

## ОТЗЫВ

на автореферат диссертации **Коржук Викторией Михайловны** «**Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа**», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Стремительный рост интереса к автоматизированным системам управления, в том числе киберфизическим системам, приводит к развитию технологий беспроводных сетей, в том числе беспроводных сенсорных сетей. Беспроводные сенсорные сети, состоящие из множества датчиков, обладают возможностью самоорганизации и могут включать в себя несколько тысяч различных устройств. Открытый канал связи, относительно невысокая скорость передачи данных и разнообразие систем, в которых используются беспроводные сенсорные сети, делают их привлекательными для злоумышленников. Обладая программно-аппаратными средствами, разработанными для тестирования состояния сети, злоумышленник имеет возможность перехватывать данные, пересылаемые в беспроводной среде передачи данных. В связи с этим, возрастает необходимость своевременного обнаружения и предотвращения подобных инцидентов. Используемые методы и средства должны учитывать особенности беспроводных сенсорных сетей, которые не позволяют использовать существующие средства защиты на должном уровне. В контексте всего вышесказанного, работа Коржук В.М. является актуальной, так как направлена на обнаружение атак сетевого уровня в беспроводных сенсорных сетях и учитывает упомянутые ограничения.

Соискать успешно решила задачу повышения эффективности идентификации атак благодаря разработке нового теоретически обоснованного набора характеристик сети, использованию оптимальных алгоритмов машинного обучения для классификации поведения сети и разработке комплексной методики, позволяющей использовать программные средства, созданные в процессе исследования, и осуществлять более гибкую настройку системы идентификации атак. Необходимо отметить такое достоинство работы Коржук В.М. как использование вычислительного эксперимента, для моделирования атак на беспроводные сенсорные сети.

Работа обладает теоретической и практической значимостью, так как предложенные результаты могут быть использованы в качестве базиса для

дальнейшего развития научной области и как составляющие элементы для разработки и модификации систем обнаружения вторжений и атак.

К автореферату могут быть предъявлены следующие замечания:

- 1) В тексте автореферата упоминается тестирование различных алгоритмов машинного обучения для идентификации атак, однако не представлены результаты сравнения и обоснование выбора случайного леса.
- 2) Не вполне ясно, учитывается ли при оценке эффективности такой показатель, как вычислительная сложность алгоритма.

Несмотря на отмеченные замечания, диссертация Коржук Виктории Михайловны «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» является законченной научно-квалификационной работой; выполнена в соответствии пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 01.10.2018). Считаю, что соискатель В.М. Коржук заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

ООО «Газинформсервис»

Начальник Отдела Технологии Анализа

к.т.н.

Большаков А.А.

Руководитель Службы  Управления Персоналом

Сапогова М.Н.

Дата: 20 декабря 2019

Адрес: Кронштадтская ул., 10,  Санкт-Петербург, 198096

Тел.: 8 (812) 677-20-50

Сведения о составителе отзыва:

Большаков Анатолий Афанасьевич, к.т.н.

Должность: начальник Отдела Технологии Анализа

Место работы: ООО «Газинформсервис»

Адрес: 198096, Санкт-Петербург, Кронштадская ул., д.10

Тел: (812) 677-20-50

e-mail: resp@gaz-is.ru