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

Высокие темпы роста рынка промышленного интернета вещей (IIoT), говорят не только о возможности повышения производительности и трансформации целых отраслей с целью улучшения качества продукции, но и возникновении новых вызовов в области информационной безопасности. Злоумышленники могут использовать слабые места и уязвимости в системе IIoT для проведения кибератак на промышленные объекты, что может иметь серьезные последствия в виде остановки производства, потери данных и повреждения физической инфраструктуры.

В этой связи, тема диссертационного исследования Шамсутдинова Рината Рустемовича, безусловно актуальна, так как интеллектуальная система мониторинга информационной безопасности IIoT может обеспечить обнаружение аномалий, предотвращение и обнаружение кибератак, а также принимать решения на основе адаптивности и самообучения. В целом, актуальность этой темы обусловлена необходимостью обеспечения безопасности в IIoT, подверженному все возрастающему количеству угроз и с учетом значимости промышленных объектов, которые могут быть под угрозой в случае успешной кибератаки.

В части научной новизны полученных результатов, необходимо отметить следующие:

- предложена концепция построения интеллектуальной системы мониторинга информационной безопасности (ИБ) промышленного Интернета вещей на основе многоагентной платформы гибридной многоуровневой интеллектуальной системы обнаружения атак и аномалий сетевого трафика IIoT, отличающаяся интеграцией механизмов искусственных иммунных систем, методов машинного обучения, подсистемы корреляции событий информационной безопасности (SIEM-системы), что позволяет повысить полноту и точность выявления внешних и внутренних угроз безопасности информации;

- разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе адаптивных механизмов искусственных иммунных систем (ИИС), отличающиеся интеграцией различных подходов в рамках теории ИИС (негативная селекция, клональный отбор, теория опасности, теория иммунной сети) и модификации известных алгоритмов клональной селекции, дендритных клеток и обновления детекторов, что позволяет в совокупности существенно снизить уровень принятия ошибочных решений, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации Научная новизна полученных результатов;

- предложена концепция построения интеллектуальной системы мониторинга информационной безопасности (ИБ) промышленного Интернета вещей на основе многоагентной платформы гибридной многоуровневой интеллектуальной системы обнаружения атак и аномалий сетевого трафика IIoT, отличающаяся интеграцией механизмов искусственных иммунных систем, методов машинного обучения, подсистемы корреляции событий информационной безопасности (SIEM-системы), что позволяет повысить полноту и точность выявления внешних и внутренних угроз безопасности информации;

- разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе адаптивных механизмов искусственных иммунных систем (ИИС), отличающиеся интеграцией различных подходов в рамках теории ИИС (негативная селекция, клональный отбор, теория опасности, теория иммунной сети) и модификации известных алгоритмов клональной селекции, дендритных клеток и обновления детекторов, что позволяет в совокупности существенно снизить уровень принятия ошибочных решений, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации;

- разработана архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей на основе комитета классификаторов, отличающаяся использованием многоагентного подхода к построению многоуровневых распределенных гибридных интеллектуальных систем, что позволяет более полно использовать преимущества применения различных технологий интеллектуального анализа данных, учесть особенности структурно-функциональной организации (состава подсистем) объекта мониторинга, многообразие угроз безопасности информации и уязвимостей программного обеспечения, дополняя полученную информацию текущими данными от взаимодействующей SIEM-системы.

Теоретическая значимость полученных результатов состоит в развитии методов обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе использованием ансамбля методов машинного обучения и подсистемы корреляции событий ИБ.

Практическая значимость полученных результатов заключается в разработке программных модулей исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей, а также методики ее применения для обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей.

Замечания

1. Несмотря на высокую точность и устойчивость к шуму комитет (ансамбль) классификаторов (КК) всё же имеет ряд недостатков, которые, впрочем, в ряде случаев, удаётся нивелировать за счёт настроек КК. В этой связи, хотелось бы видеть в тексте автореферата сведения о вычислительной сложности, затратах на обучение и чувствительности к переобучению при использовании КК.

2. В целях лучшей интерпретации результатов, желательно в тексте автореферата было бы привести не только количественные данные по метрикам качества обучения, но и графическую интерпретацию, например матрицы ошибок.

В целом, указанные замечания не снижают высокой научной ценности и практической значимости выполненного исследования.

Диссертация Шамсутдинова Рината Рустемовича является законченной научно-квалификационной работой и удовлетворяет требованиям п. 9 «Положения ВАК о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор – Шамсутдинов Р.Р., заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность.

Доктор технических наук, профессор, заведующий кафедрой систем информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»)

Остапенко Александр Григорьевич

Докторская диссертация защищена по специальности 05.09.05 – «Теоретическая электротехника»

Даю согласие на обработку персональных данных.

Подпись профессора Остапенко А.Г. заверяю

Адрес места основной работы: Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»), 394026, Воронеж, Московский проспект, 14, тел. 2523420, email: sub316@mail.ru

Доктор технических наук, доцент, профессор кафедры систем информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»)

Разинкин Константин Александрович

Докторская диссертация защищена по специальности 05.13.01 - Системный анализ, управление и обработка информации

Даю согласие на обработку персональных данных.

Подпись профессора Разинкина К.А. заверяю

Адрес места основной работы: Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»), 394026, Воронеж, Московский проспект, 14, тел. 2523420, email: kostyr@mail.ru