УТВЕРЖДАЮ:
Ректор ФГБОУ ВО «ГУМРФ имени
О. Макарова»,
ческих наук, профессор
ов

«14» ноября 2019 г.

ОТЗЫВ

ведущей организации

на диссертационную работу 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»

Актуальность темы диссертации

В диссертационной работе решается задача разработки и обоснования научно-методического аппарата по идентификации атак сетевого уровня на беспроводные сенсорные сети (БСС) на основе анализа новой комбинации признаков, характеризующего поведение такой сети.

В современных автоматизированных системах, в основе которых лежат БСС, важное значение приобретают системы мониторинга состояния сети и системы обнаружения вторжений. Применение таких систем необходимо для своевременной реакции на изменения поведения сети, которые могут быть вызваны не только внутренними параметрами и техническими сбоями, но и злоумышленным воздействием. При этом необходимо обеспечивать достаточный уровень целостности и доступности информации, циркулирующей в таких сетях. Известные решения в области обнаружения атак на беспроводные сети не в полной мере подходят для БСС из-за ограничений, связанных с устройством узлов сети, что обуславливает недостаточную эффективность применяемых средств защиты информации. Более того, частные решения, направленные на обнаружение и идентификацию атак в БСС, позволяют идентифицировать малое количество атак и не имеют гибкой методики идентификации. Указанные противоречия приводят к необходимости разработки научно-методического аппарата для идентификации атак сетевого уровня на БСС с помощью анализа поведенческих характеристик такой сети.

Диссертационное исследование Коржук Виктории Михайловны направлено на решение данной задачи, что обуславливает ее актуальность и востребованность полученных результатов.

Соответствие темы диссертации научной специальности

Диссертация Коржук Виктории Михайловны является законченной научной работой, в которой в качестве объекта исследования рассматриваются системы обеспечения информационной безопасности БСС, а в качестве предмета исследования – модели и методы идентификации атак сетевого уровня на БСС.

Тема и содержание диссертации Коржук В.М. соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», в частности, по следующим пунктам:

Пункт 3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

Пункт 14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.

Структура диссертационной работы

Диссертация состоит из введения, трех глав, заключения, списка сокращений и условных обозначений, библиографического списка и пяти приложений.

Во введении обоснована актуальность работы, ее научная значимость, новизна, теоретическая и практическая ценность. Описаны принципы используемых подходов. Сформулированы цель и задачи, предмет и объект исследования. Приведены основные положения, выносимые на защиту, изложены сведения о внедрении и апробации результатов работы, публикациях автора по теме диссертации.

В первой главе приведен анализ современного состояния проблемы защиты информации в БСС. Описана специфика обеспечения информационной безопасности в таких сетях, сформулированы ограничения и допущения исследования. Обоснованы модели угроз и нарушителя информационной безопасности в БСС, выделен перечень исследуемых атак. Проведен анализ существующих моделей и методов идентификации атак на беспроводные сети. Выбраны показатели эффективности идентификации атак, представляющие собой точность, полноту, количество идентифицируемых атак, и количество идентификационных признаков.

Предложена формальная постановка задачи диссертационного исследования.

Во второй главе описана формальная модель профиля поведения БСС. Представлен процесс формирования набора данных об атаках и предложен математических аппарат для моделирования реализации атак на БСС. Осуществлена оценка информативности признаков модели профиля поведения с помощью нескольких методов. Предложен метод идентификации атак на основе алгоритма «случайный» лес на основе представленной модели профиля поведения, а также сделано предположение о возможности использования неполного набора признаков для идентификации атак. Обосновано применение вероятностного классификатора и параметра степени уверенности для повышения эффективности метода идентификации.

В третьей главе представлена методика идентификации атак на БСС, позволяющая использовать разработанные в процессе работы программы для ЭВМ. Описаны расширенные эксперименты по оценке эффективности при условии изменения параметров сети, уровня степени уверенности и изменения вероятности нормального поведения сети. Проведена комплексная оценка разработанных модели, метода и методики с учетом данных описанных экспериментов, а также сформулированы практические рекомендации, касающиеся возможных вариантов определения аномального поведения сети, действий администратора сети, дальнейших разработок в области программно-аппаратного средства мониторинга.

В заключении представлены основные результаты, полученные соискателем, и выводы по работе.

В приложениях представлены разработанные модели угроз и нарушителя для БСС, средние значения признаков, характеризующих различные варианты поведение сети, а также листинги программ, свидетельства о регистрации программ для ЭВМ и копии актов внедрения.

Общий объем работы составляет 206 страниц с приложениями и 221 источников литературы. По объему и структуре работа в целом соответствует требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук.

Научная новизна результатов

В диссертационной работе Коржук Виктории Михайловны получены следующие основные результаты, обладающие научной новизной:

1. Разработана модель профиля поведения БСС, представляющая собой новую комбинацию признаков поведения, обоснована ее корректность. Доказана возможность идентификации 14 различных атак на БСС на основе

описанной модели при условии различных топологий и других настроек сети.

2. Предложен метод идентификации атак сетевого уровня на БСС, позволяющий задавать необходимую точность идентификации при использовании подвектора признаков разработанной модели, за счет совокупного применения алгоритма «случайный лес» и вероятностного классификатора.

3. Разработана методика идентификации атак на БСС, повышающая эффективность идентификации атак, учитывающая такие показатели, как количество анализируемых признаков, количество распознаваемых атак, точность и полнота классификатора. Предложенная методика включает в себя разработанные модель и метод, а также программы для ЭВМ, созданные в процессе проведения исследования.

Достоверность и обоснованность результатов исследований

Достоверность результатов проведенного исследования подтверждается корректностью использования математического аппарата, корректным формированием комплекса ограничений и допущений и сравнительным анализом с существующими методами. Для обоснования принятых в ходе исследования решений и проверки достоверности полученных результатов соискателем осуществлена разработка программной модели реализации атак на БСС, проведена серия практических экспериментов. Адекватность разработанных модели, метода и методики подтверждена согласованностью теоретических расчетов с экспериментальными данными и практическими результатами, а также непротиворечивостью достигнутых результатов и результатов работ других авторов.

Значимость полученных автором диссертации результатов для развития соответствующей отрасли науки

Теоретическая значимость диссертационной работы заключается в развитии методов повышения эффективности детектирования и идентификации сетевых атак за счет разработки математического, методического и алгоритмического обеспечения процесса идентификации атак сетевого уровня на БСС на основе анализа поведенческих характеристик, что позволяет обеспечить необходимых уровень защищенности информационных ресурсов.

Практическая ценность диссертационной работы определяется разработкой комплекса программных средств, реализующих отдельные этапы процесса идентификации атак, а также разработкой практических

рекомендаций для применения полученных результатов. Описанный научно-методический аппарат может быть использован для защиты компьютерных сетей различного назначения.

Рекомендации по использованию результатов и выводов, приведенных в диссертации

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 т.ч. управление производством, в системах контроля и управления доступом. В частности, результаты исследования могут применяться для проведения аудита информационной безопасности в ЗАО «Перспективный мониторинг», при разработке информационных систем в АО «Эврика», при разработке программно-аппаратных средств защиты информации в ОАО «Инфотекс», АО «Лаборатория Касперского», ЗАО «РНТ». Также, результаты могут быть использованы для подготовки специалистов по информационной безопасности, например, в Университете ИТМО.

Полнота опубликованных результатов работы, их соответствие паспорту специальности, внедрение результатов диссертационной работы

Представленная диссертация выполнена с соблюдением основных рекомендаций, установленных ВАК при Минобрнауки России. Стиль изложения в целом соответствует требованиям к научным работам. Ссылки на библиографические источники, включая собственные публикации автора, оформлены в соответствии с требованиями стандарта, а библиографический список достаточно полно характеризует выбранное автором научное направление.

Основные материалы диссертации опубликованы в 11 рецензируемых научных изданиях, в т.ч. 3 публикации – в журналах, рекомендуемых ВАК при Минобрнауки России, и 8 – в Scopus. Соискателем получено 3 свидетельства об официальной регистрации программ для ЭВМ. Результаты работы применяются на практике, что подтверждается актами о внедрении результатов исследования от федерального государственного бюджетного учреждения науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук», федерального государственного автономного образовательного учреждения высшего образования

«Национальный исследовательский университет ИТМО» и коммерческой организации «Реактор».

По представленному библиографическому списку и прилагаемому перечню собственных публикаций автора можно сделать вывод о том, что основные положения диссертации достаточно полно изложены в печати и апробированы на конференциях.

Автореферат адекватно отражает текст диссертации.

Основные замечания по диссертации

В качестве недостатков работы можно отметить следующие:

1. Не вполне понятно, в соответствии с каким принципом были выбраны приведенные в первой главе показатели эффективности процесса идентификации. Также не указано, каким образам представленным показателям присваивались весовые коэффициенты.

2. В главе второй осуществляется выбор алгоритма машинного обучения, применяющегося для классификации признаков поведения, однако не произведена оценка его сложности и быстродействия. В рамках применения в системах обнаружения вторжений в БСС эти показатели являются особенно важными.

3. В тексте диссертации при описании экспериментов встречается информация об обучающих и тестовых выборках, однако явно не указывается, какое количество записей было использовано для обучения и тестирования классификаторов.

4. При описании разработанной методики идентификации атак не приводятся в соответствие этапам методики формальные выражения, используемые в тесте диссертации.

Отмеченные недостатки носят частный характер и не снижают ценности полученных соискателем научных результатов.

Заключение

Диссертационная работа Коржук Виктории Михайловны является самостоятельной научно-квалификационной работой, обладает внутренним единством, и раскрывающей сформулированную автором цель исследования. В диссертации соискателем решена актуальная научная задача по разработке научно-методического аппарата по идентификации атак на БСС, позволяющей повысить эффективность идентификации атак сетевого уровня при проведении анализа поведенческих характеристик БСС, имеющая важное значение для развития цифровых технологий в области защиты информации в целом и систем обнаружения вторжений в частности. Полученные автором результаты достоверны, подтверждены

экспериментально, на должном уровне прошли апробацию и внедрены в практику.

На основании изложенного можно сделать вывод, что диссертация «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» соответствует критериям, изложенным в пунктах 9-14 Положения «О порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 года № 842 в редакции от 01.10.2018 года, предъявляемым к кандидатским диссертациям, а ее автор Коржук Виктория Михайловна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа Коржук Виктории Михайловны обсуждена на заседании кафедры комплексного обеспечения информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», протокол № 3 от «12» ноября 2019 года.

Заведующий кафедрой
комплексного обеспечения
информационной безопасности,
д.т.н., доцент Соколов Сергей Сергеевич

Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова» (ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»).
Двинская ул., д. 5/7, г. Санкт-Петербург, 198035; тел.: (812) 748-96-92;
e-mail: otd_o@gumrf.ru http://www.gumrf.ru