УТВЕРЖДАЮ:
Ректор ФГБОУ ВО «ГУМРФ имени
адмирала С.О. Макарова»,
доктор технических наук, профессор

С.О. Барышников
04 _____ 2022 г.

ОТЗЫВ

ведущей организации

на диссертационную работу Семенова Виктора Викторовича «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

1. 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 диссертационной работе решена научная задача повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов.

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.

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, являющихся объектами критической инфраструктуры, что в совокупности с недостаточной точностью и оперативностью обнаружения нарушений ИБ КФС определяет важность и значимость решаемой научной задачи.

В связи с вышеуказанным, тема диссертации «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе

анализа временных рядов» является актуальной, а решаемая в диссертационной работе научная задача имеет как теоретическую, так и практическую значимость.

2. ЛИЧНОЕ УЧАСТИЕ АВТОРА И АПРОБАЦИЯ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Личное участие автора в проведенных исследованиях заключается в разработке модели формирования признакового описания состояния ИБ, метода оценивания защищённости элементов киберфизических систем от информационных угроз, а также методики идентификации состояния информационной безопасности киберфизических систем на основе анализа временных рядов.

Автором самостоятельно разработан и зарегистрирован в установленном порядке прототип программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз на основе анализа временных рядов.

Положения, выносимые на защиту, и результаты работы базируются на теории информационной безопасности информационных систем, методах математической статистики, теории предпочтений, методах машинного обучения и математического моделирования.

Результаты работы докладывались и обсуждались на всероссийских и международных научно-технических 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.

По результатам диссертационного исследования автором опубликовано 29 работ, из них статей 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» – 11, входящих в базы цитирования Web of Science и Scopus – 9, в прочих изданиях – 8, свидетельств о государственной регистрации программы для ЭВМ – 1.

Результаты диссертационного исследования реализованы при выполнении

НИР и НИОКТР:

– 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.

3. НОВИЗНА ИССЛЕДОВАНИЯ И ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ, ВЫВОДОВ И РЕКОМЕНДАЦИЙ

В отличие от ранее проводимых исследований, для увеличения точности оценивания защищённости киберфизических систем от информационных угроз диссертантом предложено оригинальное идентификационное признаковое пространство, формируемое с использованием метода анализа главных компонент. Разработан алгоритм, способный из доступного числа параметров КФС выделить наиболее информативные для данной КФС и использовать их для формирования признакового описания состояния ИБ КФС.

Особенностью предложенного подхода является 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, что позволяет снизить время и повысить точность идентификации, по сравнению с существующими подходами, рассмотренными в работе.

Диссертантом разработана методика идентификации состояния ИБ КФС использующая методы машинного обучения при анализе значений временных рядов от наиболее информативных источников.

На основе предложенного подхода диссертантом определены направления адаптации разработанных методов для совершенствования средств обеспечения аудита и мониторинга состояния объектов, находящихся под воздействием угроз нарушения информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.

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.

Особенностью результатов является использование комбинированного подхода, для чего диссертантом выполнено:

1. Определение угроз информационной безопасности, характерных для различных типов КФС, и разработка модели угроз ИБ объектов исследования.
2. Разработка алгоритма, способного из доступного числа параметров КФС выделить наиболее информативные для данной КФС и использовать их для формирования признакового описания состояния ИБ КФС.
3. Разработка метода оценивания состояния ИБ элементов КФС, основанного на применении ансамбля параллельно работающих классификаторов и весовых коэффициентов Фишберна в качестве постобработки результатов классификации.
4. 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.
5. Разработка прототипа программного обеспечения, реализующего оценивание защищённости КФС от информационных угроз на основе анализа временных рядов.
6. Количественное сравнение полученных в диссертационной работе результатов с результатами других исследователей.

Указанные научно обоснованные технические и технологические решения способствуют повышению уровня защищенности КФС, а предлагаемая методика идентификации, демонстрирует повышение оперативности, точности и полноты оценивания защищённости ИБ КФС, что позволяет на практике эффективно применять разработанный подход в системах мониторинга событий информационной безопасности.

4. ЗНАЧИМОСТЬ ПОЛУЧЕННЫХ АВТОРОМ ДИССЕРТАЦИИ РЕЗУЛЬТАТОВ ДЛЯ НАУКИ И ПРАКТИКИ

Полученные в диссертации научные результаты являются еще одним существенным шагом на пути совершенствования технологий идентификации состояния информационной безопасности элементов киберфизических систем.

Практическую значимость результатов диссертационной работы составляют разработанная модель, метод и методика идентификации. Предложенная методика идентификации состояния ИБ элементов КФС позволяет достигать

точности идентификации 99,85 %.

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 и даёт возможность применять результаты в системе событиями информационной безопасности, системах обнаружения атак.

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 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.

Совокупность предложенных в исследовании методов позволяет осуществить решение задачи разработки и обоснования научно-методического аппарата оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов, что обуславливает значимость полученных автором диссертации результатов для развития соответствующей отрасли науки.

5. ДОСТОВЕРНОСТЬ И ОБОСНОВАННОСТЬ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Обоснованность и достоверность полученных научных результатов определяется:

– научной обоснованностью приводимых выкладок и математических преобразований;

– использованием теории ИБ информационных систем, методов математической статистики, включая метод анализа главных компонент для вычисления информативности признаков, описывающих состояние информационной безопасности КФС, теории предпочтений для формирования соответствий элементов анализируемых временных рядов с весовыми коэффициентами значимости, методов машинного обучения для решения задач классификации состояний ИБ, методов математического моделирования для построения формализованных моделей исследуемых объектов и протекающих в них информационных процессов;

– системным анализом объекта исследования, учётом сложившихся практик и опыта в информационной безопасности;

– проведением сравнительного анализа предложенных модели, метода и методики с существующими решениями и результатами экспериментов;

– непротиворечивостью полученных результатов известным решениям.

Достоверность результатов дополнительно подтверждается корректным функционированием программного обеспечения, использующего полученные соискателем результаты (свидетельство о регистрации программы для ЭВМ: «Программа для определения состояния информационной безопасности отдельных компонентов вычислительных систем» № 2019618203 от 26.06.2019).

6. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ РЕЗУЛЬТАТОВ И ВЫВОДОВ

Проведенные в диссертации исследования представляется перспективным развивать в направлении расширения практических возможностей разработанной методики и интеллектуальной программной системы.

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».

7. СООТВЕТСТВИЕ СОДЕРЖАНИЯ ДИССЕРТАЦИИ И АВТОРЕФЕРАТА

Автореферат отражает содержание диссертационной работы и содержит все требуемые ГОСТ Р 07.0.11-2011 разделы.

Содержание диссертации в полной мере соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Автореферат и диссертация удачно структурированы, написаны в хорошем стиле и на понятном техническом языке.

По предоставленному библиографическому списку и прилагаемому перечню собственных публикаций автора можно сделать вывод о том, что основные положения диссертации достаточно полно изложены в печатных работах и апробированы на профильных научных и технических конференциях.

8. ОСНОВНЫЕ ЗАМЕЧАНИЯ ПО ДИССЕРТАЦИИ

В качестве недостатков работы можно отметить следующие:

1. Исследование направлено на оценивание защищённости киберфизических систем от информационных угроз, однако недостаточно внимания уделено особенностям киберфизических систем, позволяющим однозначно определять природу происхождения деструктивных воздействий.

2. Не вполне понятно, в соответствии с каким принципом следует выбирать количество главных компонент, по которым рассчитывается информативность признаков, и как повлияет увеличение или уменьшение порогового значения совокупной объяснённой дисперсии на конечный результат идентификации защищённости КФС.

3. Недостаточно акцентировано внимание на преимуществах классифицирующего алгоритма на основе деревьев решений, повлекшего его выбор для решения обозначенных в диссертационном исследовании задач, а также мало внимания уделено ограничениям, возникающим в результате его использования.

4. В тексте диссертации недостаточно ясно отражена практическая реализация методики идентификации состояния информационной безопасности киберфизических систем, её место в задаче организации информационной безопасности.

5. Необходим анализ ресурсоемкости и вычислительной сложности предложенных решений, чтобы говорить о возможности применения в программном обеспечении, реализующем оценивание защищённости киберфизических систем от информационных угроз в режиме реального времени.

Перечисленные замечания и недостатки не снижают научный уровень проведенных исследований и не влияют на общий положительный вывод о качестве представленной к защите диссертации.

9. ЗАКЛЮЧЕНИЕ ПО ДИССЕРТАЦИОННОЙ РАБОТЕ

Представленная диссертация соответствует требованиям ВАК, предъявляемым к кандидатским диссертациям, обладает научной новизной и практической значимостью.

Диссертационное исследование Семенова Виктора Викторовича является законченной самостоятельной научно-квалификационной работой, которая вносит значительный вклад в решение актуальной задачи разработки методов повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов, что позволяет на практике эффективно применять разработанный подход в системах мониторинга событий информационной безопасности.

Содержание и основные научные результаты соответствуют паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». Автореферат диссертации достаточно полно отражает основное содержание диссертационной работы. По оформлению работа соответствует требованиям, предъявляемым к диссертациям.

На основании изложенного можно сделать вывод, что 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 порядке присуждения

ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 года № 842 (в редакции Постановлений 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».

Диссертационная работа Семенова Виктора Викторовича обсуждена на заседании кафедры комплексного обеспечения информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», присутствовали 23 чел., из них 8 докторов технических и военных наук, протокол № 09 от «08» апреля 2022 года.

Отзыв составил профессор кафедры комплексного обеспечения информационной безопасности, д.т.н., профессор Ныркова А.П.

Профессор кафедры комплексного
обеспечения информационной
безопасности,
д.т.н., профессор Ныркова Анатолий Павлович

Заведующий кафедрой
комплексного обеспечения
информационной безопасности,
д.т.н., доцент Соколов Сергей Сергеевич

Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова» (ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»).
Адрес: Двинская ул., д. 5/7, г. Санкт-Петербург, 198035;
тел.: (812) 748-96-92;
e-mail: otd_o@gumrf.ru;
сайт: https://gumrf.ru/.