ОТЗЫВ

официального оппонента, кандидата технических наук
Павленко Евгения Юрьевича
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 избранной темы диссертации

Глобальные изменения, связанные с цифровизацией жизнеобразующих отраслей деятельности и стремительным развитием беспроводных, сенсорных и облачных технологий, привели к появлению нового типа объектов и систем – киберфизических. Киберфизические системы (КФС) объединяют в себе информационную и физическую составляющие, реализуя автономно от человека различные технологические процессы посредством обмена данными и реагирования компонентов системы на значения передаваемых параметров.

Актуальность избранной темы диссертационной работы вызвана критичностью нарушений корректного функционирования КФС. Выход из строя таких систем, интегрированных с критическими отраслями деятельности, может повлечь за собой экологическую катастрофу и привести к человеческим жертвам. В связи с этим, для получения наиболее достоверной оценки защищенности КФС, следует принимать во внимание не только безопасность циркулирующей в системе информации, но и характеристики протекания технологических процессов, свидетельствующие о наличии либо отсутствии нарушений. В таких условиях диссертационная работа соискателя Семенова В.В., несомненно, является актуальной, поскольку, решая задачу оценивания защищённости КФС от информационных угроз, соискатель учитывает не только информационную безопасность, но и корректность протекания технологических процессов, что реализуется, в том числе, за счет повсеместного применения в КФС различных датчиков и контроллеров, обменивающихся информацией.

Актуальность решения задачи оценивания защищённости киберфизических систем от информационных угроз подчеркивается активно ведущимися работами по созданию промышленных КФС и вытекающей из этого необходимостью обеспечения их корректного функционирования, в том числе в условиях реализации на них кибератак. За последние 10 лет число проектов, разработок и исследований, направленных на автоматизацию производственных процессов и

инфраструктуры критических отраслей деятельности, значительно увеличилось. Таким образом, предлагаемые в диссертации модель, метод и методика идентификации состояния информационной безопасности КФС, являются актуальными и востребованными.

2. Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность

Достоверность и обоснованность результатов исследования определяются применением апробированных средств и методов исследования, корректностью принятых допущений и ограничений, достоверностью исходных данных, оказывающих существенное влияние на анализ предметной области, серией расширенных вычислительных экспериментов, непротиворечивостью полученных результатов и их согласованностью с результатами исследований, проведенных другими авторами по тематике, близкой к теме диссертационной работы, а также актами внедрения и публикациями в рецензируемых и приравненных к ним изданиях.

Автором диссертационной работы в процессе решения поставленных задач разработано программное обеспечение, вошедшее в состав функционирующих систем организаций реального сектора экономики, что подтверждается полученным свидетельством о регистрации программы для ЭВМ.

3. Научная новизна диссертационной работы

Новизна исследования и полученных результатов заключается в том, что лично автором впервые:

- обоснована модель формирования признакового описания состояния информационной безопасности (ИБ) элементов киберфизических систем, отличающаяся от известных применением метода 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 и апробирована методика идентификации состояния ИБ КФС, позволяющая достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС, и отличающаяся от существующих применением разработанных модели

и метода, позволяющая 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.

Модификация и теоретическое обобщение полученных результатов предоставляют возможность совершенствования и адаптации технологий идентификации состояния ИБ КФС.

Кроме того, необходимо отметить, что автором диссертационного исследования произведен анализ характеристических особенностей КФС и дана оценка их влияния на точность оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов.

4. Общая оценка диссертационной работы

В рассматриваемой диссертационной работе предложены модель, метод и методика, которые могут быть адаптированы для любой из задач идентификации, а также реализованы как часть систем мониторинга средств вычислительной техники и киберфизических систем.

В диссертационной работе для увеличения показателей полноты и точности процессов идентификации предлагается использование наиболее информативных признаков, получаемых в результате формирования признакового описания состояния информационной безопасности элементов киберфизических систем при помощи метода главных компонент.

Разработанное решение заключается в расчете и отборе информативных признаков для задачи оценивания защищённости киберфизических систем от информационных угроз и последующем анализе сформированных многомерных временных рядов, что принципиально отличает его от ряда других.

Автором было экспериментально обосновано применение вышеописанного подхода и подтверждено, что применение сформированного признакового описания состояния информационной безопасности элементов киберфизических систем позволяет повысить скорость идентификации состояния ИБ элементов КФС.

Полученные автором научные результаты позволили увеличить полноту, точность и скорость идентификации состояния ИБ элементов КФС за счёт применения параллельно работающих классификаторов и весовых коэффициентов Фишберна при анализе совокупности информативных признаков, полученных из временных рядов, характеризующих функционирование и сопутствующие информационные процессы КФС.

Результаты диссертационной работы Семенова Виктора Викторовича доложены и апробированы на 10 всероссийских и международных научно-

технических конференциях, опубликованы в 29 печатных и приравненных к ним работах (в том числе статьях 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 Web of Science и Scopus – 9).

5. Теоретическая и практическая значимость полученных результатов

Значимость результатов исследования для науки и практики заключается в обоснованных теоретических положениях (в виде модели, метода и методики), существенно расширяющих научный базис в области информационной безопасности, а также в разработанных алгоритмических и программных средствах, предназначенных для анализа многомерных временных рядов с целью выявления нарушений ИБ, направленных на изменение параметров функционирования КФС.

Результаты проведенного диссертационного исследования доведены до уровня, обеспечивающего возможность их непосредственного практического использования в системах, обеспечивающих идентификацию состояния ИБ КФС и системах оценивания защищённости киберфизических систем от информационных угроз, что обуславливает их высокую практическую значимость. Разработанная методика и алгоритмы могут быть использованы при проектировании систем мониторинга ИБ КФС в АО «Лаборатория Касперского», ООО «Яндекс», при эксплуатации беспилотных транспортных средств в ОАО «РЖД», а также в образовательном процессе при подготовке специалистов в ФГАОУ ВО «СПбПУ» по направлениям 10.05.03 «Информационная безопасность автоматизированных систем» и 10.05.04 «Информационно-аналитические системы безопасности».

Кроме того, результаты диссертационной работы на настоящий момент уже внедрены на предприятии промышленности СПбФ АО «НПК «Тристан» и в процессе проведения ряда НИОКР в ФГБУН «СПб ФИЦ РАН», по итогам внедрения соискателем получены соответствующие акты о реализации проведенных исследований.

6. Замечания и рекомендации

Диссертация написана хорошим техническим языком, грамотно и аккуратно оформлена. По каждой главе и работе в целом сделаны четкие выводы, однако работа не лишена ряда недостатков, основными из которых являются следующие:

1. Соискателю следовало бы обосновать, почему при постановке задачи диссертационного исследования (стр. 36 диссертации) КФС рассматривается как замкнутая система. Отсюда же следует вопрос о слабо определенных границах

применимости и ограничениях модели, методики и алгоритмов, предлагаемых в диссертационном исследовании.

2. Следовало бы уделить отдельное внимание формированию многомерных временных рядов, являющихся ключевым объектом анализа. А именно, следовало бы рассмотреть различные варианты объединения одномерных временных рядов (по участию источников, порождающих их, в едином технологическом процессе; по локализации источников – например, данные от одного из производственных цехов; и т.д.).

3. Возникает вопрос о влиянии обучающей выборки, связанном с изменением функциональности и типа киберфизической системы, на полученные результаты.

4. В диссертационной работе не рассматриваются альтернативные классификаторы, которые можно было бы применить в ансамбле.

5. Не приведена полная сравнительная оценка вычислительной сложности разработанных алгоритмов, что рекомендовалось бы сделать в условиях ограниченной вычислительной мощности отдельных КФС, включающих множество маломощных датчиков, актуаторов и контроллеров.

6. Встречаются незначительные отклонения от стандартов при оформлении диссертационного исследования.

Перечисленные замечания и рекомендации существенно не влияют на качество и значимость диссертационной работы и не снижают общий положительный вывод о представленной к защите диссертации.

7. Заключение

Диссертация Семенова Виктора Викторовича является законченной научно-квалификационной работой, выполненной автором самостоятельно на достаточном научно-техническом уровне, и содержит решение важной научной задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз. Автореферат диссертации удачно структурирован, полностью соответствует основному содержанию работы и составлен в соответствии с предъявляемыми требованиями.

В диссертационной работе представлены результаты, обладающие научной новизной, теоретической и практической значимостью, направленные на увеличение 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.

Диссертационная работа, выполненная соискателем, способствует

повышению значений показателей защищенности киберфизических систем от информационных угроз за счет увеличения эффективности процессов идентификации состояния ИБ на основе анализа временных рядов.

Диссертация Семенова Виктора Викторовича «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» полностью соответствует требованиям пунктов 9–14 «Положения о присуждении ученых степеней», утверждённого 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 учёной степени кандидата технических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
кандидат технических наук, доцент Института кибербезопасности и защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

«14» апреля 2022 г. Павленко Евгений Юрьевич

Подпись Павленко Е.Ю.
УДОСТОВЕРЯЮ
ведущий специалист
по кадрам
14.04 2022 г.

Сведения о составителе отзыва:
ФИО: Павленко Евгений Юрьевич
Ученая степень: кандидат технических наук
Место работы: Федеральное государственное автономное образовательное учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»
Должность: доцент
Почтовый адрес: 195251, г. Санкт-Петербург, ул. Политехническая, д. 29
Телефон: +7 (812) 552-76-32
Эл. почта: pavlenko_eyu@spbstu.ru