ОТЗЫВ

на автореферат диссертационной работы **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 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Управление инцидентами информационной безопасности, включая их выявление, фиксацию, предсказание – это постоянный сложный процесс наблюдения и анализа результатов событий информационной безопасности и иных данных. Мониторинг информационной безопасности (ИБ) киберфизических систем представляет собой комплексную задачу по работе с угрозами и нарушениями ИБ, а также технологическими сбоями и отказами, осложнёнными разнородностью промышленных сетевых устройств и протоколов, количеством данных, скоростью их поступления. Дополнительную проблему предоставляет необходимость адаптации средств мониторинга в динамически меняющихся условиях. В этих условиях научная задача разработки методов повышения полноты и точности оценивания защищённости киберфизических систем от информационных угроз, решение которой содержится в представленной диссертационной работе, является актуальной.

Научную новизну диссертационного исследования обеспечивают разработанные соискателем:

1. Модель формирования признакового описания состояния информационной безопасности элементов киберфизических систем, отличающаяся от известных применением анализа главных компонент для вычисления информативности признаков.
2. Метод оценивания состояния ИБ элементов киберфизических систем, 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.

3. Методика идентификации состояния ИБ киберфизических систем, позволяющая достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ киберфизических систем, отличающаяся от существующих применением разработанных модели и метода и позволяет повысить скорость идентификации состояния ИБ элементов киберфизических систем 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.

Теоретическая и практическая значимость исследования заключается в разработанной методике идентификации состояния ИБ киберфизических систем, в созданной модели формирования оригинального признакового описания состояния ИБ, а также в возможности практического использования и универсальной применимости предлагаемого подхода для устройств киберфизических систем различной архитектуры.

Достоверность полученных автором научных результатов подтверждается правильно поставленной целью исследования, системным подходом при формулировке частных задач, корректным применением научных методов исследования, совпадением теоретических результатов с результатами математического моделирования, а также представлением результатов на научных конференциях и их публикацией в рецензируемых изданиях.

Согласно автореферату, полученные основные научные результаты диссертационной работы прошли достаточную апробацию использовались в научно-исследовательских и опытно-конструкторских работах в организациях. Представленные в автореферате положения являются обоснованными, указанные результаты апробированы на 10 международных и всероссийских конференциях, а также представлены в 29 публикациях. В то же время по работе можно сделать следующие замечания:

1. 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;

2. недостаточно акцентировано внимание на преимуществах метода на основе деревьев решений, повлекшего его выбор для решения обозначенных в диссертационном исследовании задач.

Отмеченные недостатки не снижают общей положительной оценки изложенных в автореферате результатов. Диссертационная работа Семенова В.В. представлена как завершённое и самостоятельное научное исследование, соответствующее требованиям пп. 9–14 «Положения о присуждении ученых степеней», утв. Постановлением Правительства РФ от 24.09.2013 г. № 842 (в ред. Постановления Правительства РФ от 11.09.2021 г. № 1539), предъявляемым к кандидатским диссертациям. Соискатель Семенов Виктор Викторович заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Доктор физико-математических наук
профессор кафедры информационных систем в экономике
Санкт-Петербургского государственного университета

14 апреля 2022 г. ЮРКОВ А.В.

Сведения о составителе отзыва:
Фамилия, имя, отчество: Юрков Александр Васильевич
Учёная степень: доктор физико-математических наук
Учёное звание: старший научный сотрудник
Место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет»
Должность: профессор кафедры информационных систем в экономике
Почтовый адрес: 191123, г. Санкт-Петербург, ул. Чайковского, д. 62, лит. А
Телефон: +7 (812) 363-67-78
E-mail: a.v.yurkov@spbu.ru