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
Директор СПб ФИЦ РАН
Профессор РАН

_____ А.Л. Ронжин
«15» 04 2021 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) по диссертации Семенова Виктора Викторовича «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов», представленной на соискание учёной степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки)

Диссертация «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» выполнена в лаборатории интеллектуальных систем Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук».

Соискатель Семенов Виктор Викторович работает по основному месту работы в должности младшего научного сотрудника в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» с 2018 года по настоящее время.

В 2020 году Семенов Виктор Викторович окончил очную аспирантуру Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО» по направлению подготовки 10.06.01 – «Информационная безопасность», профилю «Методы и системы защиты информации, информационная

безопасность». Диплом об окончании аспирантуры 107824 № 4741047, выдан 8 июля 2020 года, квалификация «Исследователь. Преподаватель-исследователь».

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».

По результатам рассмотрения диссертации «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» принято следующее заключение:

Оценка выполненной соискателем работы:

В диссертационной работе рассмотрены и проанализированы существующие подходы к выявлению нарушений информационной безопасности (ИБ) киберфизических систем (КФС). Разработана модель угроз информационной безопасности объектов исследования, определены угрозы, характерные для различных типов киберфизических систем. Разработан алгоритм, способный из доступного числа параметров киберфизической системы выявить наиболее информативные и использовать их для формирования признакового описания состояния информационной безопасности. Разработан метод оценивания состояния информационной безопасности элементов киберфизических систем, основанный на применении ансамбля параллельно работающих классификаторов и весовых коэффициентов Фишберна в качестве постобработки результатов классификации. Разработана методика идентификации состояния информационной безопасности киберфизических систем, позволяющая достичь заданной точности и полноты, уменьшив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга информационной безопасности киберфизических систем. Применимость разработанных модели, метода и предложенной методики идентификации состояния информационной безопасности киберфизических систем обоснована при помощи вычислительного эксперимента. Произведена оценка характеристик классификации и сравнение с существующими методами. Даны рекомендации по использованию результатов исследования для повышения защищённости киберфизических систем от внешних воздействий.

Личное участие соискателя в получении результатов, изложенных в диссертации:

Теоретические и экспериментальные результаты диссертационной работы получены автором самостоятельно. Разработаны: 1. модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем; 2. метод оценивания защищённости элементов киберфизических систем от информационных угроз; 3. 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.

Степень достоверности результатов проведенных исследований:

Достоверность полученных результатов работы подтверждается согласованностью теоретических выводов с результатами экспериментальной проверки модели, метода и методики, сравнением с результатами других исследователей, практической апробацией разработанной методики и одобрением основных положений диссертационной работы на научно-технических конференциях. 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.

Основные результаты диссертации 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.

Результаты, полученные в диссертации, были реализованы 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».

Научная новизна полученных результатов:

Разработана 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.

Разработан 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.

Разработана методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности, сократив временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС, отличающаяся от существующих применением разработанных модели и метода, а также повышением 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.

Практическая значимость полученных результатов:

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 повышаются точность и полнота оценивания защищённости ИБ КФС, что позволяет на практике эффективно применять разработанный подход в системах мониторинга событий информационной безопасности.

Специальность, которой соответствует диссертация

Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки).

Полнота изложения материалов диссертации в работах, опубликованных соискателем

Основные результаты диссертационной работы изложены в достаточной полноте в печатных трудах: опубликовано 29 печатных работ, среди них статей в журналах, рекомендованных ВАК Министерстве науки и высшего образования Российской Федерации – 11, публикаций, входящих в базы цитирования Web of Science и Scopus – 9, в прочих изданиях – 8, свидетельств о государственной регистрации программ для ЭВМ – 1.

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

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. («**Перечень ВАК**»).

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. («**Перечень ВАК**»).

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.

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**).

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.

Ценность научных работ соискателя заключается в том, что они раскрывают методологию решения поставленной в диссертационном исследовании задачи разработки методов обнаружения нарушений информационной безопасности киберфизических систем, повышающих их защищённость от информационных угроз, а также обеспечивают воспроизводимость полученных научных результатов.

Диссертационная работа соответствует требованиям пунктов 9-14 «Положения о присуждении ученых степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 № 842 (в редакции от 20.03.2021).

Диссертационная работа «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» Семенова Виктора Викторовича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки).

Заключение принято на расширенном семинаре лабораторий интеллектуальных систем, информационно-вычислительных систем и технологий программирования, проблем компьютерной безопасности, кибербезопасности и постквантовых криптосистем. Присутствовало на заседании 12 чел. Результаты голосования: «за» – 12 чел., «против» – 0 чел., «воздержалось» – 0 чел., протокол № 1 от «14» апреля 2021 г.

Заведующий лабораторией
интеллектуальных систем,
доктор технических наук,
профессор

Ю.М. Искандеров

Ведущий научный сотрудник лаборатории
проблем компьютерной безопасности,
кандидат технических наук, доцент

А.А. Чечулин