# Отзыв

официального оппонента Красова Андрея Владимировича
на диссертацию Коржук Виктории 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»

## I Актуальность темы диссертационной работы

Обеспечение информационной безопасности беспроводных сетей в настоящие дни является актуальной задачей, поскольку соответственно развитию технологий и методов защиты развиваются алгоритмы, способы и методы съема, перехвата, анализа и подмены данных. В свою очередь, беспроводные сенсорные сети набирают популярность в связи с развитием таких концепций, как «киберфизические системы», «Индустрия 4.0», «Умный дом» и «Интернет вещей». В таких системах критически важна отказоустойчивость, и, следовательно, доступность и целостность информации внутри сети. Системы на основе беспроводных сенсорных сетей наиболее подвержены атакам маршрутизации, то есть наиболее уязвимыми являются сетевой и транспортный уровень передачи.

Актуальность диссертационной работы заключается в том, что стандартные методы обеспечения информационной безопасности не являются достаточными в силу различных ограничений, связанных с техническими характеристиками устройств беспроводных сенсорных сетей. Для идентификации атак в беспроводных сетях используются: сигнатурный анализ, который предполагает наличие большого объема хранимых данных и попарное сравнение; глубокая инспекция пакетов и методы, основанные на доверии, которые предполагают дополнительные мощности для принятия решений. В своей работе Коржук В.М. предлагает использовать для идентификации атак на беспроводные сенсорные сети автоматизированный анализ поведения сети, под которым понимается анализ совокупности признаков поведения, накапливаемой со временем, и разрабатывает соответствующий новый научно-методический аппарат.

В процессе проведения исследования и решения поставленной научной задачи соискатель получила следующие научные результаты:

1) модель профиля поведения беспроводной сенсорной сети;

2) метод идентификации атак на сетевой уровень беспроводных сенсорных сетей на основе анализа поведения;

3) методика идентификации атак на сетевой уровень беспроводных сенсорных сетей.

## II Структура диссертационной работы

Диссертация включает введение, 3 главы и заключение.

Во введении представлена краткая характеристика работы, обоснована ее актуальность, новизна, теоретическая и практическая значимость. Приведены цель, задачи, предмет, объект исследования, основные положения и результаты, перечислены публикации.

В первой главе представлен анализ текущего состояния предметной области, выделены особенности обеспечения информационной безопасности в беспроводных сенсорных сетях, сформированы соответствующие допущения и ограничения работы. Выделено множество исследуемых атак и сформулирован комплексный показатель эффективности идентификации. Формализована научная задача.

Вторая глава содержит разработанную модель профиля поведения беспроводной сенсорной сети и метод идентификации атак сетевого уровня. Описан процесс выбора характеристик сети, оценка их информативности и формирование набора данных. Осуществлено тестирование нескольких алгоритмов классификации, сделано предположение о возможности успешной идентификации на сокращенном наборе характеристик сети. Обосновано применение вероятностного классификатора и введения параметра степени уверенности. Предложен метод на основе комбинированного использования разработанной модели поведения, случайного леса и вероятностного классификатора. Описаны соответствующие эксперименты.

Третья глава описывает методику идентификации атак, включающую в себя модель, метод и разработанные в ходе исследования вспомогательные компьютерные программы. Представлены результаты дополнительных экспериментов при изменения параметров сети и параметров метода

идентификации. Осуществлена оценка полученных результатов с результатами других авторов, предложены практические рекомендации по дальнейшему использованию и развитию результатов работы.

В заключении сформулированы результаты и итоги исследования.

## III Научная новизна результатов диссертационной работы

1) Разработана модель профиля поведения беспроводной сенсорной сети на основе новой комбинации поведенческих признаков. Модель, в отличие от существующих, характеризуется комплексным подходом к формированию вектора признаков и применением совокупности методов оценки информативности признаков поведения сети. Представленная модель позволяет идентифицировать нормальное поведение сети и 14 атак различного типа.

2) Разработан метод идентификации атак на беспроводные сенсорные сети на основе совместного применения «случайного леса» и вероятностного классификатора. Метод отличается от существующих использованием модели профиля поведения сети и возможностью установки необходимого уровня точности и позволяет сократить необходимое для успешной идентификации атак количество признаков при сохранении достаточной точности.

3) Разработана методика идентификации атак на основе анализа поведения сети. Методика включает в себя разработанные модель и метод, отличается от существующих возможностью предварительного моделирования поведения защищаемой сети с помощью программной модели проведения атак, автоматизацией процесса оценки информативности и расчета вероятностных показателей. Использование методики позволяет повысить эффективность идентификации, при этом под эффективностью понимается совокупность таких показателей, как точность и полнота идентификации, количество идентифицируемых атак и количество идентификационных признаков.

## IV Теоретическая и практическая значимость

Теоретическая и практическая значимость результатов работы заключается в развитии методов и систем защиты информации, методов обработки информации применительно к системам обеспечения безопасности сетей.

Использование разработанных модели, метода и методики позволит повысить эффективность работы систем обнаружения вторжений за счет использования для анализа неполного набора признаков поведения и комбинации алгоритмов машинного обучения. Предложенный научно-методический аппарат может быть использован для идентификации атак и для более общих задач, связанных с классификацией векторов признаков объектов.

## V Степень обоснованности и достоверности

Обоснованность и достоверность полученных результатов достигнута за счет применения соответствующего поставленной задаче математического аппарата, формированием адекватных допущений и ограничений работы, использованием моделирования и практических экспериментов, а также сравнением полученных в процессе исследования результатов с аналогичными работами других авторов и их непротиворечивостью. Также, обоснованность и достоверность определяется практической апробацией результатов в различных научно-исследовательских проектах и учебных дисциплинах. Научные результаты работы опубликованы в 17 печатных работах, в т.ч. в 3 статьях в журналах, рецензируемых ВАК РФ, и апробированы на различных российских и международных конференциях, таких как FRUCT, RuSMART, ИБРР и пр. Кроме того, соискателем выигран грант комитета по науке и высшей школе правительства Санкт-Петербурга.

## VI Оценка содержания и степени завершенности диссертации

Диссертация соискателя обладает внутренним единством, содержит новые научные положения и результаты и представляет собой завершенный научный квалификационный труд. Диссертация состоит из 206 страниц, в т.ч. 184 страниц основного материала, и включает в себя и включает введение, три главы, заключение, список сокращений, список литературы из 221 источника и пять приложений. Стиль изложения логичный, последовательный. Присутствует достаточное количество иллюстративного материала. Проведен анализ исследуемой области, предложены в достаточной степени аргументированные и адекватные решения, получены непротиворечивые результаты.

Автореферат соответствует содержанию диссертационной работы, научная новизна, результаты и выводы представлены корректно и логично. Автореферат оформлен в соответствии с требованиями Положения о присуждении научных степеней.

**VII Недостатки диссертации**

1) В тексте диссертации не представлена информация о том, как происходит выявление аномального поведения сети и сетевых устройств и как принимается решение о том, что необходимо начинать процесс идентификации. В таких случаях допустимо определение пороговых значений признаков поведения, превышение которых подразумевает под собой вмешательство нарушителя и, соответственно, может служить сигналом к запуску процесса идентификации атак.

2) Во второй главе при описании процесса сокращения признакового пространства на основе оценки информативности представлено формализованное описание метода Шеннона и метода Кульбака, однако также используемый метод накопленных частот представлен только в вербальном виде. Для унифицированного представления информации в диссертации представляется целесообразным иметь формализованное математическое описание для всех используемых методов.

3) При описании разработки метода идентификации недостаточно ясно обоснована необходимость применения более чем одного классификатора. Необходимы уточнить, как влияет увеличение количества классификаторов на эффективность идентификации. Например, вероятно, совместное использование нескольких классификаторов позволит снизить общее количество ошибок I и II рода.

Следует отметить, что выявленные замечания не влияют значительно на полученные результаты не снижают в целом положительную оценку диссертационной работы.

**VIII Вывод**

Диссертационная работа Коржук В.М. «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» представляет собой законченную научно-квалификационную работу, в которой решена актуальная задача разработки научно-методического аппарата по идентификации атак на беспроводные сенсорные сети. Работа соответствует паспорту специальности 05.13.19 и требованиям пунктов п. 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года № 842 в редакции от 01.10.2018, предъявляемым к кандидатским диссертациям. Считаю, что Коржук Виктория Михайловна заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Официальный оппонент:
кандидат технических наук, доцент
заведующий кафедрой Защищенных систем связи
ФГБОУ ВО Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича

Красов Андрей Владимирович

«6» 12 2019 г.

Подпись А.В. Красова
ЗАВЕРЯЮ
Начальник административно-кадрового
«6» 12

**Сведения о составителе отзыва**
ФИО: Красов Андрей Владимирович
Ученая степень: кандидат технических наук
Ученое звание: доцент
Место работы: Федеральное государственное бюджетное
учреждение высшего образования Санкт-Петербургский
университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Должность: заведующий кафедрой Защищенных систем связи
Почтовый адрес: 191040, Санкт-Петербург, ул. Пушкинская д.6, кв. 43
Телефон: +7 921 999 03 14
Эл. почта: krasov@inbox.ru