ОТЗЫВ

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

На современном этапе развития киберфизических систем (КФС) отмечается повышение степени интеллектуальности систем управления, их автономности и адаптивности, вместе с этим стремительно возрастает объем обрабатываемой информации, передаваемой от различных сенсоров. Данные системы являются сложными и распределенными, что также ведет возникновению ряда проблем, связанных с их работоспособностью и информационной безопасностью (ИБ). Необходимо обеспечение постоянного мониторинга состояния КФС, в том числе оценки защищённости, крайне важным является учет временных параметров. Существующие методы и технологии обеспечения ИБ в большей мере ориентированы на классические компьютерные или информационные системы, что ограничивает возможность их применения в КФС. Применяемые на сегодняшний день решения также не обладают достаточным функционалом, обеспечивающим эффективный мониторинг в режиме реального времени, что вызывает ряд проблем обеспечения ИБ, связанных с анализом состояния отдельных устройств КФС. Возникает объективная необходимость развития и адаптации методов математического обеспечения специализированных информационных систем, интегрируемых в КФС, в целях противодействия внешним и внутренним деструктивным воздействиям.

В связи с вышеизложенным тема диссертации «Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов» является **актуальной**, а поставленная в диссертационной работе **цель**, а именно повышение полноты и точности обнаружения нарушений информационной безопасности киберфизических систем, **имеет как теоретическую, так и практическую значимость**.

Научную новизну диссертационной работы составляют:

1. Модель формирования признакового описания состояния ИБ элементов КФС. Отличается от известных применением метода анализа главных компонент для вычисления информативности признаков и выделения списка параметров, характеризующих состояние ИБ отдельных элементов КФС.
2. Метод оценивания состояния ИБ элементов КФС. Отличается от существующих комбинированным подходом, сочетающим применение в системе управления событиями ИБ ансамбля параллельно работающих классификаторов на основе деревьев решений и весовых коэффициентов Фишберна при анализе совокупности информативных признаков, полученных из временных рядов, характеризующих функционирование КФС.

3. Методика идентификации состояния ИБ КФС. Отличается от существующих применением разработанных модели и метода и позволяет достичь заданной точности, сократив при этом временные затраты на обработку многомерных данных, поступающих от систем мониторинга ИБ КФС, за счёт уменьшения размерности обрабатываемых данных и идентификации состояния ИБ на основе решающего правила, учитывающего значения временных рядов, полученные за предшествующие моменты времени.

Практическую значимость результатов диссертационной работы составляют модель, метод и методика, которые служат для мониторинга состояния КФС, находящихся под воздействием информационных угроз, восстановления хода распространения инцидента ИБ и выработки защитных мер. Позволяют повысить качество (точность, полноту) идентификации состояния ИБ КФС и идентификации атак различных типов на КФС и её отдельные элементы. Разработанные подходы могут быть применены в системах мониторинга событий информационной безопасности КФС.

Личное участие автора. Согласно информации, представленной в автореферате, результаты по положениям, выносимым на защиту, получены автором самостоятельно. Автором разработана и зарегистрирована в установленном порядке программа для определения состояния информационной безопасности отдельных компонентов вычислительных систем, реализующая оценивание защищённости КФС от информационных угроз на основе анализа временных рядов. Имеется свидетельство о государственной регистрации программы для ЭВМ.

Обоснованность и достоверность результатов диссертационной работы подтверждается результатами вычислительных экспериментов, их сравнением с результатами других исследователей, практической реализацией и внедрением разработанной методики, апробацией основных положений диссертации на научно-технических конференциях, публикациями в рецензируемых журналах.

В целом автореферат изложен достаточно четко и последовательно, написан на понятном научном языке. В нем достаточно полно отражены цели и задачи диссертационного исследования, положения, выносимые на защиту, основные результаты и практическая значимость.

Замечания по автореферату:

1. Недостаточно подробное описание метода оценивания состояния информационной безопасности элементов киберфизических систем.
2. Неточности и неаккуратность в использовании понятий, а именно:

a. В описании практической значимости работы указано, что разработанные подходы позволяют повысить оперативность оценивания защищённости ИБ КФС. Не дано определение понятию «оперативность». В описании четвертой главы приведены результаты экспериментов по оценке временных затрат на обработку данных мониторинга состояния ИБ, экспериментов по именно по оценке оперативности не представлено. Из общепринятого определения понятия оперативности, как способности правильно и быстро осуществлять те или иные практические задачи, можно предположить, что здесь под оперативностью подразумевается,

сокращение временных затрат на обработку данных мониторинга при условии обеспечения необходимого значения показателей качества (полноты и точности) идентификации состояний ИБ КФС. Эксперименты по оценке указанных показателей приведены.

b. Целью работы заявлено повышение полноты и точности обнаружения нарушений ИБ КФС, но в автореферате, в описании четвертой главы, представлены эксперименты по оценке качества идентификации состояния ИБ КФС и идентификации атак различных типов на КФС и её отдельные элементы. Однако, из текста автореферата можно сделать выводы, что обнаружение (выявление) нарушений ИБ КФС сводится к решению задачи идентификации состояния ИБ КФС и идентификации атак различных типов; и что понятия «обнаружение нарушений ИБ КФС» и «идентификация состояния ИБ КФС» в автореферате синонимичны.

3. Имеются некоторые иные стилистические неточности в тексте автореферата.

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

Таким образом, представленная диссертация соответствует требованиям пунктов 9–14 «Положения о присуждении ученых степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 г. № 842 (в действующей редакции от 11.09.2021 г.), предъявляемым к кандидатским диссертациям, обладает научной новизной и практической значимостью. Диссертация Семенова Виктора Викторовича является законченной и самостоятельной научно-квалификационной работой, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Доцент Факультета БИТ,
кандидат технических наук, доцент
«28» апреля 2022 г. Воробьева Алиса Андреевна

Сведения о составителе отзыва:
Фамилия, имя, отчество: Воробьева Алиса Андреевна
Учёная степень: кандидат технических наук
Ученое звание: доцент
Должность: доцент (квалификационная категория "ординарный доцент")
Наименование организации: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»
Адрес: 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А
Телефон: +7 (812) 312-32-69
E-mail: vorobeva@itmo.ru