ОТЗЫВ

на автореферат диссертации Шамсутдинова Рината Рустемовича «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем», представленной на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

В настоящее время все большее число промышленных систем подключается к сетям общего доступа в рамках концепции промышленного Интернета вещей, что, с одной стороны, дает предприятиям ряд преимуществ (упрощается взаимодействие с внешней средой – поставщиками, разработчиками и вендорами ПО, используются стандартные протоколы обработки и передачи информации на всех уровнях управления и т.д.), но, с другой стороны, возрастает количество уязвимостей и потенциальных угроз безопасности информации. Устройства промышленного Интернета вещей не являются в достаточной степени защищенными, а существующие системы обеспечения информационной безопасности (ИБ) не учитывают в полной мере специфику построения и функционирования систем и сетей промышленного Интернета вещей.

В последние годы значительно возрос интерес ученых и специалистов к новому направлению, связанному с разработкой и применением методов, алгоритмов и инструментальных средств обнаружения сетевых атак и аномалий промышленного Интернета вещей на основе методологии гибридных интеллектуальных систем, объединяющих в своем составе адаптивные механизмы искусственных иммунных систем и методы машинного обучения. Как показывают исследования, подобный подход позволяет обеспечить высокие показатели эффективности обнаружения сетевых атак, в том числе ранее неизвестных системе, и значительно снизить уровень принимаемых ошибочных решений. В связи с этим, тема представленной диссертационной работы Шамсутдинова Р.Р., творчески развивающей указанное выше направление исследований, безусловно, является актуальной и практически востребованной.

К основным результатам работы, обладающим научной новизной, можно отнести предложенные в работе:

– алгоритмы обнаружения атак и аномалий сетевого трафика промышленного Интернета вещей в составе двухуровневой искусственной иммунной системы, отличающиеся интеграцией различных подходов в рамках

теории искусственных иммунных систем и модификацией известных алгоритмов клональной селекции, дендритных клеток и обновления детекторов;

– алгоритмы обнаружения атак и аномалий сетевого трафика промышленного Интернета вещей в составе гибридной распределенной интеллектуальной системы мониторинга (РИСМ) ИБ, отличающиеся формированием специфического иммунного ответа искусственной иммунной системы совместно с ансамблем других методов машинного обучения (искусственная нейронная сеть, алгоритм случайного леса) и подсистемой корреляции событий ИБ, что обеспечивает дифференцированный подход к обнаружению различных типов сетевых атак и аномалий и позволяет повысить эффективность функционирования системы мониторинга ИБ в целом.

Обоснованность, достоверность и практическая ценность результатов исследований подтверждается результатами проведенных вычислительных экспериментов и решения ряда практических прикладных задач с использованием разработанных алгоритмов и инструментальных средств. Полученные результаты неоднократно обсуждались на представительных российских и международных конференциях, по материалам исследований опубликовано 17 работ, в том числе 6 – в рецензируемых научных изданиях из Перечня ВАК.

В качестве замечаний по тексту автореферата можно отметить следующие:

– не указано, каким образом в подсистеме дендритных клеток осуществляется анализ уровня опасности;

– неясно, что из себя представляют агенты первого и второго уровней искусственной иммунной системы, реализуются ли они в составе программного обеспечения, устанавливаемого на уже существующие на объекте защиты устройства Интернета вещей или же они требуют отдельного аппаратного обеспечения.

Приведённые замечания, однако, не являются принципиальными и не снижают общей высокой оценки уровня научной работы, теоретической и практической значимости полученных в ней результатов. Тема диссертационного исследования полностью соответствует научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертационная работа в целом соответствует требованиям п. 9 Положения ВАК о порядке присуждению ученых степеней, а её автор, Шамсутдинов Ринат Рустемович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Доцент кафедры безопасности
информационных технологий
ФГАОУ ВО «Южный федеральный университет»,
кандидат технических наук, с. н. с., доцент

Брюхомицкий Юрий Анатольевич

Кандидатская диссертация защищена по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Даю согласие на обработку персональных данных.

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»
Адрес: 347928, г. Таганрог, ул. Чехова 2, кафедра безопасности информационных технологий, к. И-411.
Телефон: +7 (8634) 37-19-05
E-mail: bryuhomitskiy@sfedu.ru

ПОДПИСЬ Брюхомицкого Ю.А.
ЗАВЕРЯЮ,
ДИРЕКТОР ИНСТИТУТА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТА ЮФУ
Г.Е. ВЕСЕЛОВ
08 2024 г.