ОТЗЫВ

официального оппонента Суханова Андрея Вячеславовича на диссертацию Коржук Виктории Михайловны «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа», представленной на соискание учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертации

В современном мире широкое распространение приобретают маломощные сети, состоящие из большого количества беспроводных сенсоров, способных к самоорганизации и работающих на элементах питания ограниченной ёмкости. Они предназначены для организации взаимодействия глобальных компьютерных сетей и физического мира и, фактически, являются основой для киберфизических систем. Беспроводные сенсорные сети находят применение во многих сферах жизнедеятельности общества: в мониторинге состояния различных объектов (окружающей среды, производственных процессов и т.д.), при организации систем контроля и управления доступом, при разработке систем автоматизации помещений и производства, в медицине и организации беспилотного движения. Как правило, такие сети передают данные по открытому каналу связи, и реализация компьютерных атак, направленных на нарушение конфиденциальности, целостности и доступности информации, являются относительно простыми.

Несмотря на то, что в настоящее время существует множество методов обнаружения атак на беспроводные сети, комплексных систем мониторинга состояния сети и обнаружения вторжений, обеспечение информационной безопасности беспроводных сенсорных сетей остается актуальной проблемой из-за таких особенностей и ограничений, как малый объем памяти и энергоресурсов сетей, относительно невысокая скорость передачи. Поскольку для данных сетей критически важно обеспечение доступности и целостности информации, необходимо своевременное обнаружение и противодействие атакам, связанным с сетевым уровнем передачи, без использования активного мониторинга сети. Решению описанной выше задачи в полной мере посвящена диссертационная работа Коржук Виктории Михайловны. Этим определяется **актуальность** темы рассматриваемой диссертации и полученных в ней результатов.

В ходе решения описанной выше задачи автором диссертации получены следующие новые научные положения, выносимые на защиту:

1. модель профиля поведения беспроводной сенсорной сети;
2. метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа;
3. методика идентификации атак на беспроводные сенсорные сети.

2. Оценка сущности и содержания диссертации

Диссертационная работа состоит из 206 страниц и включает три главы.

Первая глава диссертации посвящена описанию исследуемой области, постановке и обоснованию научной назади. Представлены результаты анализа текущего состояния проблемы идентификации атак, описаны существующие методы и сформулированы их ограничения. Обоснована актуальность исследования, выделены показатели эффективности идентификации. Сформулирована и формализована научная задача исследования.

Во **второй главе** диссертации представлена формальная модель профиля поведения беспроводной сенсорной сети, позволяющая определить до 14 атак сетевого уровня. Описана и математически обоснована программная модель проведения атак, используемая для формирования набора данных. Проведен анализ существующих алгоритмов классификации и предложен метод идентификации атак с задаваемым параметром уверенности на основе комбинации случайного леса и Байесовского классификатора.

Третья глава диссертации описывает разработанную методику идентификации атак на основе поведенческого анализа, результаты проведенных экспериментов при изменении параметров сети и настроек метода идентификации. Показано, что представленные модель, метод и методика являются в достаточной мере универсальными и подходят для сетей с различной топологией и количеством устройств. Сформулированы краткие практические рекомендации, касающиеся разработки программно-аппаратного решения и дополнительных настроек метода и методики.

Исследования проводились с использованием методов теории информации, системного анализа, классификации, методов математической статистики и вычислительного эксперимента. Программная реализация осуществлена с помощью методов объектно-ориентированного программирования.

3. Научная новизна, достоверность и обоснованность, практическая значимость результатов работы

3.1 Научная новизна первого положения диссертационной работы определяется тем, что автором впервые предложена формальная модель профиля поведения беспроводной сенсорной сети, представляющая собой новую комбинацию сетевых признаков, которая, в отличие от существующих, позволяет обнаружить большее количество атак.

Научная новизна второго положения обосновывается тем, что разработанный метод идентификации атак на основе поведенческого анализа заключается в новой комбинации алгоритмов анализа данных и введения субъективного параметра уверенности. Метод позволяет установить величину допустимой точности и сократить необходимое для положительной идентификации количество анализируемых признаков.

Научная новизна третьего положения определяется тем, что разработанная методика идентификации атак, в отличие от известных, включает в себя предварительную настройку модели профиля поведения и метода идентификации, а также использование разработанных программной модели проведения атак, программы оценки информативности и подсчета статистических параметров и позволяет повысить эффективность идентификации.

3.2 Теоретическая значимость результатов научного исследования заключается в возможности дальнейшего развития разработанного научно-методического аппарата в области обеспечения информационной безопасности беспроводных сенсорных сетей в частности и киберфизических систем в целом, а также в повышении гибкости и эффективности систем мониторинга и обнаружения вторжений.

3.3 Практическая значимость результатов работы состоит в том, что разработанный научно-методический аппарат частично доведен до уровня программной реализации и позволяет повысить качество идентификации атак за счет комбинирования различных классификаторов. Соответственно, он может применяться как дополнение к существующим системам обнаружения вторжений на беспроводные сети, так и в решении других более общих задач, связанных с идентификацией и классификацией поведения.

Помимо этого, о практической значимости результатов исследования свидетельствует реализация ее основных результатов в различных научно-исследовательских работах, при разработке системы мониторинга информационной безопасности коммерческого предприятия, а также в дисциплинах по соответствующим направлениям подготовки бакалавров и магистров.

3.4 Достоверность и обоснованность результатов исследования определяются применением апробированных средств и методов исследования, корректностью принятых допущений и ограничений, достоверностью исходных данных, оказывающих существенное влияние на анализ предметной области, серией расширенных экспериментов, непротиворечивостью полученных результатов и их согласованностью с результатами исследований, проведенных другими авторами по тематике, близкой к теме диссертационной работы, а также актами внедрения и публикациями в рецензируемых изданиях.

4. Оценка содержания и степени завершенности работы

Диссертационная работа Коржук Виктории Михайловны представляет собой завершенный научный труд, обладающий внутренним единством и содержащий новые научные результаты и положения, представленные к публичной защите. Диссертация оформлена в соответствии с действующими требованиями ВАК и включает введение, три главы, заключение, список сокращений, список литературы и пять приложений. Работа построена логично, аккуратно оформлена и в достаточной мере иллюстрирована. Стиль изложения ясный, лаконичный, литературный; текст работы не перегружен излишними промежуточными выкладками, что облегчает его чтение и свидетельствует о научной культуре автора. Автором проведен

подробный анализ области исследований, предложенные решения в достаточной степени аргументированы и адекватно оценены, что свидетельствует о личном вкладе автора диссертации в науку. Список использованной литературы содержит 221 наименование, включая работы иностранных авторов, текст работы содержит соответствующее количество ссылок.

5. Характеристика автореферата диссертации

Автореферат диссертации составлен в соответствии с требованиями «Положения о присуждении ученых степеней», его содержание вполне отражает основные результаты и выводы диссертации. Материал в автореферате изложен в достаточной мере логично и грамотно, стиль написания позволяет понять содержание этапов исследований.

6. Публикации и апробация основных результатов диссертации

Основные результаты диссертации изложены в 17 научных работах, среди которых: 3 статьи – в изданиях, рекомендованных перечнем ВАК, 8 статей – в журналах, индексируемых Scopus, 6 – в других изданиях. Присутствуют 3 свидетельства о государственной регистрации программ для ЭВМ. Результаты и научные положения работы апробированы на международных и региональных научных конференциях, в частности, на конференции по передовым проводным и беспроводным сетям и системам нового поколения (NEW2AN), конференции по Интернету вещей и умным пространствам (ruSMART), конференции по информационной безопасности и защите информационных технологий (IS&PIT) и других.

7. Замечания по диссертации

1. В тексте диссертации приведено вербальное описание атак на беспроводные сенсорные сети, однако отсутствует формальное представление. Более наглядно возможно было бы представить атаки с помощью, например, цепей Маркова.

2. При описании поведения беспроводной сенсорной сети не учитывается динамика и продолжительность атак, что, в конечном счете, может негативно повлиять на результаты идентификации на основе поведенческого анализа.

3. Во второй главе при обосновании модели профиля поведения сети упоминаются стандарт 802.15.4 и протокол ZigBee, однако не указано, имеются ли существенные различия между протоколами и будут ли эффективны предложенные решения для сетей, использующих другие протоколы.

4. Некоторые иллюстрации, представленные в диссертации, имеют недостаточно крупные подписи, что затрудняет восприятие графического материала (например, рис. 2.14, 2.16).

Указанные замечания в определенной степени снижают значимость результатов диссертационной работы, однако не влияют на общую высокую оценку качества выполненной работы и положительное мнение о ее результативности и завершенности.

Заключение

В представленной диссертации решена важная научная задача по разработке научно-методического аппарата для идентификации атак сетевого уровня на беспроводные маломощные сети датчиков на основе анализа характеристик поведения исследуемых сетей. Работа Коржук В.М. «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» полностью соответствует требованиям пунктов 9÷14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года № 842 (в ред. Постановлений Правительства РФ от 21.04.2016 № 335, от 02.08.2016 № 748, от 29.05.2017 № 650, от 28.08.2017 № 1024 и 01.10.2018 № 1168), предъявляемым к кандидатским диссертациям, а ее автор, Коржук Виктория Михайловна, заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Официальный оппонент:
доктор технических наук, доцент
советник генерального директора АО «ЭВРИКА»

Суханов Андрей Вячеславович

«3» декабря 2019 г.

Подпись Суханова Андрея Вячеславовича удостоверяю.
Начальник управления кадров и документационного обеспечения АО «ЭВРИКА»

Дмитриченко Анастасия Викторовна

«3» декабря 2019 г.

Сведения о составителе отзыва:
ФИО: Суханов Андрей Вячеславович
Ученая степень: доктор технических наук
Ученое звание: доцент
Место работы: акционерное общество «ЭВРИКА»
Должность: советник генерального директора
Почтовый адрес: 196084, г. Санкт-Петербург, Московский пр., д. 118
Телефон: (812) 718-61-91
Эл. почта: avsuhanov@eureca.ru