационной безопасности, профессор и утвержденном Барышниковым Сергеем Олеговичем, доктором технических наук, профессором, ректором ГУМРФ имени адмирала С.О. Макарова, указала, что в целом диссертационная работа В.В. Семенова представляет собой законченную и самостоятельную научно-квалификационную работу, выполненную на актуальную тему, обладает научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов.

В диссертационной работе Семенова Виктора Викторовича получены следующие основные результаты, обладающие научной новизной:

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.

Полученные в диссертационной работе научные результаты, выводы и практические рекомендации могут найти применение при разработке систем мониторинга состояния КФС, находящихся под воздействием информационных угроз, на коммерческих предприятиях, таких как СПбФ АО «НПК «ТРИСТАН», АО «Эврика», ООО «НеоБИТ», АО «Лаборатория Касперского», а также при проведении научно-исследовательских и опытно-конструкторских работ в организациях, подведомственных РАН, Министерству обороны РФ, Министерству внутренних дел РФ.

Полученные результаты могут быть внедрены в образовательном процессе ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О. Макарова» по направлениям подготовки бакалавриата 10.03.01 и магистратуры 10.04.01 «Информационная безопасность», а также специалитета 10.05.03 «Информационная безопасность автоматизированных систем».

Автореферат отражает содержание диссертационной работы и содержит все требуемые ГОСТ Р 7.0.11-2011 разделы.

Диссертация «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов», содержащая решение актуальной научно-технической задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз соответствует критериям, изложенным в пунктах 9–14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 года № 842 (в редакции Постановления Правительства РФ от 11.09.2021 года № 1539), предъявляемым к кандидатским диссертациям, а её автор Семенов Виктор Викторович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 29 опубликованных работ, в том числе по теме диссертации опубликовано 29 работ, их них в рецензируемых научных изданиях опубликовано 23 работы. Опубликовано в изданиях 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» – 11, индексируемых в WoS/Scopus – 9, имеется 1 свидетельство о государственной регистрации программы для ЭВМ.

Основные научные результаты опубликованы в 20 научных трудах общим объемом 10,94 п.л., из которых объем личного вклада соискателя составляет 6,85 п.л. Наиболее значимые работы по теме диссертации:

1. **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. *Личный вклад соискателя – 50 %.*
2. **Семенов В.В.** Мониторинг информационной безопасности беспилотных транспортных средств с использованием цифрового акселерометра // Информационные технологии —2020. — Т. 26. — № 7. — С. 424–430.
3. **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. *Личный вклад соискателя – 80 %.*
4. **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. *Личный вклад соискателя – 50 %.*
5. 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. *Личный вклад соискателя – 40 %.*
6. **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. *Личный вклад соискателя – 45 %.*

Оригинальность содержания диссертации составляет не менее 80 % от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной

степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На диссертацию и автореферат поступило 9 отзывов, все отзывы положительные:

1. Общество с ограниченной ответственностью «Цезурити». Отзыв составил руководитель проектов, к.т.н. Лапшин С.В. Замечания: Описание предложенной методики идентификации состояния ИБ КФС представлено автором слишком кратко. Следует пояснить, как повлияет увеличение или уменьшение числа информативных признаков на точность идентификации? Присутствуют некоторые стилистические погрешности в тексте.

2. Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет». Отзыв составил профессор кафедры информационных систем в экономике, д.т.н., старший научный сотрудник Юрков А.В. Замечания: в автореферате на стр. 14 приводятся пять способов оценки показателей качества идентификации: матрица несоответствий, полнота и точность, F-мера, AUC, однако из текста автореферата не ясна причина выбора именно таких способов оценки; недостаточно акцентировано внимание на преимуществах метода на основе деревьев решений, повлекшего его выбор для решения обозначенных в диссертационном исследовании задач.

3. Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки «Институт земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук». Отзыв составил заместитель директора по науке, д.т.н., профессор Коробейников А.Г. Замечания: На стр. 5 автореферата «методика … отличается от существующих применением разработанных модели и метода и позволяет повысить скорость идентификации состояния ИБ элементов КФС без существенной потери точности», при этом в следующем абзаце указано, что «повышается оперативность, точность и полнота». Требует пояснения, теряется точность или увеличивается? Из текста автореферата

не совсем понятно, возможно ли в рамках представленного в работе подхода различить природу возникновения нарушений информационной безопасности?

4. Санкт-Петербургский филиал Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики». Отзыв составил руководитель департамента логистики и управления цепями поставок, заслуженный деятель науки РФ, д.т.н., профессор, Лукинский В.С. Замечания: В тексте автореферата не представлены используемые модели нарушителя и угроз. На стр. 14 автореферата приведено «пять способов оценки показателей качества идентификации состояния ИБ КФС …», однако не сказано, чем вызвано такое разнообразие. Применение разработанных автором модели, метода и методики показано только на примере анализа сетевого трафика киберфизической системы водоочистки. Чем был обусловлен данный выбор?

5. Акционерное общество «Научно-Исследовательский Институт Точной Механики». Отзыв составил заместитель начальника отдела по техническим вопросам, к.т.н. Степанов Ю.Л. Замечания: В автореферате отсутствует обоснование выбора используемого классификатора, в то же время для классификации состояния информационной безопасности можно использовать большое количество различных алгоритмов машинного обучения. Для более полной оценки предлагаемых в рамках исследования подходов было бы интересно увидеть результаты применения разработанной методики с использованием других алгоритмов машинного обучения. Следовало бы уточнить, какой временной период может охватывать полученный прогноз (стр. 12 автореферата).

6. Санкт-Петербургский филиал Акционерного общества «НПК «ТРИСТАН». Отзыв составил заместитель директора по программному обеспечению к.т.н. Шахпаронян А.П и утвердил первый заместитель директора Соловьев И.Н. Замечания: Недостаточно полно раскрыт вопрос эффективности существующих методов идентификации состояния информационной безопасности, основанных на машинном обучении при рассматриваемых условиях. Представляется, что при проведении мониторинга необходимо учитывать возможности используемой вычислительной и сетевой аппаратно-программной базы. В то же время, в

описании предложенной методики идентификации состояния информационной безопасности киберфизических систем в тексте автореферата этот вопрос не рассматривается.

7. Общество с ограниченной ответственностью «АПСТЕК Лабс». Отзыв составил ведущий инженер-программист, к.т.н. Спивак А.И. Замечания: Почему сравнение результатов исследования (таблица 2 на стр. 15 автореферата) произведено только с различными вариациями классификаторов на основе нейронных сетей? Наблюдаются незначительные отклонения от ГОСТ Р 7.0.11-2011.

8. Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет». Отзыв составил профессор кафедры информационных технологий и систем безопасности, д.т.н., профессор, Бурлов В.Г. Замечания: Недостаточно подробно описана методика идентификации состояния информационной безопасности киберфизических систем. В автореферате не рассматривается возможность реагирования на выявленные инциденты информационной безопасности на основе полученных данных мониторинга.

9. Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО». Отзыв составил доцент факультета безопасности информационных технологий, к.т.н., доцент Воробьева А.А. Замечания: Недостаточно подробное описание метода оценивания состояния информационной безопасности элементов киберфизических систем. Неточности и неаккуратность в использовании понятий, а именно: а. В описании практической значимости работы указано, что разработанные подходы позволяют повысить оперативность оценивания защищённости ИБ КФС. Не дано определение понятию «оперативность». В описании четвертой главы приведены результаты экспериментов по оценке временных затрат на обработку данных мониторинга состояния ИБ, экспериментов по именно по оценке оперативности не представлено. Из общепринятого определения понятия оперативности, как способности правильно и быстро осуществлять те или иные практические задачи, можно предположить, что здесь

под оперативностью подразумевается, сокращение временных затрат на обработку данных мониторинга при условии обеспечения необходимого значения показателей качества (полноты и точности) идентификации состояний ИБ КФС. Эксперименты по оценке указанных показателей приведены. b. Целью работы заявлено повышение полноты и точности обнаружения нарушений ИБ КФС, но в автореферате, в описании четвертой главы, представлены эксперименты по оценке качества идентификации состояния ИБ КФС и идентификации атак различных типов на КФС и её отдельные элементы. Однако, из текста автореферата можно сделать выводы, что обнаружение (выявление) нарушений ИБ КФС сводится к решению задачи идентификации состояния ИБ КФС и идентификации атак различных типов; и что понятия «обнаружение нарушений ИБ КФС» и «идентификация состояния ИБ КФС» в автореферате синонимичны. Имеются некоторые иные стилистические неточности в тексте автореферата.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Примакин А.И. является известным учёным в области защиты информации и обеспечения информационной безопасности автоматизированных систем, разработал модель формирования требований к конфиденциальности, целостности и доступности данных в системе защиты информации средств вычислительной техники и автоматизированных систем; к.т.н. Павленко Е.Ю. – известный специалист в области информационной безопасности киберфизических систем, один из авторов концепции обеспечения информационной безопасности киберфизических систем на основе принципа гомеостаза; ведущая организация, Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», является известной как в России, так и за рубежом организацией в области разработки и исследований систем защиты информации, а также систем мониторинга состояния объектов, находящихся под воздействием угроз нарушения их информационной безопасности, кроме того, широко известны достижения её специалистов в области разработки методов определения аномалий информационной безопасности объектов критической инфраструктуры и методов повышения защищенности циркулирующих в них данных.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработана оригинальная методика идентификации состояния информационной безопасности киберфизических систем на основе анализа временных рядов, обеспечивающая повышение полноты и точности;

предложены:

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;

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;

методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС, отличающаяся от существующих применением разработанных модели и метода и способствующая повышению скорости 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;

доказана перспективность использования предложенных модели, метода и методики для построения систем детектирования аномалий информационной безопасности и оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов;

введены:

- модель признакового пространства для оценивания состояния информационной безопасности элементов киберфизических систем, основанная на применении наиболее информативных характеристик;
- требования к выбору признаков, позволяющих идентифицировать состояния информационной безопасности киберфизических систем.

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с использованием формальных математических доказательств и серии вычислительных экспериментов о применимости предложенных модели, метода и методики. Эти утверждения составляют основу процесса оценивания защищённости киберфизических систем от информационных угроз с целью обеспечения их безопасного функционирования;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использован аппарат теории информационной безопасности, методы математической статистики, включая метод главных компонент, теория предпочтений, методы машинного обучения, экспериментальные методы исследования;

изложены:

методологические и методические основы обеспечения информационной безопасности киберфизических систем, базирующиеся на методах машинного обучения, использующих многомерное признаковое пространство внешней идентификации текущего состояния;

доказательства адекватности и работоспособности разработанных модели, метода и методики;

раскрыты:

проблемные аспекты применения имеющихся подходов для решения задач мониторинга информационной безопасности киберфизических систем;

значимые противоречия между возможностями, которые предоставляют технологии киберфизических систем, и существующим научно-методическим и

математическим обеспечением систем и устройств, реализующих алгоритмы автоматизированной обработки в целях выявления различных инцидентов информационной безопасности в ходе функционирования;

основные вопросы, связанные с преодолением проблемы размерности в практических задачах обеспечения информационной безопасности киберфизических систем;

изучены существующие модели, методы и алгоритмы обеспечения информационной безопасности функционирования элементов киберфизических систем, при этом особое внимание уделено методам интеллектуального анализа данных и особенностям применения алгоритмов машинного обучения в задачах многоклассовой классификации;

проведена модернизация существующих моделей, методов и методик обеспечения информационной безопасности киберфизических систем с целью оптимизации управленческого цикла принятия решений в условиях внешних и внутренних информационных воздействий.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены следующие результаты диссертационной работы:

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

внедрены в рамках научно-исследовательских работ, выполненных в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (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;

• 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;

использованы 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;

определены возможности и перспективы использования полученных результатов диссертации на практике, при разработке систем обнаружения нарушений информационной безопасности элементов киберфизических систем;

создана программа для ЭВМ, представляющая собой основу для разработки комплексной системы оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов, увеличивающая полноту и точность идентификации, и позволяющая устранить недостатки существующих методов;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные модель, метод и методика.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ при реализации вычислительного эксперимента выявлено соответствие полученных расчётных результатов и результатов при внедрении в информационные производственные системы мониторинга состояния информационной безопасности;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов информационной безопасности и методологии защиты информации, методов математической статистики, теории предпочтений, методов машинного обучения, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области идентификации состояния информационной безопасности киберфизических систем и обеспечения информационной безопасности автоматизированных систем;

использованы полученные экспериментальные результаты на основе модели формирования признакового описания состояния информационной безопасности элементов киберфизических систем, метода оценивания состояния ИБ, методики идентификации состояния ИБ КФС для сравнения с результатами, приведёнными в современной научной и технической литературе;

установлено качественное и количественное соответствие результатов решения задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз. При этом подтверждено преимущество предложенного подхода перед результатами, полученными другими авторами.

использованы представительные выборочные совокупности объектов наблюдения, современные методики сбора и обработки исходных данных о состоянии киберфизических систем.

Личный вклад соискателя состоит в:

- анализе современного состояния исследований в области выявления нарушений информационной безопасности киберфизических систем;
- постановке задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз;
- разработке модели угроз информационной безопасности объектов исследования, определении угроз ИБ, характерных для различных типов КФС;

- обосновании выбора показателей эффективности идентификации состояния ИБ КФС, таких как полнота и точность, F-мера, матрица несоответствий, AUC и количество идентификационных признаков;
- разработке и обосновании модели формирования признакового описания состояния информационной безопасности элементов киберфизических систем;
- разработке и обосновании метода оценивания состояния информационной безопасности элементов киберфизических систем;
- разработке и обосновании методики идентификации состояния ИБ КФС;
- разработке прототипа программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз на основе анализа временных рядов;
- подготовке практических рекомендаций по использованию результатов исследования для повышения защищённости КФС от внешних информационных воздействий;
- подготовке основных публикаций по выполненной работе.

В ходе защиты диссертации были высказаны следующие критические замечания: автором были использованы классифицирующие алгоритмы для оценивания состояния ИБ киберфизических систем в области исследований, в которой данные могут обладать различными свойствами.

Соискатель Семенов В.В. ответил на задаваемые ему в ходе заседания вопросы и привел собственную аргументацию, что для целей оценивания защищённости киберфизических систем от информационных угроз необходимо рассматривать выборки, обладающие различными свойствами и, исходя из результатов обработки данных классифицирующими алгоритмами, выбирать модель, имеющую лучшие полноту и точность для выборок и подвыборок.

На заседании 12.05.2022 г. диссертационный совет принял решение за решение научной задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз, имеющей значение для развития теории и практики обеспечения информационной

безопасности присудить Семенову В.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 18 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за 18, против нет, недействительных бюллетеней нет.

Заместитель председателя диссертационного совета
доктор технических наук,
профессор РАН Ронжин Андрей Леонидович

Ученый секретарь диссертационного совета
кандидат технических наук Абрамов Максим Викторович
12.05.2022 г.