сильев

«01» октября 2019 г.

ЗАКЛЮЧЕНИЕ

Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО) Министерства науки и высшего образования Российской Федерации

Диссертация «Модель и метод идентификации сетевых атак на беспроводные сенсорные сети на основе поведенческого анализа» выполнена на факультете безопасности информационных технологий.

В период подготовки диссертации соискатель Коржук Виктория Михайловна работала в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики» (Университет ИТМО) Министерства науки и высшего образования Российской Федерации, факультет БИТ, ассистент.

В 2014 году окончила федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики» (Университет ИТМО) Министерства науки и высшего образования Российской Федерации, факультет БИТ по специальности 090103 – Организация и технология защиты информации.

В 2019 году окончила очную аспирантуру в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики» (Университет ИТМО) Министерства науки и высшего образования Российской Федерации, факультет БИТ по направлению 10.06.01 – Информационная безопасность.

Научный руководитель – Заколдаев Данил Анатольевич, к.т.н., доцент, федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики» (Университет ИТМО) Министерства науки и высшего образования Российской Федерации, декан факультета БИТ.

По итогам рассмотрения принято следующее заключение:

1. Личное участие соискателя ученой степени в получении результатов, изложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованных работах. Подготовка к

публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был значительным. Разработка гипотезы, планирование и проведение теоретических изысканий, стендовых и экспериментальных исследований выполнены лично автором. Представленные к защите результаты получены лично автором.

2. Степень достоверности результатов проведенных соискателем ученой степени исследований:

Достоверность подтверждена аналитическим обзором исследований и разработок в области идентификации атак на беспроводные сенсорные сети, уместным подбором методов исследования, соответствием выбранной модели как задачам исследования, так и объекту и предмету исследования, созвучностью полученных результатов опубликованным в литературе, внутренним и внешним единством отдельных данных и работы в целом, оценкой и сравнением полученных результатов с существующими методами и алгоритмами, положительными итогами компьютерного и практического моделирования результатов диссертационной работы, а также апробацией основных научно-практических положений в печатных трудах и докладах на международных конференциях.

3. Новизна и практическая значимость результатов исследования заключается в том, что:

разработана модель профиля поведения беспроводной сенсорной сети на основании новой комбинации признаков, позволяющая идентифицировать большее, по сравнению с существующими исследованиями, количество атак; разработан метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа поведения сети, отличающийся от существующих совместным использованием алгоритма «случайный лес» и вероятностного классификатора и введением параметра степени уверенности, позволяющего использовать неполный набор признаков профиля поведения сети; разработана методика идентификации атак, отличающаяся от существующих применением разработанных модели профиля поведения и метода идентификации атак, а также программ, созданных в процессе проведения исследования, и позволяющая повысить эффективности идентификации атак. Данные разработки могут быть использованы самостоятельно, в составе систем обнаружения вторжений и в рамках применения в киберфизических системах и позволяют повысить уровень доступности и целостности информации, циркулирующей в беспроводной сенсорной сети.

4. Ценность научных работ соискателя ученой степени.

Ценность научных работ заключается в том, что в них поставлена и решена научная задача развития и совершенствования научно-методического аппарата по идентификации атак на беспроводные сенсорные сети. Научные работы

соискателя развивают и дополняют теоретико-методические положения по исследуемым вопросам. Предложенные автором разработки по заявленной тематике, такие как модель профиля поведения сети и метод и методика идентификации атак на беспроводные сенсорные сети, программная модель проведения атак и вспомогательные программы определяют перспективы их практического использования системах обнаружения и идентификации атак. Основные положения диссертационного исследования и авторские разработки служат развитию научных основ и методологии обеспечения информационной безопасности беспроводных сенсорных сетей.

Диссертация соответствует научной специальности: 05.13.19 – Методы и системы защиты информации, информационная безопасность, а также требованиям, установленным п. 14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (ред. от 01.10.2018).

5. Полнота изложения материалов диссертации в работах, опубликованных соискателем.

Основное содержание диссертации опубликовано в 18 статьях, из них 8 публикаций в изданиях, рецензируемых Web of Science или Scopus, 4 публикаций в журналах из перечня ВАК и 3 свидетельства о регистрации программы для ЭВМ.

5.1. Научные издания, входящие в международные реферативные базы данных и системы цитирования:

1. Lebedev I.S., Korzhuk V.M. The Monitoring of Information Security of Remote Devices of Wireless Networks // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2015, Vol. 9247, pp. 3-10. 0,4 п.л. / 0,1 п.л. В статье поднимаются вопросы мониторинга информационной безопасности удаленных устройств самоорганизующихся беспроводных сетей. Показана модель взаимодействия удаленных устройств, определены анализируемые характеристики идентификации аномального поведения узлов для различных типов топологий. Предложен подход к оценке с использованием выделенных признаков системы.
2. Zikratov I.A., Lebedev I.S., Korzhuk V.M. The Estimation of Secure Condition of Multi-Agent Robotic System in Case of Information Influence on the Single Element // Proceedings of the 17th Conference of Open Innovations Association FRUCT - 2015, pp. 362-367. 0,3 п.л. / 0.1 п.л.. Целью работы является разработка подхода, использующего Марковские цепи для оценки безопасного состояния мультиагентной робототехнической системы, подвергающейся процессам информационного воздействия. Предлагаемые модели, методы и подходы направлены на обеспечение защищенного состояния мультиагентной робототехнической системы в условиях информационного воздействия.
3. Lebedev I.S., Korzhuk V., Krivtsova I., Salakhutdinova K., Sukhoparov M.E., Tikhonov D. Using Preventive Measures for the Purpose of Assuring Information Security of Wireless Communication Channels // Proceedings of the 18th Conference of

Open Innovations Association FRUCT - 2016, pp. 167-173 0,34 п.л. / 0,08 п.л. В статье описывается возможность применения превентивных мер для обеспечения информационной безопасности беспроводных каналов связи. Описываются особенности передачи информации по беспроводным каналам связи. Предложены рекомендации по использование превентивных мер для обеспечения целостности и доступности информации.

4. Lebedev I.S., Krivtsova I.E., Korzhuk V., Bazhayev N., Sukhoparov M.E., Pecherkin S., Salakhutdinova K. The Analysis of Abnormal Behavior of the System Local Segment on the Basis of Statistical Data Obtained from the Network Infrastructure Monitoring // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2016, Vol. 9870, pp. 503-511. 0,4 п.л. / 0,08 п.л. В статье предложен метод мониторинга информационной безопасности для беспроводных сетевых сегментов маломощных устройств «умный дом», «Интернет вещей». Проведен анализ характеристик систем на основе беспроводных технологий, возникающих в результате пассивного наблюдения и активного опроса устройств, входящих в состав сетевой инфраструктуры.

5. Korzhuk V., Krivtsova I., Shilov 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. 0,4 п.л. / 0,15 п.л. В статье предлагается программная модель проведения атак на беспроводные сенсорные сети. Приведено математическое и экспериментальное обоснование модели, описан функционал и возможности разработанной программы. Программная модель проведения атак была разработана с целью создания актуального набора данных о признаках сетевого уровня спецификации ZigBee и стандарта 802.15.4.

6. Zikratov I.A., Korzhuk V., Shilov 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. 0,4 п.л. / 0,15 п.л.. В данной статье поднимается вопрос обнаружения и идентификации атак сетевого уровня на беспроводные сенсорные сети. Описывается процесс выбора и формирования набора признаков о поведении беспроводной сенсорной сети стандарта 802.15.4 и спецификации ZigBee.

7. Korzhuk V., Shilov I., Torshenko J. Reduction of the Feature Space for the Detection of Attacks of Wireles Sensor Networks // Proceedings of the 20th Conference of Open Innovations Association FRUCT - 2017, pp. 195-201. 0,34 п.л. / 0,13 п.л.. Статья описывает процесс сокращения признакового пространства для обнаружения и идентификации атак сетевого уровня на беспроводные сенсорные сети. Описан математический аппарат оценки информативности признаков, составлено несколько наборов признаков различной полноты, необходимых для высокой точности идентификации.

8. 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. 1,15 п.л. / 0,8 п.л.. Статья описывает возможность применения вероятностного классификатора к процессу идентификации атак сетевого уровня. Приведено математическое обоснование возможности

использования метода, описан алгоритм идентификации атак при введении параметра уверенности. Предполагается совместное использование вероятностного классификатора и алгоритма «случайный лес».

5.2. Научные издания, входящие в перечень российских рецензируемых журналов:

1. Коржук В.М. Обеспечение информационной безопасности каналов связи на основе многофункционального специализированного программно-аппаратного решения / В.М. Коржук, М.Е. Сухопаров, И.С. Лебедев, И.Е. Кривцова, С.А. Печеркин // Проблемы информационной безопасности. Компьютерные системы - 2016. - № 2. - С. 70-74 0,23 п.л. / 0,09 п.л.. В статье описывается применение методов, обеспечивающих реализацию превентивных мер, направленных на повышение сложности реализации угроз информационной безопасности на компактном устройстве. Приведена оценка противодействия информационным атакам и смоделированы состояния устройства в различных режимах и при внедрении дополнительных элементов защиты.

2. Коржук В.М. Идентификация атак на беспроводные сенсорные сети на основе анализа аномального поведения сети / В.М. Коржук, П. Бонковски // Научно-технический вестник Поволжья - 2018. - № 2. - С. 83-85 0,22 п.л. / 0,15 п.л.. В статье описан разрабатываемый метод идентификации атак на сенсорные сети. Выбраны признаки, характеризующие различные атаки на информационную безопасность беспроводных сенсорных сетей; разработано признаковое пространство. Проведен анализ и выбран наиболее подходящий для поставленных условий и целей метод машинного обучения.

3. Коржук В.М. Введение параметра степени уверенности в процесс идентификации атак на киберфизические системы / В.М. Коржук, А.В. Грозных, Д.А. Заколдаев // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки» - 2019. - №10. 0,53 п.л. / 0,33 п.л.. В данной статье описан метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа. Предложена вариация метода с использованием параметра степени уверенности, позволяющая задавать допустимый уровень точности идентификации атак и количество используемых признаков. Сформулированы рекомендации по применению предложенного решения.

4. Коржук В.М. Методика идентификации атак на беспроводные сенсорные сети на основе анализа поведения сети // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки» - 2019. - №10. 0,43 п.л.. В данной статье представлена методика идентификации атак на беспроводные сенсорные сети. Разработанная методика позволяет использовать определенный набор признаков для идентификации 14 типов сетевых атак. Описывается и обосновывается применение разработанных в рамках исследования компьютерных программ, необходимых для повышения эффективности идентификации атак на беспроводные сенсорные сети. Для идентификации совместно применяются алгоритм «случайный лес» и вероятностный классификатор.

5.3. Публикации, которые приравниваются к рецензируемым научным изданиям:

1. Коржук В.М. Программная модель атак на беспроводные сенсорные сети ZigBee / В.М. Коржук, А.А. Воробьева, И.М. Шилов. – Свидетельство о государственной регистрации программы для ЭВМ №2018617190 от 20.06.2018
2. Коржук В.М. Программа подсчета информативности признаков статистической выборки / В.М. Коржук, А.А. Воробьева, И.М. Шилов. – Свидетельство о государственной регистрации программы для ЭВМ № 2018618975 от 24.07.2018
3. Коржук В.М. Программа вычисления апостериорных распределений дискретного параметра распределения многомерной случайной величины по статистической выборке / В.М. Коржук, А.А. Воробьева, А.В. Грозных. – Свидетельство о государственной регистрации программы для ЭВМ № 2018619014 от 25.07.2018

Диссертация «Модель и метод идентификации сетевых атак на беспроводные сенсорные сети на основе поведенческого анализа» Коржук Виктории Михайловны подготовлена в соответствии требованиям п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (ред. от 01.10.2018) и пунктам 3 и 14 Паспорта специальности ВАК (технические науки) по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Диссертация рекомендуется к защите на соискание ученой степени кандидата наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Заключение подготовлено на заседании факультета БИТ.

Присутствовало на заседании 67 чел.

Результаты голосования: «за» - 65 чел., «против» - 0 чел., «воздержалось» - 2 чел., протокол № 6 от «18» июня 2019 г.

Руководитель подразделения

к.т.н., доцент,
декан факультета БИТ_____ _____ Заколдаев Д.А.

Диплом об окончании аспирантуры № 107824 4740980
Выдан «08» июля 2019 г.
Подпись _____ / Даниленко Д.В.
Сотрудника отдела МАИД ИТМО