ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01,
СОЗДАННОГО НА БАЗЕ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА
ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ
НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 26.12.2019 г. № 2

О присуждении Коржук Виктории Михайловне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 24 октября 2019 г., протокол заседания № 1, диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года (с изменениями согласно приказам Минобрнауки России №105/нк от 11 апреля 2012 г. №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г.).

Соискатель Коржук Виктория Михайловна, 1992 года рождения, в 2014 г. окончила федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» по специальности 090103 «Организация и технология защиты информации» (диплом № 107824 0104307), в 2019 г. окончила очную аспирантуру в федеральном государственном

автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО) по направлению подготовки 10.06.01 «Информационная безопасность». Диплом об окончании аспирантуры № 107824 4740980 выдан 08 июля 2019 года федеральным государственным автономным образовательным учреждением высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО). В настоящее время Коржук Виктория Михайловна работает ассистентом на факультете безопасности информационных технологий в федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский университет ИТМО» Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена на факультете безопасности информационных технологий федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО) Министерства науки и высшего образования Российской Федерации.

Научный руководитель – кандидат технических наук, доцент ЗАКОЛДАЕВ Данил Анатольевич, основное место работы: федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО), декан факультета безопасности информационных технологий.

Официальные оппоненты:

СУХАНОВ Андрей Вячеславович – доктор технических наук, доцент, советник генерального директора акционерного общества «Эврика»;

КРАСОВ Андрей Владимирович – кандидат технических наук, доцент, заведующий кафедрой Защищенных систем связи Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», –

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», г. Санкт-Петербург в своем положительном отзыве, подписанном Соколовым Сергеем Сергеевичем, д.т.н., доцентом, заведующим кафедрой комплексного обеспечения информационной безопасности ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», и утвержденном ректором д.т.н., профессором Барышниковым С.О., указала, что в целом диссертационная работа В.М. Коржук является самостоятельной научно-квалификационной работой, выполненной на актуальную тему и отличающейся научной новизной и практической значимостью. Автором решена важная научная задача по разработке научно-методического аппарата по идентификации атак на беспроводные сенсорные сети, позволяющая повысить эффективность идентификации и имеющая важное значение для развития цифровых технологий в области защиты информации в целом и систем обнаружения вторжений в частности. Полученные результаты могут быть применены в ЗАО «Перспективный мониторинг» (г. Москва), АО «Эврика» (г. Санкт-Петербург), ОАО «Инфотекс» (г. Санкт-Петербург), АО «Лаборатория Касперского» (г. Москва), ЗАО «Российские наукоемкие технологии» (г. Москва), а также при подготовке специалистов по информационной безопасности в высших учебных заведениях.

В рамках исследования соискателем разработана модель профиля поведения беспроводной сенсорной сети, отличающийся от известных новой комбинацией статистических признаков поведения сети; предложен метод идентификации атак сетевого уровня на беспроводную сенсорную сеть, основанный на совместном использовании алгоритма «случайный лес» и вероятностного классификатора и введением параметра степени уверенности; разработана методика идентификации атак на беспроводные сенсорные сети, в отличие от известных включающая в себя разработанные модель профиля поведения, метод идентификации атак, программную модель реализации атак, программу оценки информативности и программу вычисления апостериорных распределений дискретного параметра распределения многомерной случайной величины по статистической выборке. Текст автореферата полностью соответствует содержанию диссертации.

Диссертационное исследование «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» является научно-квалификационной работой и соответствует критериям, изложенным в пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Коржук Виктория Михайловна заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 17 опубликованных работ, все по теме диссертации, в том числе опубликованных в рецензируемых научных изданиях 11 работ, из них опубликованных в изданиях, рекомендуемых ВАК при Минобрнауки России – 3 работы, в базах данных Scopus и Web of Science – 8; получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Основные научные результаты опубликованы в 17 научных трудах общим объемом 5 п.л., в которых объем личного вклада – 1,15 п.л. Наиболее значимые работы по теме диссертации:

1. **Коржук В.М.,** Грозных А.В., Заколдаев Д.А. Введение параметра степени уверенности в процесс идентификации атак на киберфизические системы // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки». 2019. №10. С. 111-117. (Перечень ВАК). *Личный вклад соискателя – 62%.*
2. **Коржук В.М.,** Бонковски П. Идентификация атак на беспроводные сенсорные сети на основе анализа аномального поведения сети // Научно-технический вестник Поволжья. 2018. № 2. С. 83-85. (Перечень ВАК). *Личный вклад соискателя – 68%.*
3. **Коржук В.М.,** Сухопаров М.Е, Лебедев И.С., Кривцова И.Е., Печеркин С.А. Обеспечение информационной безопасности каналов связи на основе многофункционального специализированного программно-аппаратного решения // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 70-74. (Перечень ВАК). *Личный вклад соискателя – 20%.*
4. **Korzhuk V.,** Groznykh A., Menshikov A., Strecker M. Identification of Attacks against Wireless Sensor Networks Based on Behaviour Analysis // Journal of

Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2019. Vol. 10, No. 2, pp. 1-21. (База данных Scopus). *Личный вклад соискателя – 70%.*

5. **Korzhuk V.,** Shilov I., Krivtsova I. The Model of the Attack Implementation on Wireless Sensor Networks // Proceedings of the 20th Conference of Open Innovations Association FRUCT. 2017. pp. 187-194. (База данных Scopus). *Личный вклад соискателя – 38%.*

6. **Korzhuk V.,** Shilov I., Zikratov I., Gvozdev A. Formalization of the Feature Space for Detection of Attacks on Wireless Sensor Networks // Proceedings of the 20th Conference of Open Innovations Association FRUCT. 2017, pp. 526-533. (База данных Scopus). *Личный вклад соискателя – 38%.*

7. **Коржук В.М.** Об актуальности развития и обеспечения безопасности сети ZigBee // Материалы XIV Санкт-Петербургской международной конференции «Региональная информатика (РИ-2014)» – 2014. С. 568-569. (РИНЦ)

Оригинальность содержания диссертации составляет не менее 87% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) АО «Центральный ордена Трудового Красного Знамени научно-исследовательский и проектно-конструкторский институт морского флота». Отзыв составил заведующий отделом информационных технологий, к.в.н., доцент Юрин Игорь Валентинович. Замечания: Из автореферата неясно, на основании чего начинается процесс обнаружения атак: в предложенной методике (рис.3) присутствует блок «запуск процедуры идентификации», однако не описано, достижение каких пороговых значений признаков необходимы. Качество иллюстративного материала, а именно размер графиков (например, рис.2 и рис.4), не способствует облегчению восприятия материала.

2) ЧОУ ДПО «Учебный центр «СпецПроект». Отзыв составил старший научный сотрудник, д.т.н., профессор Швед Виктор Григорьевич. Замечания: При описании метода идентификации не приведена информация о количестве записей в наборе данных, о соотношении обучающей и тестовой выборок и о сбалансированности данных. В тексте автореферата упоминаются показатели эффективности идентификации, но не описано, какие это показатели и как присваиваются веса.

3) ЗАО «Перспективный мониторинг». Отзыв составил эксперт-исследователь, к.т.н. Чемёркин Юрий Сергеевич. Замечания: В автореферате перечислены компьютерные программы, разработанные в процессе исследования, однако не упоминается возможность создания комплексного программного продукта, представляющего собой самостоятельный блок системы обнаружения атак. У соискателя имеются индивидуальные публикации в нерецензруемых изданиях, выступления на конференциях и победы в грантах, однако все публикации ВАК и Scopus выполнены в соавторстве.

4) АО «Диаконт». Отзыв составил ведущий инженер, к.т.н. Сыров Александр Александрович. Замечания: В тексте автореферата приведен перечень анализируемых атак, однако отсутствует их описание и соответствующие изменения в используемых для идентификации признаков. В процесс идентификации введен показатель степени уверенности, однако не приведено его математическое выражение. В блок-схеме алгоритма обнаружения вторжений (рис.1) 9 блок вместо обновления параметра степени уверенности указано обновление степени уверенности.

5) ФГБУН Институт проблем транспорта им. Н.М. Соломенко РАН. Отзыв составил заместитель директора по научной работе д.т.н., доцент Комашинский В.И. Замечания: Отсутствие информации о динамике идентифицируемых атак. Недостаточная степень раскрытия комплексного понятия эффективности идентификации.

6) ООО «Газинформсервис». Отзыв составил начальник Отдела Технологии Анализа к.т.н. Большаков А.А. Замечания: В тексте автореферата упоминается тестирование различных алгоритмов машинного обучения для идентификации

атак, однако не представлены результаты сравнения и обоснование выбора случайного леса. Не вполне ясно, учитывается ли при оценке эффективности такой показатель, как вычислительная сложность алгоритма.

7) АО «Эшелон-СЗ». Отзыв составил заместитель начальника испытательной лаборатории Кашин С.В. Замечания: В автореферате используются понятия «поведение» и «поведенческий анализ», однако трактовка этих терминов в некоторой степени расплывчата. Как следует из автореферата, выбранные соискателем признаки характерны только для сети на протоколе ZigBee. Непонятно, будет ли эффективен разработанный научно-методический аппарат для других протоколов.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что

доктор технических наук, доцент Суханов Андрей Вячеславович является известным учёным в области защиты информации и обеспечения безопасности автоматизированных информационных сетей;

кандидат технических наук, доцент, Красов Андрей Владимирович – крупный специалист в области обеспечения безопасности в сетях передачи данных;

ведущая организация, Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», является известной как в России, так и за рубежом организацией в области разработки и исследований систем защиты информации, составляющей, в том числе, государственную тайну.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработан новый научно-методический аппарат по идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа новой комбинации признаков, характеризующих поведение такой сети;

предложены:

– модель профиля поведения беспроводной сенсорной сети, отличающаяся использованием новой комбинации признаков, характеризующих

функционирование сети, таких как общее количество пакетов, переданных в сети, максимальное количество отправленных узлом пакетов, максимальное и минимальное количество полученных узлом пакетов и соотношение между количеством созданных и полученных пакетов, позволяющая идентифицировать 14 типов различных атак сетевого уровня на беспроводные сенсорные сети;

– новый метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа комбинации признаков, отличающийся от существующих методов совместным применением алгоритма «случайный» лес и вероятностного классификатора, а также введением параметра степени уверенности, позволяющий обеспечить более высокую точность идентификации атак при использовании неполного набора признаков профиля поведения;

– методика идентификации атак на беспроводные сенсорные сети, отличающаяся от известных применением предложенный модели профиля поведения, метода идентификации атак на беспроводные сенсорные сети, а также использованием программной модели реализации атак на беспроводную сенсорную сеть, программы комплексной оценки информативности признаков поведения сети и программы расчета апостериорных распределений дискретного параметра распределений многомерной случайной величины по статистической выборке, позволяющая повысить эффективность идентификации атак и гибкость настройки системы обнаружения вторжений, в рамках которой потенциально используются полученные результаты;

– практические рекомендации по применению разработанного научно-методического аппарата, включающие в себя обоснование выбора величины параметра степени уверенности, перечень действий администратора сети для настройки и использования модели профиля поведения, метода и методики идентификации, а также рекомендации для проектирования мобильного программно-аппаратного узла обнаружения вторжений в беспроводную сенсорную сеть;

доказана:

– возможность идентификации атак сетевого уровня при условии сохранения

заданной точности на неполном наборе признаков поведения из модели профиля поведения беспроводной сенсорной сети;

– перспективность использования предложенного научно-методического аппарата для построения систем обнаружения вторжений и атак на беспроводные сенсорные сети на основе анализа поведения исследуемой сети;

введены:

– профиль поведения беспроводной сенсорной сети для различных типов атак, который характеризуется определенными величинами признаков поведения сети;

– требования к процессу обнаружения и идентификации атак на беспроводные сенсорные сети, связанные с ресурсными ограничениями узлов исследуемых сетей;

– параметр степени уверенности, являющийся субъективным параметром, отражающим заданную ожидаемую апостериорную вероятность определенной атаки;

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с использованием формальных математических доказательств и вычислительных экспериментов о применимости предложенных модели, метода и методики. Эти утверждения составляют основу процесса идентификации атак сетевого уровня на беспроводные сенсорные сети с целью обеспечения доступности и целостности информации, циркулирующей в сети;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы концепции, подходы и методы теории информации, положения теории вероятности, методы теории информационной безопасности и методологии защиты информации, методы математической статистики и вычислительного эксперимента.

изложены методологические и методические основы использования задачи вероятностной классификации для уменьшения количества идентификационных признаков при заданной точности идентификации;

раскрыты

– проблемные аспекты применения имеющихся подходов в области обеспечения информационной безопасности и обнаружения вторжений к беспроводным сенсорным сетям вследствие их технологических особенностей;

– основные вопросы, связанные с обнаружением атак сетевого уровня, при которых нарушается доступность и целостность информации, циркулирующей внутри беспроводной сенсорной сети;

– вопросы, связанные с универсальностью и практической применимостью предложенных метода и методики идентификации атак сетевого уровня при изменении параметров сети;

изучены существующие концепции, стандарты, технологии, модели и методы обнаружения и идентификации атак на компьютерные сети и беспроводные сенсорные сети в частности, при этом особое внимание уделено идентификации атак сетевого уровня на основе анализа поведения исследуемой сети; существующие методы интеллектуального анализа данных и особенности совместного применения различных алгоритмов машинного обучения в задачах многоклассовой классификации.

проведена модернизация существующих подходов к идентификации атак сетевого уровня на беспроводные сенсорные сети на основе разработки модели профиля поведения, метода и методики идентификации при использовании анализа характеристик поведения сети.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

– модель профиля поведения беспроводной сенсорной сети на основе новой комбинации признаков, позволяющая идентифицировать 14 типов атак сетевого уровня;

– метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе совместного применения алгоритмов машинного обучения и введения

параметра степени уверенности, позволяющий обеспечить заданную точность при использовании сокращенного признакового пространства;

– методика идентификации атак на беспроводные сенсорные сети, включающая предложенные модель профиля поведения и метод идентификации атак, а также разработанные в процессе исследования программные продукты

внедрены в проекте Минобрнауки России «Разработка методов агрегации, нормализации, анализа и визуализации больших массивов гетерогенных структурированных, полуструктурированных и неструктурированных данных для мониторинга и управления безопасностью распределенной сети электронных потребительских устройств №14-604-21-0147 (2014-2016); гранте РНФ «Управление инцидентами и противодействие целевым киберфизическим атакам в распределенных крупномасштабных критически важных системах с учетом облачных сервисов и сетей Интернета вещей» №15-11-30029 (2015-2017); в образовательном процессе факультета БИТ Университета ИТМО по направлениям подготовки бакалавриата 10.03.01 и магистратуры 10.04.01 по дисциплинам «Основы информационной безопасности», «Теория информационной безопасности и методология защиты информации», «Комплексные системы защиты информации»; при разработке системы мониторинга информационной безопасности для оперативного обнаружения и классификации злоумышленного воздействия на автоматизированные системы управления и наблюдения в информационной системе сети компании АК «Реактор»;

определены возможности и перспективы практического использования полученных результатов диссертации при разработке систем обнаружения вторжений и мониторинга состояния сети и проектировании защищенных систем на основе беспроводных сенсорных сетей;

создано модельно-алгоритмическое и программное обеспечение, представляющее собой основу для разработки системы обнаружения вторжений или мониторинга состояния сети на основе анализа комбинации признаков поведения сети для повышения эффективности идентификации атак сетевого уровня;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные модель, метод и методика.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ

достоверность полученных результатов подтверждена проведением всестороннего анализа современного состояния исследуемой проблемы, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными итогами практической реализации результатов работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов теории информационной безопасности и методологии защиты информации, методов теории информации, положений теории вероятности, методов математической статистики и вычислительного эксперимента, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области идентификации атак на компьютерные сети и обеспечении информационной безопасности беспроводных сенсорных сетей;

использованы полученные экспериментальные характеристики модели профиля поведения и метода идентификации атак для сравнения с данными, приведенными по обнаружению атак на беспроводные сенсорные сети в современной научной литературе;

установлено качественное и количественное соответствие результатов решения задачи разработки модели профиля поведения, метода и методики идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа комбинации признаков, характеризующих поведение сети. При этом подтверждено преимущество предложенного подхода перед результатами, полученными другими авторами.

использованы современные методики сбора и обработки исходной информации, методы теории информации, методы теории информационной безопасности и методологии защиты информации, положения теории вероятности, методы математической статистики и вычислительного эксперимента.

Личный вклад соискателя состоит в:

1. исследовании и анализе существующих методов идентификации атак на беспроводные сенсорные сети;
2. постановке задачи разработки научно-методического аппарата по идентификации атак сетевого уровня на беспроводные сенсорные сети;
3. выявлении показателей эффективности идентификации атак, таких как точность, полнота, количество идентификационных признаков, количество идентифицируемых атак;
4. разработке и обосновании модели профиля поведения беспроводной сенсорной сети на основе новой комбинации наиболее информативных признаков, выявляемых при анализе поведения сети;
5. разработке программной модели реализации атак на беспроводную сенсорную сеть и формирование набора данных; разработке программы комплексной оценки информативности признаков поведения сети;
6. разработке и обосновании метода идентификации атак сетевого уровня на основе совместного использования алгоритма «случайного леса» и вероятностного классификатора и введением параметра степени уверенности;
7. разработке и обосновании методики идентификации атак на беспроводные сенсорные сети;
8. анализе применимости предложенных модели, метода и методики при изменении параметров сети, величины параметра степени уверенности и априорной вероятности нормального поведения;
9. разработке практических рекомендаций по применению предложенного научно-методического аппарата;
10. подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Коржук В.М. в своей диссертационной работе решила научную задачу разработки и обоснования научно-методического аппарата по идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа новой комбинации признаков, характеризующих поведение такой сети, имеющую важное социально-экономическое и хозяйственное значение. Полученные результаты могут быть использованы для построения систем мониторинга состояния сетей и систем обнаружения вторжений в компьютерные сети различного назначения: в системах мониторинга состояния окружающей среды, в системах автоматизации управления помещениями, в том числе управления производством, в системах контроля и управления доступом.

На заседании 26.12.2019 г. диссертационный совет принял решение присудить Коржук В.М. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 22 человека, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 21, против нет, недействительных бюллетеней 1.

Председатель диссертационного совета
доктор технических наук,
член-корреспондент РАН Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
кандидат технических наук Зайцева Александра Алексеевна
26.12.2019 г.