ОТЗЫВ

официального оппонента, доктора технических наук, профессора
Примакина Алексея Ивановича
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 диссертационной работы

Обеспечение информационной безопасности киберфизических систем является актуальной задачей для современной промышленности, управления процессами производства, а также целого ряда других областей. Современные задачи мониторинга включают различные области, начиная от поиска и оценки угроз и заканчивая обнаружением вторжений и аудитом инцидентов информационной безопасности (ИБ). Решение задачи обеспечения ИБ киберфизических систем невозможно без проведения комплексного и разностороннего мониторинга информационной безопасности и оценивания защищённости киберфизических систем.

В случае реализации угроз ИБ основной целью злоумышленника, как правило, является получение возможности управления киберфизической системой 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 киберфизических систем, приводя при этом к финансовым потерям, а также нанося организациям серьёзный имиджевый ущерб.

Задача идентификации состояния информационной безопасности киберфизических систем имеет важное прикладное значение, однако, применение существующих решений вызывает ряд трудностей различного характера. Противоречие между научно-методическим уровнем технологий оценивания защищённости киберфизических систем и требуемым состоянием особенно остро проявляется в связи с постоянным ростом числа обрабатываемых параметров и соответствующим ему увеличением требуемых вычислительных мощностей.

В связи с этим, актуальными являются работы, направленные на изучение и разработку моделей и методов оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов.

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

Обоснованность и достоверность полученных научных результатов

определяется:

– корректностью постановки задачи исследования и введёнными ограничениями;

– использованием апробированного математического аппарата;

– серией вычислительных экспериментов и сравнительным анализом с существующими методами оценивания защищённости киберфизических систем от информационных угроз;

– применением апробированных методов исследования, согласованностью результатов, полученных при теоретическом исследовании, с результатами экспериментов;

– практической апробацией при реализации научно-исследовательских работ, а также одобрением на всероссийских и международных научно-технических конференциях;

– корректным функционированием программного обеспечения (получено свидетельство о регистрации программы для ЭВМ), использующего полученные результаты, разработанного соискателем в ходе проведения научно-исследовательской работы «Теория и распределенные алгоритмы самоорганизации группового поведения агентов в автономной миссии» для проекта по программе Президиума РАН № 0073-2018-0008.

3. Оценка сущности и содержания диссертации

Подход автора к изучению рассматриваемой проблемы обладает новизной и продуктивностью. Структуру представленной диссертации отличает продуманность и логичность изложения. Текст диссертации, отражающий ход и результаты исследования, состоит из введения, четырех глав, заключения, списка сокращений, списка литературы, включающего 147 источников, четырёх приложений.

Во введении обоснован выбор темы исследования и её актуальность, представлена степень разработанности темы, определены объект, предмет и цель исследования; описаны частные задачи, обоснована теоретическая и практическая значимость полученных результатов; раскрыты принципы предлагаемых подходов и разработанной методики; сформулированы положения, выносимые на защиту и описана апробация результатов исследования.

Во второй главе описана постановка задачи исследования и разработана модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем (КФС), отличающаяся от существующих применением метода главных компонент для вычисления информативности признаков и создания уникального признакового описания состояния ИБ для разных типов КФС или отдельных элементов КФС.

В третьей главе разработан метод оценивания состояния информационной безопасности элементов киберфизических систем и методика, использующая предложенный метод. Приведены схемы и алгоритмы реализации предложенных подходов. Предложенный метод

позволяет существенно повысить точность идентификации состояния ИБ элементов КФС как за счёт применения ансамбля параллельно работающих классификаторов, так и с помощью обобщения и взвешенного усреднения результатов идентификации на временном отрезке, сокращая при этом ошибки из-за случайных отклонений параметров функционирования КФС.

Разработанная методика характеризуется большей полнотой идентификации атак и деструктивных воздействий, меньшим временем принятия решения за счёт лишь однократной предобработки исходных данных обучающей и тестовой выборок на этапе формирования информативных признаков и дальнейшем применении классификаторов, работающих параллельно.

В четвёртой главе показана экспериментальная реализация методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов, использующая методы их обработки. Полнота и точность идентификации при применении методики оценена на основе серии экспериментов. Произведено сравнение показателей качества идентификации с результатами других исследователей, применивших различные методы предобработки и последующей классификации временных рядов, характеризующих функционирование КФС. Выделены ограничения и разработаны практические рекомендации по применению методики для повышения защищённости КФС от внешних воздействий.

Проведенные эксперименты показали достижимость целей мониторинга инцидентов ИБ, что позволяет применять разработанные модель, метод и методику в качестве дополнительных программных систем мониторинга ИБ КФС.

В заключении приведены основные результаты диссертационной работы и выводы, описаны возможные сценарии применения методики идентификации состояния информационной безопасности элементов киберфизических систем на основе анализа временных рядов, а также сформулированы перспективы области исследования.

4. Основные результаты диссертационного исследования и оценка новизны

Научная новизна рассматриваемой диссертационной работы заключается в следующем:

– 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;

– предложена 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.

Предложенные модель, метод и методика отличаются от известных использованием оригинального признакового пространства для описания состояния информационной безопасности элементов киберфизических систем, построением модели классификации на основе ансамбля параллельно работающих классификаторов и постобработкой результатов при помощи весовых коэффициентов Фишберна, что позволяет увеличить точность оценивания защищённости киберфизических систем от информационных угроз.

Автореферат корректно отражает содержание диссертации. В нем изложены основные научные положения, результаты, выводы и рекомендации, полученные соискателем в рамках выполнения диссертационной работы.

5. Теоретическая и практическая значимость

Теоретическая значимость результатов диссертационной работы состоит в возможности дальнейшего развития теоретических выкладок и разработанного научно-методического аппарата в области обеспечения информационной безопасности КФС, а также для повышения гибкости и эффективности систем аудита и оценивания защищённости киберфизических систем от информационных угроз.

Практическая значимость работы заключается в повышении оперативности, точности и полноты оценивания защищённости ИБ КФС, что позволяет на практике эффективно применять разработанный подход в системах мониторинга событий информационной безопасности. Результаты диссертационной работы могут быть на практике внедрены при разработке и использовании систем мониторинга информационной безопасности на предприятиях, таких как ГУП «Водоканал Санкт-Петербурга», АО «НПК «Тристан», ПАО «Газпром нефть», АО «НИИ ТМ»; при проведении НИР в учреждениях науки РФ, таких как ФГБУН «СПб ФИЦ РАН», ФГУ «ФИЦ ИУ РАН» и других; в образовательном процессе ФГАОУ ВО «НИУ ИТМО» при подготовке бакалавров по направлению 10.03.01 и магистров по направлению 10.04.01 «Информационная безопасность», ФГАОУ ВО

«ГУАП» при подготовке специалистов по направлению 10.05.03 «Информационная безопасность автоматизированных систем».

Теоретическая и практическая значимость полученных автором результатов подтверждается большим числом публикаций в ведущих мировых рецензируемых изданиях, 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», свидетельством о регистрации программного обеспечения для ЭВМ, актами о внедрении и реализации результатов диссертационного исследования в научном учреждении и коммерческой организации.

6. Замечания по диссертационной работе

Отмечая достаточный научный и прикладной уровень рецензируемой работы, можно выделить следующие замечания и рекомендации:

1. В рамках диссертационного исследования делается акцент на ускорение обработки многомерных данных. Однако необходимо проводить дополнительные исследования для анализа влияния длительности обработки на время принятия управленческого решения, осуществляющего проактивные меры по поддержанию работоспособного состояния и информационной безопасности КФС в условиях деструктивных воздействий.
2. Требует пояснения возможность установки некоторых универсальных пороговых значений количества главных компонент, при которых вычисляется информативность признаков.
3. При рассмотрении предложений, связанных с использованием полученных результатов в системах мониторинга событий информационной безопасности КФС, недостаточно проработан вопрос возможной подделки значений, параметров, описывающих состояние ИБ, хотя это является важным для корректного функционирования средств мониторинга.
4. В исследовании слабо освещена оценка затрат вычислительных ресурсов при использовании предлагаемых подходов.
5. Недостаточно подробно описаны ограничения разработанной автором методики идентификации состояния ИБ КФС. Повышение ряда показателей полноты и точности идентификации может приводить к лавинообразному росту объема обрабатываемой информации, что вызывает необходимость описания ограничений, накладываемых на предлагаемые решения.
6. Неясно, чем обусловлен выбор алгоритма классификации в рамках метода оценивания состояния ИБ элементов КФС. Было бы целесообразно представить в диссертационной работе результаты анализа применения других алгоритмов машинного обучения.

Отмеченные недостатки носят непринципиальный характер и, в целом, не меняют положительной оценки диссертационной работы.

7. Заключение

Диссертационная работа, выполненная автором самостоятельно на высоком научно-техническом уровне, представляет законченный научно-исследовательский труд, содержащий решение актуальной научной задачи повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов, обладает научной новизной и практической значимостью. Работа базируется на достоверной и достаточно полной статистической информации, полученной автором.

Диссертационная работа Семенова Виктора Викторовича «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» полностью соответствует требованиям пп. 9–14 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 года № 842 (в редакции Постановления Правительства РФ от 11.09.2021 года № 1539), предъявляемым к кандидатским диссертациям.

Считаю, что Семенов Виктор Викторович заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
доктор технических наук, профессор, начальник кафедры специальных информационных технологий Федерального государственного казенного образовательного учреждения высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»

«14» апреля 2022 г. Примакин Алексей Иванович

Сведения о составителе отзыва:
ФИО: Примакин Алексей Иванович
Учёная степень: доктор технических наук
Учёное звание: профессор
Место работы: Федеральное государственное казенное образовательное учреждения высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»
Должность: начальник кафедры специальных информационных технологий
Почтовый адрес: 198206, г. Санкт-Петербург, ул. Лётчика Пилютова, 1
Телефон: +7 (812) 744-70-00
Эл. почта: a.primakin@mail.ru