ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Коржук Виктории Михайловны на тему: «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа», научный руководитель – к.т.н., доцент, декан факультета безопасности информационных технологий Университета ИТМО Заколдаев Д.А.

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Саенко И.Б. (председатель), д.т.н., проф. Осипова В.Ю., д.т.н., проф. Молдовяна А.А. после ознакомления с кандидатской диссертацией Коржук Виктории Михайловны на тему: «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» сделала вывод о том, что диссертационная работа Коржук В.М. посвящена решению актуальной научной задачи: разработка методики идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа новой комбинации признаков, характеризующего поведение такой сети, и совокупности алгоритмов машинного обучения, обеспечивающих достижение заданного уровня точности идентификации в условиях пассивного мониторинга поведения беспроводной сенсорной сети.

Целью исследования является повышение эффективности идентификации атак сетевого уровня на беспроводную сенсорную сеть при помощи оригинального научно-методического аппарата, основанного на анализе поведения сети. Значительная практическая значимость и недостаточная научная проработка проблемы определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационного исследования.

Практическую значимость исследования составляют разработанные в диссертации модель профиля поведения сети, метод и методика идентификации атак на беспроводную сенсорную сеть, которые обеспечивают решение актуальной научно-технической задачи, направленной на обеспечение информационной безопасности киберфизических систем, основанных на беспроводных сенсорных сетях, и которые вносят значительный вклад в развитие систем мониторинга и систем обнаружения вторжений в компьютерные сети. Результаты исследования внедрены в образовательном и научном учреждениях, коммерческом предприятии.

Использование предложенного набора признаков, формирующего модель профиля поведения сети, и метода идентификации на основе совокупности алгоритма «случайный лес» и вероятностного классификатора позволяет идентифицировать ряд атак, направленных на сетевой уровень беспроводной сенсорной сети, а введение параметра степени уверенности позволяет задать требуемый уровень точности, необходимой для идентификации. На основе разработанной методики идентификации возможна более гибкая настройка процесса идентификации, благодаря чему возможно повышение эффективности идентификации и использование результатов в качестве основы для построения системы обнаружения вторжений.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются использованием апробированного математического аппарата и подтверждается проведением сравнительного анализа с существующими методами; серией практических экспериментов по идентификации атак на беспроводные сенсорные сети; согласованностью результатов, полученных при теоретическом исследовании с результатами проведенных экспериментов, а также непротиворечивостью достигнутых результатов и результатов работ других авторов; практической апробацией результатов в научно-исследовательских проектах, деятельности производственных организаций и одобрением на научно-технических конференциях.

Материалы и основные результаты кандидатской диссертации Коржук В.М. удовлетворяют паспорту специальности: 05.13.19 – Методы и системы защиты информации, информационная безопасность, по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по материалам диссертационной работы опубликовано 17 научных работ, в том числе 11 статей, из которых 3 статьи в периодических журналах, рекомендованных ВАК (журналы «Проблемы информационной безопасности. Компьютерные системы», «Научно-технический вестник Поволжья», «Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки»).

Недостоверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованные соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 87%; цитирование оформлено корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Коржук В.М. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н., проф. Суханова А.В., к.т.н., доц. Красова А.В.
3. В качестве ведущей организации утвердить Федеральное государственное бюджетное образовательное учреждение высшего образования "Государственный университет морского и речного флота имени адмирала С.О. Макарова".
4. Разрешить Коржук В.М. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «26» декабря 2019 г.

Председатель комиссии: д.т.н., проф. Саенко И.Б.

Члены комиссии: д.т.н., проф. Осипов В.Ю.

д.т.н., проф. Молдовян А.А.